Communication de la CNIL relative à la mise en oeuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données

SOMMAIRE

I. La place de l'empreinte digitale au sein des données biométriques

Lorsque, en 2004, le Législateur a conféré à la CNIL un pouvoir d'autorisation concernant les traitements automatisés comportant des données biométriques, il a pris en compte la sensibilité particulière de ces nouvelles techniques d'identification mais il ne pouvait mesurer à quel point l'explosion de la biométrie allait influer sur son activité. En effet, le nombre de demandes d'autorisation adressées à la Commission ne cesse d'augmenter d'année en année. Entre 1978 et 2004, la CNIL a examiné 34 dispositifs biométriques ; 788 depuis 2004 ![1] Actuellement plus de 150 dispositifs sont en cours d'examen la tendance ne fait que s'accentuer.

De plus le recours à la biométrie concerne des usages toujours plus variés (contrôle d'accès, gestion des horaires,…). Les données biométriques, et plus particulièrement l'empreinte digitale, acquièrent en conséquence de plus en plus de valeur. Ainsi, même si tous les risques de dérive ne peuvent aujourd'hui être répertoriés, il est du rôle de la CNIL de les anticiper.

C'est pourquoi, compte tenu de l'évolution technologique dans ce domaine et de la diversité des situations rencontrées, la Commission estime nécessaire de rappeler et de préciser les principaux critères sur lesquels elle se fonde pour examiner les demandes d'autorisation des dispositifs biométriques reposant sur la reconnaissance des empreintes digitales avec un stockage sur un terminal de lecture-comparaison ou sur un serveur. Il s'agit de permettre aux entreprises, administrations, collectivités locales qui envisagent de se doter de tels dispositifs de se poser « les bonnes questions informatique et libertés » avant de prendre leur décision et de déposer, auprès d'elle, une demande d'autorisation.

A. Les données biométriques sont des données d'identité

La biométrie recouvre l'ensemble des procédés tendant à identifier un individu à partir de la « mesure » de l'une ou de plusieurs de ses caractéristiques physiques, physiologiques ou comportementales. Il peut s'agir des empreintes digitales, de l'iris de l'œil, du contour de la main, de l'ADN ou d'éléments comportementaux (la signature, la démarche)...

A la différence de toute autre donnée d'identité, et à plus forte raison de toute autre donnée à caractère personnel, la donnée biométrique n'est pas attribuée par un tiers ou choisie par la personne : elle est produite par le corps lui-même et le désigne ou le représente, lui et nul autre, de façon immuable. Elle appartient donc à la personne qui l'a générée. On comprend dès lors que toute possibilité de détournement ou de mauvais usage de cette donnée fait peser un risque majeur sur son identité. Confier ses données biométriques à un tiers, lui permettre de les enregistrer et de les conserver n'est donc jamais un acte anodin : cela doit répondre à une nécessité a priori exceptionnelle, justifiée, et être entouré de garanties sérieuses.

[1] La répartition est la suivante : 33 refus - 109 autorisations après examen en séance plénière de la Commission - 646 dans le cadre de procédures simplifiées *(cf. infra)*.

Le Législateur n'a pas souhaité établir les règles définissant le bon ou le mauvais usage de la biométrie. Il a donc confié à la CNIL la mission d'autoriser les traitements informatisés comportant des données biométriques « *nécessaires au contrôle de l'identité des personnes* ». Pour les traitements mis en oeuve par l'Etat, c'est la procédure d'un décret en Conseil d'Etat, pris après avis motivé et publié de notre Commission, qui s'applique.

B. Le statut particulier de l'empreinte digitale

1. La trace et les risques de dérive

Parmi toutes les données biométriques utilisées aujourd'hui, l'empreinte digitale présente la caractéristique d'être une biométrie à « trace » : chaque personne laisse des traces de ses empreintes digitales, plus ou moins facilement exploitables, dans beaucoup de circonstances de la vie courante[2].

Ces « traces » peuvent donc être capturées à l'insu des personnes concernées et il en résulte des risques de dérive. Ainsi, l'exemplaire de l'empreinte récupéré peut être utilisé pour :

- procéder à l'identification d'une personne à son insu par rapprochement avec un fichier nominatif d'empreintes digitales ;
- usurper l'identité d'une personne, c'est-à-dire utiliser l'exemplaire de l'empreinte relevé pour frauder un dispositif reposant sur la reconnaissance de l'empreinte digitale.

Il faut être d'autant plus vigilant :

- qu'il est possible de se procurer, sur de nombreux sites internet et à faible coût, des « kits » permettant de relever des empreintes digitales ;
- que plusieurs études ont permis de démontrer la possibilité de frauder en trompant le lecteur d'empreintes grâce à un « faux doigt ».

2. Empreintes digitales avec ou sans maîtrise par son détenteur :

La prise en compte de la particularité de l'empreinte digitale et des risques associés a amené la CNIL à distinguer les dispositifs en fonction du mode de stockage des empreintes ou des gabarits d'empreintes[3] utilisés.

a) Stockage sur un support individuel (maîtrise des données par le détenteur)

[2] Par exemple sur un verre ou une poignée de porte etc. A noter que c'est aussi le cas des empreintes génétiques. D'autres biométries ne présentent pas cette caractéristique (contour de la main, réseau veineux) en l'état actuel de la technologie.

[3] Identifiant (suite alphanumérique) calculé grâce à un algorithme à partir des points caractéristiques (minuties) présents sur l'empreinte digitale.

Dans le cas d'un stockage sur un support individuel (tel que carte à puce ou clé USB), exclusivement détenu par la personne concernée, **la personne a la maîtrise de sa donnée biométrique.** Celle-ci reste sous sa responsabilité et ne peut pas être utilisée pour l'identifier à son insu. En cas de vol ou de perte du support de stockage, on ne peut avoir accès qu'à une seule donnée biométrique éventuellement associée à l'identité de la personne.

b) Stockage sur un support non individuel (maîtrise des données par un tiers)

Dans le cas d'un stockage sur le terminal de lecture-comparaison ou sur un serveur, la personne perd la maîtrise de sa donnée biométrique qui est ainsi détenue par un tiers[4]. En cas d'intrusion dans le terminal ou le serveur, on peut accéder à l'ensemble des empreintes ou gabarits qui y sont stockés et qui sont généralement associés aux identités des personnes.

A ce stade, chacun comprend que les risques de dérive sont plus importants dans le second cas que dans le premier puisqu'il y a là une plus grande concentration de données d'identification dont le contrôle échappe aux personnes concernées.

Ce constat a amené notre Commission à considérer que si les deux modes de stockage pouvaient être utilisés, seul un fort impératif de sécurité peut justifier le stockage sur un terminal de lecture-comparaison ou sur un serveur.

REMARQUE

Si un mot de passe a été divulgué, il est possible de le renouveler. En revanche, il est impossible de changer son empreinte digitale qui est un élément du corps humain. C'est pourquoi, le risque de « divulgation » ou de « corruption » de cette donnée est d'autant plus sensible.

3. La distinction entre authentification et identification :

a) L'authentification biométrique :

L'authentification revient à vérifier, *via* le dispositif biométrique, que le porteur de la carte ou du badge d'accès est bien le bon titulaire. Techniquement, le système vérifie que l'empreinte digitale du doigt apposé sur le lecteur, par le porteur de la carte, correspond au gabarit enregistré dans la carte.
On parle alors de mode « *1 contre 1* » : l'utilisateur présente une donnée, et elle est comparée à une seule donnée. L'opération consiste à s'assurer de la similitude entre le doigt apposé sur le lecteur et le gabarit stocké sur la carte.

Dans ce mode d'utilisation, il n'est pas nécessaire de connaître l'identité de la personne *a priori* ni de stocker cette information dans une partie du système qui ne serait pas totalement sous contrôle de l'utilisateur. En effet, il n'est pas indispensable d'associer un gabarit biométrique à une identité pour que le contrôle d'accès biométrique puisse fonctionner. Dans ce cas, les risques de dérives visant à utiliser le dispositif pour identifier et « tracer » une personne à son insu sont, à l'évidence, limités.

[4] Son employeur, un prestataire, une administration…

b) L'identification biométrique :

L'identification consiste à s'assurer, via le système biométrique, de l'identité de la personne, par rapprochement avec un fichier nominatif comprenant plusieurs personnes . À partir de l'empreinte digitale du doigt apposé sur le lecteur, le dispositif recherche s'il y a un gabarit correspondant dans la mémoire du terminal de lecture-comparaison ou du serveur. Ce gabarit est lui même associé à l'identité de la personne.

On parle alors de mode « *1 contre N* » : l'utilisateur présente une donnée et elle est comparée à toutes celles qui sont stockées dans le système. **Ce type de procédé est plus intrusif** au regard de la protection des données dans la mesure où :

- il repose nécessairement sur un stockage des données dans un terminal de lecture-comparaison ou sur un serveur ;
- il implique nécessairement d'associer la donnée biométrique à d'autres éléments d'identité.

RAPPEL

Tous les dispositifs biométriques sont soumis à l'autorisation préalable de la CNIL. Les dispositifs reposant sur le stockage des empreintes digitales dans un support individuel comportant moins de risques, ils bénéficient d'un régime d'autorisation simplifié. Ainsi, si le dispositif a pour finalité le contrôle de l'accès aux locaux par les employés[5], l'autorisation est délivrée automatiquement dans un délai d'une semaine. La procédure consiste, dans ce cas, à se connecter au site de la CNIL et effectuer un engagement de conformité à l'autorisation unique AU-007[6].

[5] A ce jour, l'utilisation de dispositifs reposant sur la reconnaissance des empreintes digitales doit se limiter au contrôle d'accès. En effet, dans un jugement du 19 avril 2005, le Tribunal de grande instance de Paris a indiqué, concernant un dispositif de contrôle des horaires des salariés reposant sur la reconnaissance des empreintes digitales, que l'utilisation d'un élément *« qui met en cause le corps humain et porte ainsi atteinte aux libertés individuelles peut cependant se justifier lorsqu'elle a une finalité sécuritaire ou protectrice de l'activité exercée dans des locaux identifiés. »* En l'espèce, faisant application de l'article L. 120-2 du Code du travail qui dispose que *« nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché »*, le Tribunal a interdit la mise en œuvre dudit traitement considérant qu'il n'apparaissait ni adapté ni proportionné au but recherché.

[6] Les dispositifs reposant sur la reconnaissance du contour de la main bénéficient également d'une procédure d'autorisation simplifiée. En effet, le contour de la main est une donnée biométrique qui ne laisse pas de traces susceptibles d'être captées à l'insu de la personne et d'être utilisées à des fins étrangères à la finalité initiale. La Commission a ainsi adopté deux autorisations uniques : AU-007 du 27.04.2006 relative aux dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail ; AU-009 du 27.04.2006 relative aux traitements de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire.

II. Les critères de l'autorisation par la Commission

Sur quels critères notre Commission se fonde-t-elle pour autoriser ou non les dispositifs reposant sur la reconnaissance des empreintes digitales avec un stockage dans une base de données ?

Quatre questions doivent être posées.

A. Première question : la finalité du dispositif de reconnaissance par empreinte digitale avec stockage dans une base de données

Pour la Commission, la finalité d'un tel dispositif de reconnaissance des empreintes digitales doit être **limitée au contrôle de l'accès d'un nombre limité de personnes à une zone bien déterminée**[7] représentant ou contenant un **enjeu majeur dépassant l'intérêt strict de l'organisme et ayant trait à la protection de l'intégrité physique des personnes ou à celle des biens et des installations ou à celles de certaines informations**.

1. La protection de l'intégrité physique des personnes

En ce qui concerne les personnes, ce qui est en jeu, c'est leur intégrité physique. Il doit s'agir :

- **de protéger des installations comportant un risque élevé d'explosion ou de diffusion de matières dangereuses ou de détournement de celles-ci par des tiers non autorisés;**
- **d'assurer la protection de personnes exposées à des risques particuliers en raison de leurs activités .**

C'est ainsi qu'a été autorisée la protection par un système d'empreintes digitales avec stockage sur le lecteur-comparaison ou sur un serveur :

- d'une zone spécifique à l'intérieur d'une installation nucléaire de base ;
- de certains sites classés SEVESO II, pour un large périmètre ou seulement pour des zones sensibles, compte tenu de la nature des produits manipulés et de la réglementation applicable en l'espèce (Plan d'Opération Interne imposé par arrêté préfectoral par exemple) ;
- d'une cellule de production des vaccins où se déroulent des cultures bactériennes ;
- d'un bloc opératoire dans un CHU confronté à des problèmes spécifiques d'intrusion liés au voisinage ;
- de l'utilisation d'un matériel dangereux, tels que des chariots élévateurs.

[7] La zone doit être clairement et précisément délimitée, rendue « étanche » par toutes les techniques en usage en matière de sécurité et être exclusivement réservée aux personnes habilitées à y avoir accès de par leurs fonctions. Il peut s'agir de locaux, ou de matériels. Le dispositif biométrique peut également avoir pour objet de contrôler l'accès à une application informatique : par exemple contrôler l'accès au poste de pilotage des automates d'une installation de production de fermentation bactérienne et permettre une traçabilité des opérations effectuées.

2. La protection des biens et des installations

En ce qui concerne les biens et les installations, ce qui est en jeu, c'est le dommage grave et irréversible qui peut leur être porté, indépendamment de la valeur du bien lui-même (sauf cas exceptionnels) et sous réserve que cela dépasse l'intérêt strict de l'organisme.

La Commission a autorisé la mise en œuvre de tels systèmes **lorsque le fonctionnement de services essentiels à la collectivité peut être menacé par l'intrusion de personnes non autorisées dans telle ou telle partie d'un organisme :**

Il s'agit par exemple du contrôle d'accès :

- à certaines zones d'une entreprise travaillant pour la Défense nationale ;
- au centre de contrôle et de sécurité d'une grande entreprise de messageries ;
- aux zones sensibles d'un centre départemental d'incendie et de secours ;
- aux zones sensibles d'une imprimerie fiduciaire soumise à des règles de sécurité nationales et internationales[8].

3. La protection des informations

Il s'agit des informations ou des données devant faire l'objet d'une protection particulière en raison des conséquences que leur divulgation, leur détournement à d'autres fins ou leur destruction auraient pour les personnes concernées par l'activité de l'entreprise, de l'institution ou de l'organisme.

C'est le cas, par exemple, du « secret défense », d'un secret industriel, d'un secret professionnel, ou de données dont la divulgation porterait un préjudice grave et irréversible aux tiers concernés.

C'est ainsi qu'ont été autorisés des contrôles d'accès biométrique avec base de données d'empreintes digitales :

- aux locaux d'une entreprise classée ICPE[9] développant des procédés et matériels sensibles faisant l'objet de restrictions à l'exportation ;
- à la salle sécurisée contenant des informations de clients de niveau « confidentiel défense » d'une entreprise spécialisée dans les systèmes d'information de grandes entités et dans leurs problématiques de sécurité ;
- aux locaux d'un cabinet-conseil en matière de propriété intellectuelle et industrielle, habilité à gérer des dossiers sensibles (confidentiel ou secret défense, etc.) ;
- au bâtiment d'un service de l'Education nationale contenant les sujets d'examens et concours[10].

[8] En revanche, la CNIL n'a pas accepté, par exemple, le recours à des dispositifs reposant sur l'enregistrement des empreintes digitales dans une base de données :

- pour la protection de la salle informatique « classique » d'une collectivité locale ;
- pour l'accès à des zones de fabrication de vêtements destinés à certains services de l'Etat.

[9] Installation Classée pour la Protection de l'Environnement

B. Deuxième question : la proportionnalité du dispositif de reconnaissance par empreinte digitale avec stockage dans une base de données en fonction de la nécessité de la protection des données et de la finalité recherchée

Il importe de savoir **si le système proposé est bien adapté ou est le mieux adapté à la finalité préalablement définie** eu égard aux risques qu'il comporte en matière de protection des données à caractère personnel.

- N'y a-t-il pas d'autres données non biométriques et utilisables avec un niveau équivalent, ou suffisant, de sécurité par rapport à l'enjeu ?

- Qu'est-ce qui justifie, en l'espèce, ou rend même indispensable le recours à une base centrale plutôt qu'à une carte à puce individuelle stockant le gabarit biométrique de l'utilisateur ?

Il faut rappeler que l'objectif poursuivi par le recours au stockage des empreintes digitales dans une base de données peut presque toujours être atteint par le truchement du système de stockage individualisé sur carte à puce : en l'état actuel de la technique et des informations disponibles, **du point de vue de la sécurisation des accès**, **le dispositif avec base centrale et le dispositif avec support individuel se valent**[11].

Il est vrai qu'une base centrale présente un avantage lorsque l'accès doit être assuré à tout moment et sans délai, pour faire face à des situations d'urgence nécessitant une intervention aussi rapide que possible. C'est le cas par exemple du contrôle de l'accès à des zones de stockage d'un site classé « SEVESO » dans lesquelles sont entreposées des substances toxiques.

Enfin, dans la mesure où il s'agit de situations où l'enjeu de sécurité est majeur, la pertinence, l'adéquation et le caractère non excessif d'un système avec une base d'empreintes digitales doivent aussi être examinés au regard du nombre des personnes concernées : plus la zone est circonscrite et le nombre des personnes concernées réduit, plus les inconvénients d'une base d'empreintes digitales diminuent.

[10] En revanche, l'enregistrement des empreintes digitales dans une base de données n'a pas été accepté pour le contrôle de l'accès à l'ensemble des locaux d'une société de gestion d'abonnements pour le compte de sociétés de publication de presse périodique, ni pour l'accès à l'ensemble du réseau informatique et des postes de travail fixes et mobiles de la totalité des agents d'un organisme de contrôle des assurances.

[11] A l'exception du ré-enrôlement d'un utilisateur dont on souhaite vérifier que la nouvelle donnée biométrique enregistrée est proche de celle présentée au précédent enrôlement

C. Troisième question : la fiabilité et la sécurité du dispositif de reconnaissance par empreintes digitales avec stockage dans une base de données

Le dispositif doit permettre à la fois une authentification et/ou une identification fiable des personnes et comporter toutes les garanties de sécurité pour éviter la divulgation des données.

1. Sur les caractéristiques du dispositif biométrique

Afin de permettre une bonne évaluation du dispositif, il est nécessaire de bien connaître les caractéristiques techniques, de les préciser à la CNIL et de fournir une documentation détaillée pouvant être transmise par le fabricant ou le distributeur du produit.

Les points sur lesquels la Commission porte tout particulièrement son attention sont les suivants :

- nature du capteur ;
- présence ou non de mesures techniques permettant de lutter contre les attaques par « faux doigt » ;
- algorithme de chiffrement des gabarits utilisé ;
- nombre de points caractéristiques relevés ;
- ports de communication dont est équipé le lecteur biométrique ;
- modalités de stockage des gabarits (base de données dans le lecteur, sur un poste informatique relié au réseau ou dans une carte à puce) ;
- taux de fausse acceptation et de faux rejet du dispositif pour différents paramétrages du système ;
- taux d'échec à l'enrôlement ;
- nombre de lecteurs biométriques et lieu de leur installation dans les locaux ;
- utilisation du dispositif en identification ou en authentification.

Les phases de collecte et d'effacement des données sont des étapes sensibles qui nécessitent une vigilance particulière. C'est pourquoi la Commission vérifie :

- les conditions dans lesquelles sont collectées pour la première fois les données biométriques de la personne qui serviront de référence lors des contrôles futurs (ex : enrôlement par un personnel formé…) ;
- les modalités d'effacement des gabarits quand l'utilisateur cesse d'utiliser le dispositif;

S'agissant de la durée de conservation des données biométriques, elles doivent être effacées lorsque la personne n'est plus habilitée à pénétrer dans la zone dont l'accès est contrôlé ou à accéder à l'application protégée (démission, retraite …).

2. Sur la sécurité du système dans son ensemble

S'agissant de l'environnement dans lequel s'inscrit le dispositif, une attention particulière doit être portée à l'architecture du système d'information, aux mesures de sécurité ainsi qu'aux sauvegardes. Il appartient à l'installateur, à l'administrateur et parfois également à l'usager d'un dispositif biométrique de garantir la sécurité des données, c'est-à-dire d'éviter qu'elles soient détruites, endommagées ou communiquées à un tiers.

Dans ce contexte, la Commission a besoin d'une description du système informatique (système d'exploitation, caractéristiques techniques des postes informatiques …), de connaître la nature du réseau informatique et des dispositifs techniques permettant d'assurer sa sécurité physique et logique.

Les points particulièrement sensibles sont :

- les procédés de protection contre les intrusions extérieures ;
- les autres mesures destinées à assurer la confidentialité des données ;
- la sécurité des lecteurs ou des capteurs biométriques (dans quelles conditions il est possible de les connecter pour récupérer des données)
- les modalités du contrôle d'accès aux applications informatiques ainsi que la gestion des habilitations ;
- le paramétrage des dispositifs et des logiciels de configuration de ceux-ci.

Grâce à ces informations, la Commission peut apprécier si les mesures prises en vue de garantir la sécurité des données sont conformes à l'état de l'art et permettent de circonscrire les risques d'attaques physiques et logiques à l'encontre du système d'information et plus particulièrement du dispositif biométrique.

D. Quatrième question : l'information des personnes concernées

Il s'agit d'une phase essentielle de la mise en œuvre d'un dispositif informatique tant du point de vue de la loi « informatique et libertés » que du Code du travail (dans un environnement où il s'applique).

Il s'agit de faire preuve de transparence vis à vis des personnes concernées qui devront notamment être informées :

- de la finalité du dispositif ;
- des destinataires ou catégories de destinataires des données ;
- des modalités d'exercice de leur droit d'accès et de rectification aux données (il s'agit, par exemple, du droit à accéder à l'historique des passages lorsque le dispositif permet d'en éditer un).

Cette information peut, par exemple, reposer sur une note remise aux personnes concernées dans laquelle les modalités de fonctionnement du dispositif et les raisons de sa mise en œuvre seront présentées et expliquées.

Lorsque les personnes concernées sont des salariés, l'information individuelle doit être associée à la consultation des instances représentatives du personnel. Même si ce dernier point ne résulte pas de la loi « informatique et libertés » mais du Code du travail, le fait d'avoir l'assentiment des instances représentatives est un élément pris en considération par notre Commission dans le cadre de l'examen des demandes d'autorisation.

Aussi est-il recommandé de communiquer à la CNIL le résultat de cette consultation lorsqu'elle a déjà été faite ou d' indiquer sous quel délai elle le sera.

* *

*

C'est à la suite d'un examen attentif de l'ensemble des points énumérés ci-dessus que la CNIL se prononce sur la mise en œuvre des traitements qui lui sont soumis. Dès lors chacun peut noter qu'aucun critère préétabli n'est à lui seul déterminant. Enfin, la Commission se prononce toujours, bien entendu, « *en l'état actuel de la technologie* ».