Avis n° 17 /2008 du 9 avril 2008

Objet : Avis d'initiative relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes (A/2008/017)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la"LVP"), en particulier l'article 29 ;

Vu le rapport du Président, Monsieur DEBEUCKELAERE ;

Émet d'initiative, le 09/04/2008, l'avis suivant :

I. CHAMP D'APPLICATION DE L'AVIS

1. Le présent avis d'initiative porte sur le traitement de données biométriques dans le cadre de l'authentification de personnes.

2. Le présent avis ne porte pas sur l'utilisation de la biométrie afin de procéder au contrôle des frontières ni aux traitements effectués par les services de police et services de sécurité (law enforcement). La Commission reste néanmoins attentive aux développements actuels à cet égard, notamment au niveau européen, mais elle se prononcera en la matière en temps opportun.

3. L'authentification est un processus qui consiste à vérifier l'identité prétendue d'une entité donnée (telle une personne)[1]. L'authentification peut en général être faite de différentes manières :

   - soit par un élément dont on est le seul à connaître, tel un mot de passe ("ce que l'on sait"),
   - soit par le fait qu'on détienne un objet, tel qu'un badge ("ce que l'on détient"),
   - soit par "ce que l'on est", telle l'utilisation d'une caractéristique biométrique.

4. Si l'identification permet de connaître une identité d'une entité, c'est-à-dire de déterminer l'identité d'un individu au sein d'une certaine population[2], l'authentification vise à vérifier cette identité (obtenir l'assurance que l'individu est bien la personne qu'il prétend être).

5. L'authentification est généralement utilisée pour octroyer des droits qui sont normalement réservés à un public déterminé (accès à un local, à un système informatique...).

---

[1] Voir les définitions données par l'ISO :

- L'authenticité : "the property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information" (ISO/IEC 13335-1: 2004).

- L'authentification: "Provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication)" (ISO/IEC 18028-4: 2005)

[2] Définition proposée à l'ISO: "Recognizing an entity within some context with unique identity references and additional information that characterizes the entity" (**http://www.jtc1sc27.din.de/sce/SD6**).

6. Dans plusieurs situations, il est utile de vérifier que des individus prétendant être répertoriés sont effectivement bien ceux qu'ils prétendent être : c'est le cas notamment lors du contrôle et de la gestion de l'accès à des espaces réservés (entrée d'un bâtiment, zones aéroportuaires, entrepôts de marchandises, ...), du contrôle d'accès à des services réservés (accès à un système de PC banking) ou lors du contrôle du temps de travail.

7. La Commission émet cet avis en tenant compte des connaissances actuelles de la technologie biométrique et se réserve bien entendu la possibilité de se repositionner ultérieurement en la matière, compte tenu de l'évolution des technologies et de son expérience en la matière.

II. LA BIOMETRIE : EXPLICATIONS GENERALES

A. Définition et intérêt de la biométrie

8. La biométrie est la science des variations biologiques dont le but est de déterminer ou de vérifier l'identité d'un individu à l'aide de procédés s'appuyant sur des caractéristiques humaines distinctes et individuelles[3].

9. Certaines caractéristiques sont en effet à ce point propres à chaque individu, voire uniques, qu'elles peuvent le distinguer des autres personnes parmi une certaine population. Les caractéristiques biométriques ont la particularité d'être des "caractéristiques physiques uniques et particulières d'une personne pouvant – du moins théoriquement – lui être attribuées en tout lieu et en tout temps avec une certitude quasi absolue"[4].

10. Les caractéristiques peuvent être de différents ordres et notamment physiques, comportementales ou génétiques, tels que l'ADN, la rétine, l'iris, les empreintes digitales, la géométrie du contour de la main, la reconnaissance faciale, la voix, l'écriture manuscrite, la manière de taper sur un clavier d'ordinateur ou de se déplacer, etc.

---

[3] Voir par exemple, Corien Prins, "Biometric technology law. Making our body identify for us : legal implications of biometric technologies", *Computer Law & Security Report*, Vol. 14, n°3, 1998, p. 159 et s ; Daniel Guinier, "Biométrie : classification au vu des nouveaux motifs", *Expertises*, Février 2005, p. 62 et s. ; Le "Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques" élaboré par le Conseil de l'Europe en février 2005 ; Ann Cavoukian et Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy,* Information and Privacy Commissioner/Ontario, Mars 2007; Gérard Dubey, "L'identité à l'épreuve de la biométrie", in *La sécurité aujourd'hui dans la société de l'information*, Contributions réunies et coordonnées par Stéphanie Lacour, L'harmattan, Paris, 2007, p. 87 et s.

[4] Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données élaboré par PRIVATIM, les commissaires suisses à la protection des données, octobre 2006, n°3.1.2.

11. Si la biométrie existe depuis longtemps, son utilisation tend à se développer, notamment grâce à l'introduction de nouvelles technologies qui permettent d'automatiser le processus d'analyse et de comparaison des traits des individus. Cette automatisation accélère le traitement et diminue également le risque d'erreur. Par ailleurs, la diminution des coûts relatifs à l'utilisation de ces technologies participe également à son expansion.

12. Les technologies biométriques, parce qu'elles utilisent des caractéristiques intrinsèquement liées à la personne, peuvent améliorer la sécurité et diminuer certains risques de fraudes. En effet, l'utilisation de la biométrie permet, en comparaison avec la seule utilisation des autres moyens d'authentification (l'usage de mots de passe ou de badges), de renforcer la preuve, c'est-à-dire le lien, entre la personne physique et son identité. Cela justifie le fait que l'on considère aujourd'hui la biométrie comme un moyen d'authentification fort[5].

B. Mode de fonctionnement

1) Deux phases de collecte et deux fonctions des systèmes biométriques

13. Le mode de fonctionnement d'un système biométrique est scindé en deux phases de collecte d'information et il existe deux manières de comparer les informations collectées (les deux fonctions des systèmes biométriques) :

14. La première phase de collecte, dite de l'inscription (ou de l'enrôlement), est le moment où une caractéristique biométrique d'un individu est collectée par un capteur et enregistrée sur un support de stockage (soit un support individuel telle qu'une carte à puce, soit dans une base de données). Cet échantillon de référence sera, en fonction du système choisi, soit une image (les "données brutes") soit des données pertinentes extraites de cette image, appelées le gabarit (ou "template" et qui consiste en une suite de chiffres qui caractérisent l'élément biométrique). Le stockage de l'image nécessite plus d'espace mémoire que le stockage du gabarit.

[5] Selon la définition de l'authentification: "[...] Strong authentification is either based on strong mecanisms (e.g. biometrics) or makes use of at least two (...) factors (so-called multi-factor authentification)" (ISO/IEC 18028-4: 2005).

15. La seconde phase de collecte se déroule lorsqu'une personne se présente devant le système biométrique qui doit l'authentifier. On effectue alors une deuxième collecte d'échantillon biométrique (par exemple, la personne passe son doigt devant le capteur) et l'information qui en découle (l'image ou le gabarit) est alors comparée avec l'échantillon de référence afin de vérifier si elles correspondent. Lorsque l'information collectée lors de la deuxième collecte et l'échantillon de référence correspondent (appariement positif), le système considère que la personne qui se présente est bien celle qui a été enregistrée préalablement lors de la phase de l'inscription.

16. Il existe deux manières de comparer les informations obtenues lors des deux phases de collecte et elles constituent les deux principales fonctions de la biométrie : la fonction d'identification et la fonction de vérification. Ces fonctions peuvent toute deux être utilisées dans le cadre de l'authentification (voir toutefois le paragraphe 59 de cet avis où la Commission recommande l'utilisation de la fonction de vérification dans le cadre de l'authentification de personnes).

17. La fonction d'identification consiste à comparer l'information présentée lors de la seconde phase avec toutes les informations biométriques disponibles dans le système biométrique et qui sont nécessairement contenues dans une base de données ("one-to-many comparison"). Cette fonction permettra en premier lieu d'identifier l'utilisateur parmi l'ensemble des personnes enregistrées, et peut servir dans un second temps à l'authentifier.

18. La fonction de vérification consiste à comparer l'information présentée lors de la seconde phase avec l'information préalablement enrôlée appartenant à une seule personne[6] ("one-to-one comparison"). Cette fonction est particulièrement adaptée aux situations où la personne souhaite se faire authentifier et est donc prête à communiquer volontairement un élément permettant de l'identifier (comme une carte à puce ou un badge) et sur la base duquel l'échantillon biométrique de référence sera déterminé et ensuite comparé avec l'échantillon de la nouvelle collecte.

[6]Définition de la fonction de vérification proposée à l'ISO: "Biometric product function that performs a one-to-one comparison" (**http://www.jtc1sc27.din.de/sce/SD6**). Nous soulignons le fait que dans le cadre particulier de la biométrie, la définition de la vérification a un sens spécifique qui se distingue totalement de la notion d'authentification. En effet, l'authentification (c'est-à-dire le processus de vérification d'identité) peut se réaliser par les deux fonctions biométriques, c'est-à-dire soit par la fonction d'identification soit par la fonction de vérification (voir toutefois le paragraphe 59 de cet avis où la Commission recommande l'utilisation de la fonction de vérification dans le cadre de l'authentification).

2) Les systèmes biométriques sont fiables mais il existe toujours un certain taux d'erreur

19. Il faut souligner que l'image ou le gabarit des données de référence ne seront que très rarement identiques aux informations présentées ultérieurement. Il suffit de présenter la caractéristique biométrique dans des circonstances quelque peu différentes pour que l'information extraite soit également différente (par exemple, la luminosité influence les données relatives au visage, la température influence les données relatives à la main, la pression qu'on exerce avec son doigt influence également les données relatives à l'empreinte digitale, etc.). C'est la raison pour laquelle la comparaison s'effectue toujours sur la base de calculs de probabilité.

20. Par conséquent, tout système biométrique implique nécessairement un certain taux d'erreur. Il s'agit du "taux de faux rejets" (False Rejection Rate), qui implique le rejet d'un certain pourcentage de personnes qui auraient dû être acceptées (rejet "d'utilisateurs légitimes"), et du "taux de fausses acceptations" (False Acceptation Rate), qui implique l'acceptation d'un certain pourcentage de personnes qui n'auraient pas dû l'être (acceptation "d'imposteurs").

21. Le choix de la technique utilisée influence la fiabilité du système. Ainsi, l'utilisation de l'empreinte digitale à l'heure actuelle est plus fiable que celle de la reconnaissance du visage. Il est également possible de combiner l'utilisation de différentes caractéristiques biométriques afin d'améliorer la fiabilité du système.

22. Par ailleurs, l'échelle d'acceptation des erreurs est modulable et sera adaptée au cas pas cas par le fournisseur de solutions biométriques, selon les finalités de l'utilisation prévue et selon les besoins du responsable de traitement. Pour être rapide à l'utilisation et éviter qu'une personne ne doive présenter plusieurs fois d'affilée sa caractéristique biométrique ou procéder à nouveau à l'enrôlement, il faut mettre en place un système ayant un taux de faux rejets le plus bas possible. En effet, si on utilise un système avec un taux de faux rejets trop élevé, on exige une très forte similitude entre l'information biométrique présentée et l'échantillon de référence. Ce système a pour conséquence d'écarter plus facilement un utilisateur qui aurait dû être accepté ("utilisateur légitime") mais qui n'aurait pas présenté sa caractéristique biométrique d'une manière suffisamment similaire que lors de la collecte de sa donnée biométrique de référence. Cependant, diminuer le taux de faux rejets augmente nécessairement celui des fausses acceptations, ce qui diminue le niveau de sécurité du système dès lors que le risque d'accepter des personnes qui n'auraient pas dû l'être (des "imposteurs") augmente. Le juste équilibre à trouver sera normalement discuté entre le fournisseur de solutions biométriques et le responsable de traitement.

23. Il faut souligner le fait que les systèmes biométriques sont généralement des systèmes performants. Toutefois, on ne peut oublier l'existence d'un certain risque d'erreur inhérent au système et on ne peut donc pas considérer ces systèmes comme étant infaillibles.

24. En outre, les systèmes biométriques ne sont pas toujours utilisables par l'ensemble des individus. Ainsi par exemple, 4% de la population ne dispose pas d'empreintes digitales suffisamment distinctes pour une reconnaissance automatisée par un système biométrique[7]. Certaines personnes souffrant d'un handicap pourraient également se voir empêchée de pouvoir utiliser un système biométrique. Il faudrait éviter que la biométrie ne soit pas source de discrimination en marginalisant les personnes qui ne peuvent utiliser ces systèmes[8].

III. APPLICABILITE DE LA LOI RELATIVE AUX TRAITEMENTS DE DONNEES (LVP)

A. La donnée biométrique est une donnée personnelle

25. Conformément à l'article 1 §1 de la LVP, il faut entendre par "données à caractère personnel" toute information concernant une personne physique identifiée ou identifiable, (...); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

26. La donnée biométrique, qu'elle soit une image ou des données extraites de cette image (le gabarit), est une caractéristique physique d'un individu. Cette donnée peut révéler en soi une information relative à une personne physique, et des informations personnelles additionnelles pourront également résulter des circonstances de la collecte (par exemple, le traitement des données relatives au moment et au lieu de la collecte permettront d'avoir connaissance de la présence d'une personne à un lieu et à un moment donné).

---

[7] Voir le rapport "Identity Management for eGovernment, Study and assessment of Biometric techniques for eGovernment application", *op. cit.*, p. 15. D'autres sources parlent de 2%, voir le "Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données" élaboré par PRIVATIM, *op. cit.*

[8] Dr Jean-Philippe Walter (Préposé fédéral suppléant à la protection des données en Suisse), "Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé", 26e Conférence internationale des Commissaires à la protection des données et à la vie privée Wroclaw, 14 – 16 septembre 2004.

27. Dès lors que le lien entre la donnée biométrique et une personne physique peut être réalisé avec des moyens raisonnables, que ce soit par le responsable de traitement ou toute autre personne, il s'agit d'une donnée à caractère personnel.

28. Par conséquent, la Commission considère en principe[9] les données biométriques comme étant des données à caractère personnel.

B. La donnée biométrique peut être une donnée sensible[10]

29. Certaines données biométriques peuvent révéler des informations sur l'état de santé ou l'origine raciale d'un individu[11].

30. Lorsque les données biométriques sont utilisées pour en déduire une information relative, par exemple à l'état de santé ou l'origine raciale, ces données doivent être considérées comme des données sensibles.

31. Le fait de ne traiter qu'une partie des données extraites de l'image (le gabarit) et non l'image, peut aider à éviter le traitement de données sensibles[12].

---

[9] Dans de rare cas, une donnée biométrique ne sera pas une donnée personnelle. Il s'agit par exemple d'une donnée biométrique dont le lien ne peut être réalisé avec une personne concernée avec des moyens raisonnables. Cela peut dépendre de la qualité de la donnée collectée (empreinte digitale partielle ne pouvant être exploitable) ou des circonstances de la collecte d'une donnée (circonstances de lieu et de moment qui ne permettent pas de cibler un groupe suffisamment déterminé dont la personne concernée ferait partie). Il est néanmoins essentiel de souligner qu'une donnée biométrique qui n'est pas une donnée personnelle à un moment déterminé peut le devenir par la suite (nouvelles circonstances de fait ou nouvelles technologies qui permettront de réaliser plus facilement une identification).

[10] Dans le cadre de la protection de la vie privée, les données sensibles sont les données visées par les articles 6, 7 et 8 de la LVP.

[11] Ainsi les données relatives à l'ADN mais également d'autres types de données biométriques comme l'empreinte digitale ou la géométrie du contour de la main (par exemple, l'utilisation d'un tel système pourrait révéler un problème de santé qui impliquerait des variations physiques courantes de la main et qui rendraient difficile l'utilisation du système biométrique pour cette personne).

[12] Ainsi, les données qui peuvent révéler l'état de santé ou l'origine raciale de la personne concernée peuvent être présentes sur l'image, mais peut-être plus dans les données extraites de cette image (le gabarit ou "template"). Voir également à cet égard le point 74 du "Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques", *op. cit.*

C. L'utilisation de la Biométrique implique un traitement de données

32. La LVP définit le "traitement" comme étant toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel[13].

33. L'utilisation de systèmes biométriques suppose la collecte, l'enregistrement, le stockage de données personnelles, biométriques ou non, et cela à l'aide de moyens automatisés.

34. Par conséquent, l'utilisation de ces systèmes implique un traitement de données.

IV. APPLICATION DES PRINCIPES DE LA LOI RELATIVE AUX TRAITEMENTS DE DONNEES (LVP)

A. La légitimité et la proportionnalité[14]

1) Le principe de légitimité

35. Toute donnée personnelle doit être traitée pour des finalités déterminées, explicites et légitimes, et ne doit pas être traitée ultérieurement de manière incompatible avec ces finalités.

36. Pour être légitime, toute finalité doit notamment répondre à l'une des conditions de l'article 5 de la LVP.

37. Le traitement des données biométriques à des fins d'authentification de personnes peut en principe intervenir lorsque les personnes concernées ont donné leur consentement[15]. Le consentement permet certainement que ces nouvelles technologies rencontrent les acceptations sociales des utilisateurs.

---

[13] Article 1 §2 de la LVP.

[14] Articles 4 et 5 de la LVP.

[15] Article 5.a) de la LVP.

38. La Commission souligne que, pour être valablement octroyé, le consentement doit être libre, spécifique et informé[16].

39. Il faut attirer l'attention sur le fait que l'obtention du consentement ne pourra pas rendre légal un traitement disproportionné (voir le paragraphe 41 ci-dessous). C'est par exemple le cas lorsque le traitement biométrique n'est pas strictement nécessaire pour permettre de réaliser le résultat escompté.

40. Par ailleurs, le traitement peut également être autorisé si celui-ci est prévu par une loi[17] ou si le responsable de traitement peut faire valoir un intérêt légitime prépondérant prévalant l'intérêt ou les droits et libertés fondamentaux de la personne concernée[18].

2) Le principe de proportionnalité : mise en balance des intérêts en présence

41. Une finalité légitime implique également que le traitement soit proportionné : l'intérêt général ou les intérêts légitimes du responsable de traitement doivent être mis en balance avec le droit à la protection de la vie privée des personnes enregistrées.

a. Intérêt du responsable de traitement

42. L'utilisation de la biométrie peut comporter certains avantages pour le responsable de traitement dès lors que le processus d'authentification est automatisé, plus sûr que d'autres systèmes classiques et parfois moins cher.

43. Outre les avantages relatifs aux coûts et à la facilité du système, l'avantage spécifique de l'utilisation d'un système biométrique est certainement l'amélioration de la sécurité dans de nombreux cas. En effet, le système biométrique est considéré comme un moyen d'authentification fort[19].

44. Perfectionner la sécurité peut améliorer la protection des personnes, des biens ou l'efficacité de la lutte contre la fraude. La biométrie permet en effet de lutter contre la fraude (par exemple,

---

[16] Voir la définition du consentement à l'article 1 §8 de la LVP.

[17] Article 5.c) de la LVP.

[18] Article 5.f) de la LVP.

[19] Selon la définition de l'authentification: "[…] Strong authentification is either based on strong mecanisms (e.g. biometrics) or makes use of at least two (…) factors (so-called multi-factor authentification)" (ISO/IEC 18028-4: 2005). Les facteurs visés sont l'authentification par la connaissance, par la possession ou par les caractéristiques personnelles.

l'accès illicite à des services) dès lors qu'elle peut empêcher que le moyen d'authentification (tel un mot de passe ou un badge) soit délibérément passé à un tiers ou usurpé. Par exemple, lorsque la gestion des horaires d'employés ne se base que sur l'utilisation d'un badge, il est toujours possible que des personnes fraudent en donnant leur badge à des collègues afin de prétendre leur présence ("fraude à la pointeuse"), ce qui n'est plus possible lorsqu'on insère un moyen d'authentification biométrique.

b. Intérêt des individus quant au respect de leur vie privée

45. L'utilisation de données biométriques suscite des considérations particulières relatives à la protection des données. En effet, les données biométriques sont une catégorie spécifique de données, dans la mesure où elles émanent du corps humain et qu'elles sont dans les situations normales inaltérables à vie[20]. Par ailleurs, l'intégrité du corps humain et la manière dont il est utilisé constituent un aspect de la dignité humaine[21].

46. En outre, une donnée biométrique est un identifiant[22] qui permet d'identifier de manière unique un individu dans un certain contexte[23].

[20] Voir le point 107-1 du "Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques", *op. cit*. Ce rapport particulier avec le corps permet de renforcer le lien entre la donnée et la personne ("linkability") et implique dès lors également davantage de risques en termes de possibilité de profilages, d'interconnections d'informations par le biais de cet identifiant et par conséquent d'atteinte à la vie privée (voir le rapport "Identity Management for eGovernment, Study and assessment of Biometric techniques for eGovernment application", Instituut voor Breedband Technologie (IBBT), Juin 2007, n°3.3.2, p. 13).

[21] Ainsi la dignité humaine pourrait être violée notamment "lorsque des procédés biométriques –parfois combinés avec d'autres applications techniques- conduisent à considérer l'être humain exclusivement comme un objet ou un numéro, en d'autres termes, comme une marchandise", voir le Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données élaboré par PRIVATIM, *op. cit*.

[22] Identity Management of eGovernment, Deliverable 4.1, "Study and assessment of biometric techniques for eGovernment applications, Het Interdisciplinair instituut voor Breedband Technologie (IBBT), projet IDEM, , June 2007, p. 13.

[23] Le Comité consultatif national français d'éthique pour les sciences de la vie et de la santé a également souligné les risques particuliers des techniques d'identification des personnes sur la base de leurs caractéristiques biologiques et notamment celui du glissement du contrôle de l'identité à celui des conduites et de la personnalité, de l'interconnexion des données et de l'obtention de ces dernières à l'insu des personnes concernées.

47. Il existe également des risques liés à l'utilisation de la biométrie, comme le vol d'identité. Le vol d'identité est d'autant plus un risque important que l'objectif de la biométrie est de fournir une authentification plus forte (c'est-à-dire, un lien plus fort entre l'utilisateur et son identité)[24]. De plus, les conséquences du vol d'identité peuvent être souvent sous-estimées et difficiles à prouver[25]. Par ailleurs, l'utilisation de la biométrie peut impliquer de nouveaux risques physiques pour les utilisateurs. Ainsi, en ce qui concerne le vol de voiture de luxe, il a été observé que des voleurs n'ont pas hésité à faire usage de violence physique pour contourner la mesure de sécurité biométrique qui avait été utilisée pour protéger le véhicule[26].

48. Il faut souligner que les risques en termes d'atteinte à la vie privée peuvent varier en fonction du type de données biométrique utilisé. Par exemple, les systèmes biométriques se référant à des caractéristiques physiques qui ne laissent pas de traces créent moins de risques pour la protection de la vie privée que les systèmes utilisant des caractéristiques physiques qui laissent des traces[27].

49. "Les caractéristiques biométriques qui laissent des traces" concernent des particularités physiques biométriques qui se déposent là où la personne concernée a été physiquement présente et qui donc "laissent des traces" (ainsi les empreintes digitales déposées sur les objets ou des cheveux tombés contenant l'information ADN). D'autres caractéristiques biométriques ne laissent pas de traces (tels que le réseau veineux du doigt ou de la main, le contour de la main, l'iris ou la rétine).

50. La Commission souligne que les systèmes utilisant des caractéristiques biométriques ne laissant pas de traces créent moins de risques pour la protection des libertés et des droits fondamentaux des personnes. En effet, les systèmes biométriques "avec traces" présentent davantage de risque que les données soient réutilisées pour d'autres finalités que celles initialement prévues.

---

[24] Identity Management of eGovernment, Deliverable 4.1, "Study and assessment of biometric techniques for eGovernment applications, Het Interdisciplinair instituut voor Breedband Technologie (IBBT), projet IDEM, June 2007, p. 14.

[25] *Ibidem*.

[26] Le voleur aurait coupé le doigt du propriétaire du véhicule, voir le site web de la BBC news http://news.bbc.co.uk , information rapportée le 31 mars 2005.

[27] Voir le document de travail de la biométrie du Groupe de l'article 29, *op. cit.*, pp. 6-7.

51. D'une façon plus générale, la Commission souhaite attirer l'attention sur le choix de société qu'implique une généralisation de l'utilisation de la biométrie. L'expansion des systèmes biométriques pourrait entraîner un risque important de désensibilisation du public quant à l'utilisation toujours croissante de ses données et aux conséquences que ces traitements pourraient avoir sur sa vie quotidienne[28]. Le groupe de l'article 29[29] souligne par exemple que l'utilisation de la biométrie dans les bibliothèques scolaires implique le risque pour les enfants d'être moins conscients des risques qui sont liés à la protection des données ce qui peut avoir des conséquences pour eux plus tard dans la vie[30].

c. Conséquence de l'application du principe de proportionnalité pour le responsable de traitement:

- Appréciation stricte du principe de proportionnalité et motivation de l'utilisation

52. La Commission estime que l'appréciation de la proportionnalité des traitements de données biométriques doit être réalisée par les responsables de traitement de manière stricte et cela en prenant en compte l'intérêt à long terme des personnes concernées.

53. Les responsables de traitement doivent réaliser une mise en balance concrète et consciencieuse des intérêts en présence et les raisons justifiant leur intention d'utiliser un système biométrique doivent être clairement définies, motivées et portées à la connaissance des personnes concernées.

- Vérification de la réelle nécessité de traiter des données personnelles

54. La première question que doivent se poser les responsables de traitement est la réelle nécessité de vérifier l'identité des personnes concernées (authentification). La restriction d'accès à des lieux ou à des services n'implique pas toujours qu'un traitement de données personnelles soit nécessaire. Par exemple, les consommateurs devraient avoir la possibilité de consommer ou de souscrire à des services de manière anonyme.

---

[28] Voir le document de travail de la biométrie du Groupe de l'article 29, GT80, adopté le 1er août 2003, pp. 2-3.

[29] Le groupe de l'article 29 regroupe notamment des représentants de l'ensemble des autorités européennes nationales de protection des données.

[30] Voir le document de travail de la biométrie du Groupe de l'article 29, GT80, adopté le 1er août 2003, p. 3.

- Opter pour un système biométrique respectueux de la vie privée et comparaison des systèmes de traitement de données disponibles sur le marché

55. Lorsque le responsable de traitement désirer utiliser un système biométrique, il convient d'opter pour le système le plus respectueux de la vie privée et donc proportionné.

56. Sous certaines conditions, le choix d'un système biométrique peut être considéré en soi comme étant proportionné. Lorsque les conditions ne sont pas remplies, le responsable de traitement devra réaliser une analyse préalable afin de comparer le système biométrique qu'il envisage d'utiliser avec les autres systèmes de traitement de données (non-biométriques) existants sur le marché.

- *Un système biométrique en soi proportionné*

57. La Commission considère le choix d'un système biométrique comme étant en soi proportionné lorsque le responsable de traitement :
    1) est face à une situation où un traitement de données personnelles est nécessaire ou proportionné
    2) utilise un système biométrique se référant à des caractéristiques physiques qui ne laissent pas de traces (voir les paragraphes 48-50 de cet avis),
    3) Respecte les recommandations suivantes :

➲ **De ne pas utiliser des systèmes biométriques stockant les données biométriques de référence dans une base de données**

58. En effet, lorsqu'on utilise un système biométrique à des fins d'authentification de personnes, il n'est pas nécessaire de rassembler les informations biométriques de référence dans une base de données centrale. Ces informations devraient être préférablement enregistrées sur un support amovible sécurisé[31] (tel qu'une carte à puce) détenu par la personne concernée ou, le cas échéant, dans l'appareil contenant le capteur biométrique (par exemple à l'entrée du bâtiment) qui doit être sécurisé et n'être accessible que localement (sans possibilité de connexion avec d'autres systèmes informatiques).

[31] Voir le paragraphe 88 de ce document pour une information sur les mesures de sécurité du support.

59. Il convient dès lors d'utiliser la fonction de vérification du système biométrique (comparaison "one-to-one", voir aux paragraphes 17 et 18 de cet avis), et non la fonction d'identification (comparaison "one-to-many") qui implique nécessairement le recours à l'usage d'une base de données.

60. Le stockage centralisé de données biométriques accroît le risque de réutilisation des données pour des finalités ultérieures incompatibles ainsi que le risque que les données soient utilisées comme une clé pour interconnecter différentes bases de données[32].

61. Le fait que le stockage dans une base de données rende le système biométrique plus convivial (cela permet en effet de s'authentifier sans avoir besoin d'avoir avec soi un support amovible supplémentaire, telle qu'une carte à puce) ne permet pas de justifier les risques additionnels porté à la protection des données résultant du stockage dans une base de données.

62. Stocker les données sur un support amovible sécurisé détenu par la personne concernée permet de plus à la personne concernée de garder un contrôle sur ses données biométriques.

➲ **De ne pas stocker les données brutes biométriques (les images) mais les gabarits**

63. Il n'est pas nécessaire de stocker les données brutes biométriques, par exemple l'image de l'empreinte digitale. Seul le gabarit (ou "template"), c'est-à-dire les données pertinentes extraites des données brutes, devrait être conservé.

64. L'enregistrement de l'image crée davantage de risques en termes de recoupage d'informations et d'interconnexions de bases de données.

➲ **De ne pas utiliser des technologies qui permettent de collecter et/ou de traiter des données biométriques à l'insu de la personne concernée.**

[32] Voir le document de travail de la biométrie du Groupe de l'article 29, *op. cit.*, p. 8 ; ainsi que le rapport "Identity Management for eGovernment, Study and assessment of Biometric techniques for eGovernment application", *op. cit.*, n°3.3.4, p. 14.

65. Les technologies biométriques doivent être transparentes pour les personnes concernées (voir ci-dessous au point B, paragraphe 78) et il convient de ne pas collecter ou traiter des données biométriques à l'insu des personnes concernées. Certains systèmes biométriques, tels que la reconnaissance faciale à distance, la collecte d'empreintes digitales ou l'enregistrement de la voix, présentent davantage de risques à cet égard[33].

➲ D'utiliser un système biométrique sécurisé

66. Le système biométrique doit également être sélectionné en fonction des mesures de sécurité qui y sont apportées afin de protéger les données biométriques (voir ci-dessous au point D, paragraphe 84)

- *Nécessité de comparer le système biométrique envisagé avec les autres systèmes de traitement de données (non-biométriques) existants sur le marché et respect des recommandations*

67. A l'inverse, lorsque le responsable de traitement désire utiliser un système se référant à des caractéristiques physiques qui laisse des traces, il faudra qu'il réalise une analyse préalable afin de comparer son système biométrique avec les autres systèmes de traitement de données existants sur le marché.

68. Il devra dès lors faire une balance concrète des différents systèmes de traitement qui sont à sa disposition afin d'obtenir le résultat désiré et privilégier ceux qui sont plus respectueux de la vie privée et généralement accepté par la société civile. Le responsable de traitement doit donc réaliser une comparaison des différents systèmes d'authentification et vérifier si le même résultat ne pourrait être obtenu avec un système moins intrusif pour la vie privée, telle que la reconnaissance visuelle (comparaison avec la photo d'une carte ou d'un badge).

69. La biométrie est un moyen d'authentification fort[34] et il devrait être réservé aux situations nécessitant un tel niveau de sécurité.

---

[33] Voir le document de travail de la biométrie du Groupe de l'article 29, *op. cit.*, p. 9.

[34] Selon la définition de l'authentification: "[…] "Strong authentification is either based on strong mecanisms (e.g. biometrics) or makes use of at least two (…) factors (so-called multi-factor authentification)". Les facteurs visés sont l'authentification par la connaissance, par la possession ou par les caractéristiques personnelles (ISO/IEC 18028-4: 2005).

70. L'on peut par exemple mettre en doute la nécessité d'utilisation de système biométrique de manière généralisée dans le cadre scolaire. Ce n'est que lorsque la situation particulière à l'établissement justifie un contrôle de haut niveau que la mesure pourrait être considérée comme proportionnée.

71. Il en est de même pour la gestion des horaires des employés. Si l'avantage particulier de la biométrie à cet égard est la lutte contre la fraude, les responsables de traitement devraient faire une analyse préalable pour évaluer la nature et l'importance du risque de fraude particulier à l'établissement au regard de l'impact des mesures biométriques envisagées sur les personnes concernées. Le nombre d'employés de l'entreprise visée doit bien entendu être également pris en considération car un nombre restreint d'employés limite naturellement le risque de fraude.

72. Les systèmes biométriques ne devraient pas être utilisés seulement parce qu'ils sont pratiques, mais parce qu'ils constituent le seul moyen pour permettre de réaliser la finalité initialement décrite.

73. Par ailleurs, si l'avantage économique peut évidemment être pris en considération dans le cadre de la mise en balance entre la finalité première du besoin d'une authentification forte et le droit à la vie privée des individus, il ne peut justifier à lui seul le recours à des mesures biométriques.

74. Si, à la suite de cette mise en balance concrète des différents systèmes de traitement, le responsable de traitement opte pour un système biométrique, il devra, en tout état de cause, respecter également les recommandations prévues aux paragraphes 58 à 66 de cet avis.

- Limiter l'application du système biométrique aux utilisations nécessaires

75. Si le responsable de traitement estime que l'authentification doit nécessairement être mise en place par un système biométrique, il convient en premier lieu de limiter son utilisation aux espaces/services justifiant ces mesures particulières. Par exemple, pour ce qui est du contrôle d'accès, un site pourrait contenir certains espaces de libre accès et d'autres justifiant l'utilisation de la biométrie (une salle ou un bâtiment contenant des objets de valeur, des informations particulièrement confidentielles à protéger, un espace informatique contenant les données sensibles etc.). L'accès géré par des systèmes biométriques pourrait être limité à ces derniers espaces et les données biométriques traitées pourraient être limitées à celles relatives aux personnes en droit d'y accéder.

76. Par ailleurs, pour limiter l'accès à un lieu à certain groupe d'individus, il n'est pas forcément toujours nécessaire de traiter des données personnelles directement identifiantes (tel que le nom) des individus disposant du droit d'accès. Ainsi tant qu'une personne est titulaire du droit d'entrer et que la biométrie permet de le vérifier, il n'est pas nécessaire de lier l'information biométrique à des données additionnelles identifiantes.

- Lorsque l'authentification peut être faite sans identification, ne pas combiner le traitement de données biométriques avec d'autres données identifiantes

77. Il est parfois possible de gérer une authentification sans devoir nécessairement connaître l'identité des personnes concernées lors de chaque utilisation. Par exemple, on peut imaginer que la gestion de l'accès à un lieu soit réservée à un groupe d'individus. Pour éviter que les tiers aient accès, il n'est pas nécessaire de connaître l'identité des individus appartenant au groupe lors de chaque accès. Ainsi, tant qu'une personne fait partie du groupe, et dispose donc d'une donnée biométrique appartenant au groupe (elle dispose par exemple d'une carte à puce du groupe contenant sa donnée biométrique), il n'est pas nécessaire de lier l'information biométrique à des données additionnelles identifiantes (telles que le nom ou le numéro d'employé de la personne concernée). Lorsqu'on désire supprimer l'accès à cette personne, il suffit de récupérer le support amovible contenant son information biométrique.

B. Information des personnes concernées

78. Lors de tout traitement de données, il convient d'informer les personnes quant aux finalités de traitement, à l'identité du responsable de traitement et des destinataires (ou catégories de destinataires) des données ainsi qu'à l'existence du droit d'accès et de rectification de la personne concernée[35].

79. Afin de garantir une transparence vis-à-vis des personnes concernées, il conviendrait également de fournir spontanément de l'information quant au type de système biométrique utilisé (type de stockage notamment), quant à l'existence d'un taux d'erreur de reconnaissance inhérent à tout système biométrique et quant à la procédure à suivre par la personne concernée lors d'une prétendue non reconnaissance par le système.

[35] Article 9 de la LVP.

80. Il faut en effet éviter que les systèmes biométriques soient présentés comme étant des systèmes infaillibles. De même, on ne peut les considérer comme des systèmes de preuve infaillibles. Pour cette raison, il convient de toujours permettre à la personne concernée d'apporter une preuve contraire par toutes les autres voies de droit.

C. Durée de stockage des données

81. Les données biométriques ainsi que les données additionnelles résultant des circonstances de la collecte (voir le paragraphe 26) ne devraient pas être conservées plus longtemps que la durée nécessaire pour la réalisation de la finalité poursuivie[36].

82. Ainsi par exemple, lorsque les données sont utilisées afin de gérer l'accès à un site professionnel, il convient de supprimer les données stockées sur le support amovible dès que l'utilisateur perd son droit d'accès à cet espace.

83. En outre, le capteur biométrique qui permet de collecter la caractéristique biométrique ne devrait pas conserver de copie de la donnée biométrique au-delà de la durée nécessaire pour effectuer la comparaison.

D. Mesures de sécurité

84. Le responsable de traitement et le cas échant, son sous-traitant, doivent prendre des mesures techniques et organisationnelles de sécurité[37] afin de protéger les données biométriques ainsi que les autres données personnelles qu'ils traitent contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

85. Compte tenu de la nature particulière des données biométriques et des risques d'atteintes à la sécurité concernant ces données[38], le niveau de sécurité doit être particulièrement élevé.

---

[36] Article 4, §1, 5° de la LVP.

[37] Article 16 de la LVP.

[38] Pour une description des risques de sécurité, voir le point 2.3.2 du rapport "Identity Management for eGovernment, Study and assessment of Biometric techniques for eGovernment application", *op. cit.*, p. 8.

86. Il convient d'adopter des mesures de sécurité durant toutes les phases de traitement de données biométriques[39].

87. Il est par exemple essentiel d'éviter, lors de la phase de l'inscription, qu'une personne non autorisée se fasse enregistrer comme étant autorisée. Pour cette raison, l'inscription des données biométriques de référence (et la création de support amovible sécurisé) devrait avoir lieu dans un environnement sécurisé et de confiance. Le nombre de personnes habilitées à enregistrer les données de référence devrait être limité.

88. Le support contenant les données biométriques devrait être sécurisé afin d'éviter que les données puissent être utilisées de manière illégitime. Ainsi, on pourrait utiliser des cartes dont le contenu serait protégé par des systèmes de chiffrement, des systèmes de signatures électroniques ou des fonctions de brouillage (par exemple, hashage) afin de protéger l'information[40].

89. Des mesures devraient également être prises afin que la sécurité du capteur permettant la collecte des données biométriques ne puisse être compromise.

90. L'intégrité et la confidentialité des informations échangées entre le support amovible sécurisé et le capteur doit également être adéquatement protégée.

91. Enfin, il est essentiel que le responsable de traitement suive les évolutions technologiques afin d'adapter les mesures de sécurité à celles-ci[41]. Le fait d'opter pour une solution sécuritaire telle qu'un système biométrique implique nécessairement une responsabilité en termes de suivi technologique.

---

[39] Voir la suggestion de certaines mesures de sécurité dans le "Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données" élaboré par PRIVATIM, *op. cit*, n°3.2.

[40] Voir le document de travail de la biométrie du Groupe de l'article 29, *op. cit.*, pp. 10 et 11.

[41] Article 16 de la LVP.

92. Conformément à l'article 15 bis de la LVP, le responsable de traitement pourra être tenu pour responsable des dommages causés par le non-respect des obligations relatives aux mesures de sécurité.

Pour L'Administrateur e.c.,
Le Chef de section OMR

Le Président,

(sé) Patrick Van Wouwe

(sé) Willem Debeuckelaere