N° 465

SÉNAT

SESSION ORDINAIRE DE 2013-2014

Enregistré à la Présidence du Sénat le 16 avril 2014

RAPPORT

FAIT

au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur la proposition de loi de M. Gaëtan GORCE et plusieurs de ses collègues visant à **limiter** *l'***usage** *des* **techniques biométriques**,

Par M. François PILLET,

Sénateur

(1) Cette commission est composée de : M. Jean-Pierre Sueur, *président ;* MM. Jean-Pierre Michel, Patrice Gélard, Mme Catherine Tasca, M. Bernard Saugey, Mme Esther Benbassa, MM. François Pillet, Yves Détraigne, Mme Éliane Assassi, M. Nicolas Alfonsi, Mlle Sophie Joissains, *vice-présidents ;* Mme Nicole Bonnefoy, MM. Christian Cointat, Christophe-André Frassa, Mme Virginie Klès, *secrétaires ;* MM. Alain Anziani, Philippe Bas, Christophe Béchu, François-Noël Buffet, Gérard Collomb, Pierre-Yves Collombat, Jean-Patrick Courtois, Mme Cécile Cukierman, MM. Michel Delebarre, Félix Desplan, Christian Favier, René Garrec, Gaëtan Gorce, Mme Jacqueline Gourault, MM. François Grosdidier, Jean-Jacques Hyest, Philippe Kaltenbach, Jean-René Lecerf, Jean-Yves Leconte, Antoine Lefèvre, Mme Hélène Lipietz, MM. Roger Madec, Jean Louis Masson, Michel Mercier, Jacques Mézard, Thani Mohamed Soilihi, Hugues Portelli, André Reichardt, Alain Richard, Simon Sutour, Mme Catherine Troendlé, MM. René Vandierendonck, Jean-Pierre Vial, François Zocchetto.

Voir le(s) numéro(s) :

Sénat : **361** et **466** (2013-2014)

S O M M A I R E

Pages

CONCLUSIONS DE LA COMMISSION DES LOIS

Réunie le mercredi 16 avril 2014, sous la présidence de M. Jean-Pierre Sueur, président, la commission des lois a examiné, sur le rapport de M. François Pillet, la **proposition de loi visant à limiter l'usage des techniques biométriques** (n° 361, 2013-2014).

Après avoir dressé un bref état des lieux des techniques biométriques existantes, le rapporteur a exposé le régime juridique d'autorisation préalable à la mise en œuvre de traitements automatisés comportant des données biométriques, institué par le législateur en 2004 et complété par la doctrine, en cours d'évolution, de la Commission nationale de l'informatique et des libertés (CNIL).

Le rapporteur a ensuite présenté la proposition de loi qui vise à encadrer le pouvoir d'autorisation préalable de la CNIL, en soumettant la mise en œuvre de traitements de données biométriques à la condition de justifier d'une finalité de « *stricte nécessité de sécurité* ».

Le rapporteur a estimé qu'il revenait effectivement au législateur de se prononcer sur les finalités légitimes des traitements de données biométriques. Il a d'ailleurs observé que cette proposition de loi offrait l'occasion au Sénat d'avancer sur ce sujet, dans la perspective de la discussion prochaine du projet de loi sur les libertés numériques.

Le rapporteur a cependant souhaité modifier le dispositif proposé sur deux points :

- préciser la notion de « *stricte nécessité de sécurité* » pour fixer des principes d'interprétation à la CNIL ;

- prévoir un dispositif transitoire de manière à accorder un délai aux responsables de traitements autorisés avant l'entrée en vigueur de la loi, pour les mettre en conformité avec la nouvelle législation.

La commission a adopté les deux amendements de son rapporteur et la proposition de loi ainsi modifiée.

Mesdames, Messieurs,

La biométrie est usuellement définie comme embrassant 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.

Cette définition recouvre de multiples techniques et types de données biométriques. Si chacun pense immédiatement aux empreintes digitales, à l'ADN, à la reconnaissance de la voix ou de l'iris de l'œil, on imagine plus rarement les données biométriques comportementales telles la démarche ou la dynamique de la signature ou de la frappe sur un clavier.

Différentes typologies peuvent être dressées pour classer ces données. Cependant avec le développement fulgurant des technologies auquel on a pu assister ces dernières années, les catégories évoluent. Ainsi par exemple de la distinction opérée il y a encore peu entre données « à trace » et « sans trace », selon qu'elles pouvaient ou non être recueillies et utilisées à l'insu de la personne concernée. Les progrès réalisés dans le traitement des images – photos, vidéos – et l'amélioration de la qualité de celles-ci coïncidant avec la multiplication des dispositifs de vidéoprotection conduisent à placer dorénavant la reconnaissance faciale parmi les techniques biométriques « traçantes ».

Parallèlement à l'essor de nouvelles technologies, de nouveaux usages se font jour. La biométrie reste essentiellement utilisée à des fins d'authentification des individus. Toutefois, au classique contrôle de l'accès physique à des locaux s'ajoute désormais, entre autres, celui de l'accès logique à des applications voire même à des données ou à des services distants.

Face à la rapidité des évolutions technologiques et au développement de nouveaux usages, le droit peine à appréhender, donc à encadrer ce mouvement. Comment s'assurer du bon usage de ces techniques ? Comment préserver les droits individuels, tout particulièrement celui à l'intégrité de son identité ? Où placer les garde-fous et quelle forme leur donner ?

C'est à cette réflexion que nous invite la proposition de loi de notre collègue Gaëtan Gorce et le groupe socialiste et apparentés visant à limiter l'usage des techniques biométriques (n° 361, 2013-2014).

I. UN ENCADREMENT JURIDIQUE TÂTONNANT FACE À DES TECHNOLOGIES ET USAGES BIOMÉTRIQUES ÉVOLUTIFS

A. RETOUR SUR LA BIOMÉTRIE

L'utilisation de la biométrie à proprement parler n'est pas neuve : l'usage de la photographie ou des empreintes digitales à des fins d'authentification des personnes est déjà ancien. L'innovation principale qui est à l'origine de l'essor que les techniques biométriques connaissent depuis maintenant plusieurs années consiste en son **couplage avec l'informatique**. Notre collègue député Christian Cabal en faisait la démonstration dans son rapport d'information présenté au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques :

« *La biométrie est un système d'identification des individus utilisant des caractéristiques mesurables comme les empreintes digitales, l'iris, la rétine, la forme du visage, de la main, la voix voire la démarche ou le système veineux. […]* ***Quasiment tout, dans l'anatomie ou le comportement d'un individu, peut être transformé en un code informatique permettant de l'identifier****.*

« *À partir d'un élément biométrique propre à un individu on détermine un gabarit, c'est-à-dire une suite numérique qui caractérise l'élément biométrique et c'est le gabarit qui est conservé et non l'image de l'élément biométrique à proprement parler. La technique d'élaboration du gabarit est propre à chaque éditeur de logiciel biométrique.*

« *Pour reconnaître un individu, on extrait des paramètres de l'image photographiée (empreinte, face, iris...) puis on compare le gabarit obtenu avec tous les paramètres précédemment extraits et sauvegardés.*

« *La novation de ce système de reconnaissance à partir d'éléments de biométrie est son caractère automatisé par le recours à l'informatique.* »[1]

Le traitement informatique des données biométriques a ainsi permis une **diversification des techniques** que l'on pourrait schématiquement classer en deux groupes :

- les techniques de **reconnaissance anatomique** qui utilisent les empreintes génétiques ou digitales, la géométrie de la main, l'iris, la rétine, le visage, le réseau veineux du doigt ou de la paume, mais aussi l'odeur, la forme de l'oreille, la pression sanguine, l'électrocardiogramme, l'électroencéphalogramme…

- les techniques de **reconnaissance dynamique** qui s'appuient sur des données comportementales telles la reconnaissance vocale, la signature manuscrite dynamique, la frappe sur un clavier, la démarche…

---

[1] Cf. *Rapport sur les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre, fait par M. Christian Cabal, député, au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (n° 355, 2012-2013).*

Si certaines de ces techniques sont désormais bien maîtrisées comme les empreintes digitales ou la reconnaissance du réseau veineux, la plupart sont encore expérimentales et ne connaissent que peu ou pas de mise en œuvre pratique. Par ailleurs, le coût de certaines de ces techniques telles la reconnaissance de l'iris explique leur faible utilisation en dépit de leur grande fiabilité. D'après les données fournies par la Commission nationale de l'informatique et des libertés (CNIL) à votre rapporteur, les techniques biométriques les plus utilisées seraient ainsi les empreintes digitales, le réseau veineux et le contour de la main.

Selon les usages seront privilégiés tels ou tels types de biométrie, la fiabilité des techniques étant fonction de la plus ou moins grande maturité de la technologie biométrique, le taux de faux – rejet ou acceptation – variant selon la technique biométrique utilisée mais également selon le dispositif employé.[1]

B. LA BIOMÉTRIE SAISIE PAR LE DROIT

1. Une loi elliptique

Parce que la donnée biométrique est produite par le corps lui-même et le désigne ou le représente de façon immuable, que le détournement ou le mauvais usage de cette donnée pourrait avoir des conséquences particulièrement graves pour la protection de la personne concernée, le respect de son identité et de sa liberté, le législateur a souhaité accorder une protection particulière à cette catégorie de données à caractère personnel. À l'initiative de la CNIL, il a donc introduit, par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, une disposition visant à **soumettre le traitement des données biométriques à un régime d'autorisation préalable**.

En effet, alors même que la loi n° 2004-801 du 6 août 2004 précitée procédait à l'allègement des procédures préalables à la mise en place de la plupart des traitements de données à caractère personnel par l'introduction d'un régime de droit commun de déclaration préalable, le législateur a ici fait application de la faculté qui lui était offerte par l'article 20 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, de prévoir dans certains cas un contrôle *a priori* des traitements de données[2].

---

[1] *Votre rapporteur note que l'étude suscitée menée par le député Christian Cabal au nom de l'OPECST était à cet égard très éclairante, mais qu'elle mériterait une actualisation étant donné la vitesse à laquelle évoluent les techniques.*

[2] « 1. Les États membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre. »

En matière de traitement de données biométriques, le législateur a ainsi distingué deux régimes d'autorisation :

- le premier soumet à autorisation préalable de la CNIL « *les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes* », conformément au 8° du I de l'article 25 de la loi n° 78-17 du 6 janvier 1978 précitée ;

- le second conditionne la mise en œuvre pour le compte de l'État de traitements de données biométriques à une autorisation délivrée par décret en Conseil d'État pris après avis motivé et publié de la CNIL, en vertu du 2° du I de l'article 27 de la même loi[1].

Afin de faciliter la tâche de la CNIL dans le cadre de son activité d'autorisation préalable et lui permettre de faire face à des demandes massives, le législateur a toutefois prévu, au II de l'article 25, que « *les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.* » L'avis de la CNIL sur le projet de loi de 2004 envisageait d'y recourir largement « *si la nécessité s'en faisait sentir* », dans le cas de traitements de données biométriques. Tel est effectivement le fondement des cinq **autorisations uniques** adoptées par la CNIL en matière de traitement de données biométriques :

- l'autorisation unique n° AU-007, adoptée par la délibération n° 2006-101 du 27 avril 2006 et modifiée par la délibération n° 2012-322 du 20 septembre 2012 portant autorisation unique de mise en œuvre de traitements reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la restauration sur les lieux de travail[2] ;

- l'autorisation unique n° AU-008, adoptée par la délibération n° 2006-102 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail ;

---

[1] *Il convient de noter que si le 8° du I de l'article 25 mentionne* « les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes » *tandis que le 2° du I de l'article 27 encadre* « les traitements de données à caractère personnel mis en œuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes », *la CNIL n'a pas jugé souhaitable de tenir compte de cette différence de rédaction qui aurait pu conduire à une méthodologie d'analyse différente selon que le dispositif était ou non opéré pour le compte de l'État.*

[2] *La modification de l'autorisation a consisté en la suppression de la finalité de contrôle des horaires des salariés jugée disproportionnée à la suite d'une consultation des organisations syndicales et patronales, de la Direction générale du travail et de professionnels du secteur.*

- l'autorisation unique n° AU-009, adoptée par la délibération n° 2006-103 du 27 avril 2006 portant autorisation unique de mise en œuvre de traitements automatisés 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 ;

- l'autorisation unique n° AU-019, adoptée par la délibération n° 2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail ;

- l'autorisation unique n° AU-027, adoptée par la délibération n° 2011-074 du 10 mars 2011 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux postes informatiques portables professionnels.

En imposant un contrôle *a priori* de tout traitement de données biométriques, la France s'est ainsi dotée de l'un des régimes juridiques les plus protecteurs en la matière. Ce régime d'autorisation préalable fait d'ailleurs figure de quasi exception en Europe.

En 2004 cependant, **le législateur ne s'est aucunement prononcé sur la pertinence des différents usages des techniques biométriques**. Il s'est ainsi borné à confier à la CNIL la mission d'autoriser les traitements de données biométriques « *nécessaires au contrôle de l'identité des personnes* » en lui laissant toute latitude pour élaborer une doctrine.

2. Une doctrine de la CNIL en cours d'évolution

Comme pour toute demande d'autorisation d'un traitement de données à caractère personnel, l'examen par la CNIL d'une demande d'autorisation d'un traitement de données biométriques consiste en l'analyse de sa **proportionnalité** eu égard à la **finalité** envisagée, en application des 2° et 3° de l'article 6 de la loi n° 78-17 du 6 janvier 1978 précitée qui disposent que les données collectées « *sont adéquates, pertinentes et non excessives au regard des finalités [déterminés, explicites et légitimes] pour lesquelles elles sont collectées* ». Est ainsi appréciée l'adéquation entre, d'une part, le dispositif proposé et les risques d'atteinte à la confidentialité des données (principe de sécurité) ainsi qu'au respect des droits et libertés des personnes concernées – avec, au premier chef, le droit à l'information préalable – et, d'autre part, la finalité déclarée.

Confrontée à un nombre de demandes d'autorisation croissant, la CNIL a peu à peu dégagé une grille d'analyse spécifique aux traitements de données biométriques.

a) Une doctrine initialement assise sur les spécificités des différents types de biométrie

De 2005 à 2012, la CNIL a procédé en distinguant les techniques biométriques utilisées selon qu'elles étaient :

- **« à trace »**, c'est-à-dire mettant en œuvre des éléments laissant des traces susceptibles d'être capturées à l'insu de la personne pour l'identifier ou être utilisées pour usurper son identité, telles les empreintes génétiques ou digitales ;

- ou **« sans trace »** – contour de la main, reconnaissance vocale, réseau veineux du doigt ou de la paume de la paume, iris de l'œil, reconnaissance faciale, biométrie comportementale.

Le recours aux techniques biométriques « à trace » était donc plus strictement limité et encadré.

À titre d'illustration, dix ans après s'être prononcée pour la première fois sur un dispositif reposant sur la reconnaissance des empreintes digitales, la CNIL a formalisé ses critères d'autorisation par une « *communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données* », en date du 28 décembre 2007. Du fait de la spécificité des empreintes digitales, le stockage sur support individuel permettant à la personne concernée de conserver la maîtrise de sa donnée biométrique était privilégié. Le stockage sur un terminal de lecture-comparaison ou sur un serveur comportant davantage de risque, il n'était autorisé qu'à la condition, en particulier, que la finalité du dispositif soit « *limitée au contrôle de l'accès d'un nombre limité de personnes à une zone bien déterminée, 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* ». Par « *zone bien délimitée* », la CNIL indiquait entendre aussi bien des locaux que du matériel ou une application informatique par exemple.

À partir de 2013, la CNIL a pris conscience de la faiblesse de cette *summa divisio*, des techniques précédemment considérées comme « sans trace » donc moins intrusives basculant dans le champ des techniques « à trace ». Ainsi par exemple de la reconnaissance faciale du fait de la convergence des développements technologiques et de la multiplication des dispositifs de vidéosurveillance.

b) Le retour aux fondamentaux de la loi : une nouvelle doctrine en cours d'élaboration basée sur les finalités des traitements

De ce constat est née une réflexion sur la méthodologie d'instruction des demandes d'autorisation de dispositifs biométriques qui, après consultation de représentants de la société civile, de la communauté scientifique et de l'industrie, a débouché sur une nouvelle typologie que la CNIL a commencé de tester au cours des derniers mois.

La perception par les Français de la biométrie au quotidien

Dans le cadre de sa réflexion sur la biométrie, la CNIL s'est associée au Centre de recherche pour l'étude et l'observation des conditions de vie (CREDOC) pour mener une étude sur les attitudes de la population française face aux enjeux et questions que pose le développement des technologies biométriques.

Selon la note de synthèse, cette étude « *met en évidence qu'aujourd'hui, la population consent à un usage de la biométrie dans des cas très précis (fichier de police, carte d'identité) conjuguant la présence d'un cadre institutionnel et des fins sécuritaires. L'utilisation de données biométriques comme moyen de paiement, pour s'identifier dans un cadre professionnel ou de loisirs suscite de grandes réticences. Les Français étant particulièrement soucieux de pouvoir choisir d'accepter ou de refuser, au cas par cas, l'usage de ces techniques dans leur vie quotidienne* ».

Cette étude souligne que « *nos concitoyens sont en effet particulièrement préoccupés par rapport au détournement potentiel de leurs données personnelles par des entreprises*. » De là l'importance accordée au consentement.

Source : Sandra Hoibian, Les Français se montrent réservés sur l'usage de la biométrie dans la vie quotidienne*, CREDOC, Collection des rapports, mai 2013.*

Trois cas seraient désormais envisagés par la CNIL selon la finalité du dispositif proposé :

- **Cas n° 1 : la « biométrie de sécurité »**

Dans cette hypothèse, la mise en œuvre d'un dispositif biométrique apparaît comme indispensable pour répondre à une contrainte de sécurité physique ou logique d'un organisme. Cela entraîne pour conséquence que l'utilisation du dispositif biométrique sera exclusive, seul un dispositif de secours exceptionnel le doublant afin d'assurer la continuité du service. Il en découle une absence de choix des utilisateurs qui devront cependant être dûment informés des conditions d'utilisation du dispositif par une note d'information précisant la finalité du traitement, la stricte nécessité de l'usage de la biométrie, l'absence de dispositif alternatif et le numéro de l'autorisation délivrée par la CNIL.

La finalité de sécurité doit dans ce cas être démontrée par une analyse des risques remise à la CNIL. Une étude d'impact sur la vie privée doit permettre, par ailleurs, de déterminer les mesures à mettre en œuvre pour faire face aux nouveaux risques d'atteinte à la vie privée des personnes concernées, nés de la mise en œuvre du dispositif biométrique.

- **Cas n° 2 : la « biométrie de service », mettant en exergue le libre consentement de l'usager**

Dans cette deuxième hypothèse, la finalité du dispositif envisagé est double, à la fois de sécurité pour un contrôle de l'accès à un site physique ou à une application logique ou un équipement, et d'ergonomie d'utilisation – l'impératif de sécurité n'étant pas ici strict, une analyse de risque ne sera pas

exigée. Dès lors, un dispositif alternatif au dispositif biométrique doit nécessairement être proposé aux utilisateurs sans contrainte ni surcoût. L'information de l'utilisateur doit être écrite, individuelle, préalable et spécifique au dispositif mis en œuvre. La signature par l'utilisateur de la note d'information permet de s'assurer de son consentement exprès. Enfin, le stockage des données biométriques est sécurisé.

Synthèse des critères applicables aux biométries « de sécurité » et « de service »

Biométrie de sécurité	Biométrie de service
Confidentialité des données garantie par une **analyse de risques obligatoire**	**Confidentialité** des données garantie par un **stockage soumis à des exigences techniques et organisationnelles minimales**
Absence de dispositif alternatif	**Dispositif alternatif obligatoire**
Absence de consentement	Nécessité d'un **consentement**
Information des personnes sur **l'objectif de sécurité** (démontré par une analyse de risques) et l'absence de dispositif alternatif	**Information renforcée** des personnes : • sur l'existence d'un **dispositif alternatif** • sur la possibilité de **choisir librement** le dispositif biométrique ou un autre

Source : CNIL

- **Cas n° 3 : les expérimentations**

Par expérimentation, la CNIL entend les travaux de recherche fondamentale menés par des laboratoires ou centres de recherche, les expérimentations de recherche et développement conduites par des consortiums publics et/ou privés ou encore tout test opérationnel préalable à la généralisation d'un dispositif réalisé par une entreprise. Ces expérimentations servent en particulier à vérifier la fiabilité technique des dispositifs, mais aussi à identifier les risques et impacts relatifs à la vie privée. L'autorisation est soumise au respect de cinq critères :

- justifier d'un apport significatif en termes de connaissances ;
- limiter la durée de l'expérimentation ;
- présenter un bilan de l'expérimentation à la CNIL ;
- recueillir le consentement exprès et préalable des personnes participant à l'expérimentation ou, au contraire, démontrer l'impossibilité de le recueillir ;
- garantir la sécurité des données.

La définition de ce troisième cas a de fait permis la formalisation des autorisations précédemment délivrées par la CNIL dans le cadre d'expérimentations. Désormais, les décisions de la CNIL comportent la durée de l'expérimentation, par défaut établie à un an sauf spécificités (au lieu de durées oscillant entre 6 mois et 3 ans précédemment). Elles précisent ce que devra comporter le bilan de l'expérimentation. Les services de la CNIL doivent recevoir le bilan de l'expérimentation au plus tard deux mois après la fin de celle-ci – un tableau de suivi permettant de relancer le responsable de traitement en cas d'omission. Les services analysent ces bilans au regard de l'autorisation initiale. À l'issue de l'expérimentation, toute pérennisation d'un dispositif doit faire l'objet d'une nouvelle autorisation conformément au 1° de l'article 6 de la loi n° 78-17 du 6 janvier 1978 précitée imposant le caractère loyal de la collecte et du traitement des données.

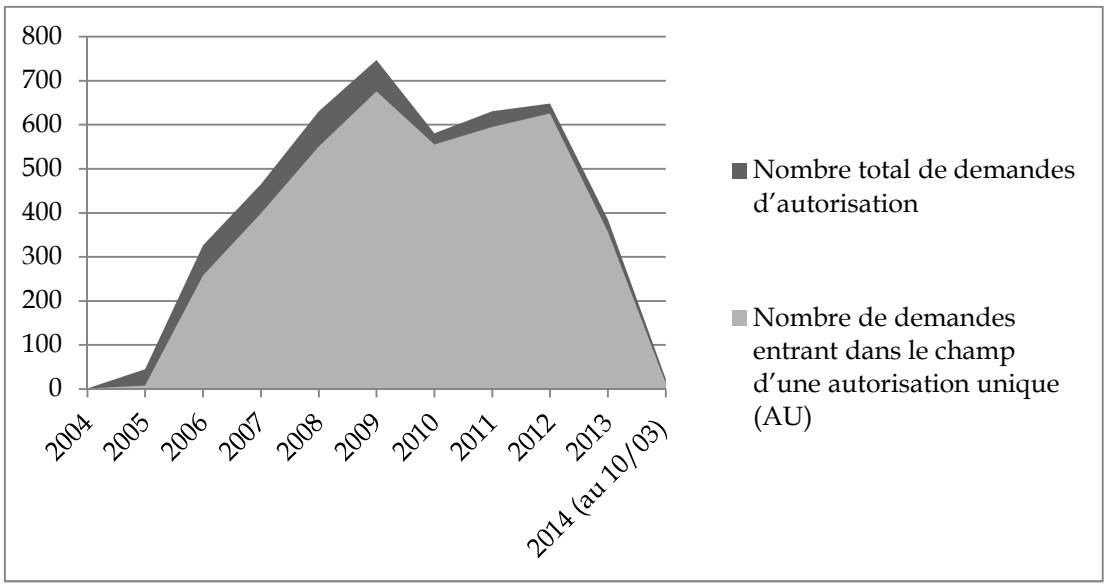
Dans tous les cas envisagés, le respect du principe de proportionnalité reste au cœur de l'examen mené par la CNIL pour délivrer ou non une autorisation.

Si **la CNIL** tente ainsi d'adapter ses exigences aux finalités envisagées pour un traitement de données biométriques, elle **ne s'autorise pas à juger de la pertinence de ces finalités**.

C. LA BANALISATION DE L'USAGE DES TECHNIQUES BIOMÉTRIQUES

Dès son rapport d'activité pour 2005, la CNIL constatait une « *réelle banalisation de la biométrie* ». Le nombre des demandes d'autorisation présentées à la CNIL par la suite n'a pas démenti ce constat, loin de là.

Évolution des demandes d'autorisation
de mise en œuvre de dispositifs biométriques depuis 2004



Source : commission des lois à partir des données fournies par la CNIL

Votre rapporteur observe ainsi une **augmentation massive des demandes d'autorisation à partir de 2006**, avec un pic en 2009, mais un recul notable en 2013, peut-être dû aux incertitudes nées de l'annonce par la CNIL d'une révision de sa doctrine. Il note également le rôle majeur des engagements de conformité à des autorisations uniques (AU) qui ne donnent pas lieu à examen *a priori* par la CNIL, seulement à des contrôles *a posteriori*, et sont donc tous autorisés : ils représentent en effet plus de 90 % des demandes d'autorisation. Les demandes d'autorisation spécifiques, au nombre de 443 au total, représentent donc moins de 10 % des demandes ; elles ont un taux d'acceptation de près de 77 %, soit un taux de rejet d'environ 23 %.

Statistiques sur les demandes d'autorisation présentées à la CNIL de 2004 au 10 mars 2014

	Demandes d'autorisation		**Autorisations délivrées**			**Refus**
Année	Nb de demandes entrant dans le champ d'une autorisation unique	**Nb total de demandes**	Nb d'autorisations « spécifiques »	Nb d'autorisations *via* un engagement de conformité à une AU	**Nb total d'autorisations délivrées**	**Nb de refus**
2004	1	**1**	0	1	**1**	**0**
2005	8	**45**	30	8	**38**	**5**
2006	258	**326**	59	258	**317**	**9**
2007	399	**465**	45	399	**444**	**21**
2008	550	**630**	61	550	**611**	**19**
2009	676	**747**	68	676	**744**	**3**
2010	555	**581**	22	555	**577**	**4**
2011	595	**631**	28	595	**623**	**8**
2012	626	**648**	22	626	**648**	**0**
2013	357	**385**	5	357	**362**	**12**
2014	13	**22**	0	13	**13**	**0**
TOTAL	4038	**4481**	340	4038	**4378**	**81**[1]

Source : commission des lois à partir des données fournies par la CNIL

La banalisation est également celle des usages qui, tout comme les techniques, ont connu une grande diversification. L'étude des principales délibérations prises par la CNIL au cours de ces années permet de relever certains de ces nouveaux usages :

- le contrôle d'accès physique à des locaux : autrefois réservé à l'accès à des locaux sensibles, il est désormais étendu à des cantines

[1] *Ce chiffre correspond au nombre de refus délibérés en séance et notifiés : il ne compte pas les dossiers soumis à la CNIL puis « abandonnés » par les déclarants.*

scolaires[1], des locaux de loisirs – salle de sport[2] ou cercle de jeux[3] –, ainsi que, par exemple, à des salles d'examen afin d'empêcher la substitution de candidat[4] ;

- le contrôle d'accès logique à des services[5] ou des applications[6] ;

- la signature de documents électroniques[7] ;

- la gestion de mots de passe[8] ;

- le contrôle de la présence de travailleurs handicapés[9] ;

- le contrôle d'accès à un équipement bureautique[10] ;

- la gestion d'une carte de fidélité[11] ;

- le contrôle de l'identité des patients pris en charge en radiothérapie[12] ;

- l'accès à un dossier médical partagé[13].

---

[1] Cf. *l'autorisation unique n° AU-009, adoptée par la délibération n° 2006-103 du 27 avril 2006.*

[2] Cf. *la délibération n° 2009-311 du 7 mai 2009 (Centre de culture physique d'Aquitaine – reconnaissance du contour de la main).*

[3] Cf. *la délibération n° 2010-469 du 16 décembre 2010 (CERCLE WAGRAM – reconnaissance du visage en trois dimensions exclusivement enregistrée sur un support individuel détenu par la personne concernée).*

[4] Cf. *la délibération n° 2009-360 du 18 juin 2009 (Graduate Management Admission Council (GMAC) représenté par Pearson Education France – reconnaissance du réseau veineux de la paume de la main).*

[5] *Par exemple, la délibération n° 2005-206 du 22 septembre 2005 (société Bloomberg L.P – reconnaissance de l'empreinte digitale – contrôle de l'accès logique à un service d'informations financières).*

[6] *Exemple de la délibération n° 2011-325 du 13 octobre 2011 (société FACEO SECURITE PREVENTION – reconnaissance des empreintes digitales – accès à une application de main courante électronique d'un poste de sécurité).*

[7] *Première autorisation : délibération n° 2006-232 du 17 octobre 2006 (société l'Oréal SA – reconnaissance des empreintes digitales).*

[8] *Exemple de la délibération n° 2007-248 du 13 septembre 2007 (manufacture française de pneumatique Michelin – reconnaissance vocale).*

[9] Cf. *la délibération n° 2008-038 du 7 février 2008 (Centre d'Aide au Travail - « le Vert Coteau » de Thionville – reconnaissance du réseau veineux).*

[10] Cf. *la délibération n° 2010-085 du 25 mars 2010 (société Apave Parisienne – reconnaissance du réseau veineux des doigts – contrôle d'accès à des appareils de reprographie multifonctions).*

[11] *Une seule autorisation délivrée à ce jour par la délibération n° 2005-115 du 7 juin 2005 portant autorisation de la mise en œuvre par la Chambre de commerce et d'industrie de Nice-Côte d'Azur d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion d'une carte de fidélité impliquant l'utilisation d'un dispositif biométrique de reconnaissance des empreintes digitales.*

[12] *La délibération n° 2012-236 du 12 juillet 2012 autorisant le Centre Oscar Lambret à mettre en œuvre, à titre expérimental, un traitement automatisé de données à caractère personnel utilisant un nouveau dispositif biométrique de contrôle de l'identité des patients pris en charge en radiothérapie fait suite à une première délibération (n° 2010-033 du 11 février 2010).*

[13] *Par exemple, la délibération n° 2012-445 du 6 décembre 2012 (établissement public de santé Maison Blanche, réseau santé mentale précarité – reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel sous le contrôle exclusif de son détenteur).*

Les organismes bancaires s'intéressent également à la biométrie afin de sécuriser les transactions financières, notamment les paiements en ligne ou sans contact, ou l'accès à des coffres forts numériques. Au cours des derniers mois, plusieurs expérimentations ont été autorisées par la CNIL dans ce secteur.

Ce bref aperçu non exhaustif permet de constater combien **la biométrie pénètre peu à peu tous les domaines de la vie quotidienne**, de l'école à l'entreprise, de la santé à la banque.

II. LA PROPOSITION DE LOI : UN OBJECTIF AFFICHÉ AMBITIEUX, UNE MISE EN ŒUVRE PLUS MODESTE

La proposition de loi présentée par notre collègue Gaëtan Gorce s'inscrit en réaction à l'inflexion de la doctrine de la CNIL à l'œuvre depuis plusieurs années. Son auteur estime en effet que certains usages, pourtant autorisés par la CNIL, ne devraient pas être encouragés, à l'instar de l'autorisation unique relative à la biométrie dans les cantines scolaires. Face à la biométrie « de confort », séduisante par son ergonomie, l'auteur doute de la valeur du consentement de l'usager confronté au choix entre deux modes alternatifs. Il propose donc au législateur de mettre un frein à une banalisation excessive de l'usage des données biométriques.

A. UN ENCADREMENT PAR LE LÉGISLATEUR DES FINALITÉS LÉGITIMES DE LA BIOMÉTRIE

1. L'exposé des motifs : l'esquisse d'un statut spécifique de la donnée biométrique

Dans l'exposé des motifs de sa proposition de loi, l'auteur justifie l'encadrement par le législateur de l'usage des techniques biométriques par la nature spécifique des données biométriques, « *produites* » par le corps humain. Il observe ainsi que si ces données ne peuvent bénéficier de la même protection que celle que le code civil accorde au corps humain dans la mesure où elles ne se confondent pas avec celui-ci, elles devraient toutefois, en tant que « *prolongement direct* » du corps humain, bénéficier d'une protection plus rigoureuse que toute autre donnée personnelle et faire l'objet de « *règles « inspirées » de celles protégeant le corps humain* ».

Introduit par la loi n° 94-653 du 29 juillet 1994 relative au respect du corps humain, l'article 16-1 du code civil affirme en effet le droit de chacun au respect de son corps, avant de poser les principes de l'inviolabilité et de l'indisponibilité du corps humain. Ce second principe est étendu par le même article du code civil aux « éléments » et « produits » du corps

humain.[1] Ainsi que l'expliquait M. Bernard Bioulec, rapporteur de la commission spéciale de l'Assemblée nationale, « *l'indisponibilité du corps humain fait obstacle à ce que le corps et ses éléments soient traités comme des marchandises et deviennent objets de commerce.* »[2] Ce principe est ensuite explicité par les articles 16-5 affirmant la nullité de toute convention à titre onéreux portant sur le corps et ses éléments, 16-6 interdisant la rémunération de ceux qui se prêtent à une expérimentation, à la collecte de sang ou au prélèvement d'éléments ou de produits du corps, et enfin 16-7 affirmant la nullité des conventions de mère porteuse.

En se référant au chapitre II du titre Ier du livre Ier du code civil, l'auteur de la proposition de loi semble ainsi inviter le législateur à envisager un statut de la donnée biométrique s'inspirant de ces dispositions.

2. Le dispositif : l'encadrement du pouvoir d'autorisation de la CNIL

Pourtant, et contrairement à ce que pourrait laisser croire de prime abord l'exposé des motifs, l'article unique de la proposition de loi ne modifie pas le code civil mais vient compléter l'article 25 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, par l'insertion d'un nouveau paragraphe II *bis* précisant les conditions d'application du 8° du I du même article relatif aux « *traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes* ». Ceux-ci ne seraient autorisés qu'à condition d'être justifiés par une « *stricte nécessité de sécurité* ».

En premier lieu, votre rapporteur rappelle que cet article 25 soumet à autorisation préalable directe de la CNIL les traitements de données qui ne sont pas mis en œuvre pour le compte de l'État. Ces derniers sont en effet soumis à un régime distinct d'autorisation : les articles 26 et 27 de la même loi prévoient que cette autorisation est délivrée par un acte réglementaire pris après avis motivé et publié de la CNIL ; le 2° du I de l'article 27 renvoie au décret en Conseil d'État dans le cas de traitements de données biométriques.

Cela emporte deux conséquences :

- est exclu du champ de la proposition de loi tout traitement de données biométriques mis en œuvre pour le compte de l'État ;

- la proposition de loi encadre le seul pouvoir d'autorisation de la CNIL, non celui du pouvoir réglementaire.

---

[1] *« Art. 16-1. – Chacun a droit au respect de son corps.*
« Le corps humain est inviolable.
« Le corps humain, ses éléments et ses produits ne peuvent faire l'objet d'un droit patrimonial. »

[2] *Cf. JO Débat AN, 1ère séance du 19 novembre 1992, p. 5718.*

En second lieu, votre rapporteur attire l'attention sur le fait que la proposition de loi ne vient que préciser les conditions de finalité dans lesquelles peuvent être autorisés les traitements prévus au 8° du I, sans amender la rédaction de celui-ci. Ainsi la proposition de loi n'a pas pour conséquence de modifier la mission de la CNIL ou d'élargir le champ de son contrôle à des traitements de données biométriques qui ne seraient pas « *nécessaires au contrôle de l'identité des personnes* », autrement dit à des dispositifs qui poursuivraient d'autres objectifs que l'authentification ou l'identification des individus. Cela est cohérent avec l'objet même de la loi n° 78-17 du 6 janvier 1978 précitée qui consiste en la protection des personnes à l'égard des traitements de données à caractère personnel, une donnée personnelle étant définie par son article 2 comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ».

La proposition de loi ne définit donc pas un statut de la donnée biométrique. **Elle se contente de conditionner l'autorisation de la mise en œuvre d'un traitement de données biométriques à une « *stricte nécessité de sécurité* »**.

B. UN ENCADREMENT CIRCONSCRIT

En vertu du premier alinéa de l'article 2 de la loi n° 78-17 du 6 janvier 1978 précitée, celle-ci « *s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.* » Le même article définit par ailleurs le traitement de données comme « *toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment 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.* »

L'article 2 crée ainsi en son premier alinéa une **« exception domestique »**. Si la rédaction actuelle, introduite par la révision de la loi en 2004, découle des dispositions du dernier alinéa de l'article 3 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 précitée, cette exception reprend une restriction qui figurait à l'article 45 de la loi initiale. La discussion parlementaire ayant conduit à inclure dans le champ d'application de la loi tous les fichiers, y compris non automatisés, cette restriction avait pour objet de répondre « *à l'obligation touchant au caractère trop extensif de la notion de fichier qui aurait pu aller jusqu'à englober de simples*

agendas »[1]. Si cette exception concerne donc au premier chef les fichiers liés à des activités personnelles ou domestiques tels les annuaires privés ou les bases servant à la gestion d'une cave à vin, qu'ils soient sous format papier ou dématérialisés, son champ a été étendu aux sites web et blogs personnels dont l'accès est restreint[2].

La proposition de loi s'inscrivant dans le cadre de la loi n° 78-17 du 6 janvier 1978 précitée, **sont donc exclus de son champ d'application les traitements de données biométriques mis en œuvre par un responsable de traitement pour l'exercice d'activités exclusivement personnelles**. Ainsi par exemple des dispositifs biométriques d'authentification placés sur les ordinateurs et téléphones portables personnels.

C. LES EFFETS SUR LES DISPOSITIFS EXISTANTS

Interrogée par votre rapporteur sur les effets, en cas d'adoption de la proposition de loi, sur les traitements autorisés avant son entrée en vigueur, la CNIL a indiqué que si toutes les autorisations délivrées à ce jour répondaient à une finalité de sécurité, toutes ne répondaient néanmoins pas à une finalité de « stricte nécessité de sécurité » interprétée selon les critères définis dans le cadre du cas n° 1 de la nouvelle méthodologie. Ainsi, si la plupart des autorisations spécifiques délivrées pourraient être maintenues, il en irait différemment pour les engagements de conformité à des autorisations uniques dont une grande part cesserait d'être autorisée par la loi.

La CNIL a également fait valoir que « *la nouvelle doctrine que la CNIL est susceptible d'adopter concernant la biométrie « de service » (anciennement dénommée « de confort ») ne pourrait être retenue* », ce qui empêcherait la mise aux nouvelles normes définies par la CNIL de ces nombreux traitements autorisés avant 2014.

S'agissant des expérimentations, la proposition de loi ne les autoriserait implicitement que dans l'hypothèse où elles seraient menées pour des finalités de « stricte nécessité de sécurité ».

---

[1] *Cf. rapport de M. Jean Foyer, fait au nom de la commission des lois de l'Assemblée nationale, sur le projet de loi relatif à l'informatique et aux libertés (n° 3352, V^e^ législature), p. 7.*

[2] *En cas d'accès non restreint, la délibération n° 2005-284 du 22 novembre 2005 décidant la dispense de déclaration des sites web diffusant ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'une activité exclusivement personnelle (norme d'exonération n° 6) exonère le responsable de traitement de l'obligation de déclaration préalable ; le traitement reste cependant soumis aux dispositions de la loi n° 78-17 du 6 janvier 1978 précitée.*

III. LA POSITION DE LA COMMISSION : UNE INITIATIVE BIENVENUE MAIS UN DISPOSITIF PERFECTIBLE

A. LE PRINCIPE : UNE PRISE DE POSITION LÉGITIME DU LÉGISLATEUR

Dans son rapport d'activité pour 2012, la CNIL s'interrogeait sur son rôle face à l'essor des dispositifs biométriques. Elle se demandait en particulier s'il lui revenait d'« *imposer une frontière claire entre les usages pertinents de la biométrie et ceux qui ne sont pas considérés comme acceptables car présentant trop de risques pour la vie privée eu égard à leur finalité* »[1]. Bien que le législateur n'ait pas saisi l'opportunité offerte en 2004 par l'introduction dans la loi de la biométrie pour se prononcer, votre rapporteur estime que ce rôle revient légitimement au législateur.

La proposition de loi de notre collègue Gaëtan Gorce permet d'engager cette réflexion à un moment particulièrement opportun puisque le Gouvernement devrait présenter dans les prochains mois un projet de loi sur les libertés numériques, qui amènera le Parlement à réexaminer certains pans de la loi n° 78-17 du 6 janvier 1978 précitée.

Par ailleurs, votre rapporteur observe que les préoccupations exprimées par cette proposition de loi font écho à celles qui se font jour au niveau international. En effet, à l'occasion de la révision de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe, dite « Convention 108 », le comité de réflexion a proposé, en décembre 2012, d'intégrer au sein des données sensibles les données biométriques. L'article 6 de la convention, dans le projet final, stipule que « *le traitement de données biométriques identifiant un individu de façon unique […] n'est autorisé qu'à la condition que la loi applicable prévoit des garanties appropriées, venant compléter celles de la présente convention* ». Et de préciser que « *les garanties appropriées doivent être de nature à prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination.* » Ainsi, le Conseil de l'Europe lui-même semble inviter le législateur français à réexaminer les garanties entourant le traitement de données biométriques.

Si votre rapporteur partage l'objectif poursuivi par la proposition de loi d'un usage raisonné des techniques biométriques eu égard à la nature si particulière des données ainsi collectées, il a néanmoins émis quelques réserves sur le dispositif envisagé et proposé à votre commission des modifications.

---

[1] *Cf. rapport d'activité 2012, Commission nationale de l'informatique et des libertés, p. 86.*

B. LES QUESTIONS SOULEVÉES PAR LE DISPOSITIF DE LA PROPOSITION DE LOI

1. Son articulation avec le règlement européen à venir sur la protection des données à caractère personnel

Votre rapporteur observe tout d'abord que toute réflexion sur le traitement de données à caractère personnel ne saurait utilement être conduite sans tenir compte de l'élaboration en cours du règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (COM(2012)0011), qui remplacera la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 précitée. Un règlement européen, contrairement à une directive, étant d'application directe et immédiate, ce règlement se substituera à la loi n° 78-17 du 6 janvier 1978 précitée lors de son entrée en vigueur.

L'une des modifications majeures de la proposition de règlement par rapport à la directive consisterait en un changement de logique : toute contrainte *a priori* pesant sur le responsable de traitement serait supprimée en contrepartie d'un renforcement *a posteriori* de sa responsabilité. Cela vaudrait également pour la mise en œuvre de traitements de données biométriques, rendant obsolète le dispositif de l'article 25 de la loi n° 78-17 du 6 janvier 1978 précitée que vient compléter la proposition de loi.

Votre rapporteur note cependant avec satisfaction que l'attention particulière portée par la France aux traitements de données biométriques pourrait être reprise à terme dans le règlement européen. En effet, à l'issue de son examen par le Parlement européen en première lecture, les données biométriques ont été intégrées parmi les catégories particulières de données. L'article 9 de la résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement pose, en son paragraphe 1, le principe de l'interdiction du traitement de données biométriques[1].

Ce principe est tempéré par une série d'exceptions énumérées en son paragraphe 2. On relève parmi ces dernières que le traitement peut toutefois être autorisé si la personne concernée y a consenti, à moins qu'une disposition nationale y fasse obstacle[2]. Ainsi la législation nationale pourrait

---

[1] *« 1. Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances philosophiques, l'orientation sexuelle ou l'identité de genre, l'appartenance et les activités syndicales, ainsi que* ***le traitement des données génétiques ou biométriques*** *ou des données concernant la santé ou relatives à la vie sexuelle, aux sanctions administratives, aux jugements, à des infractions pénales ou à des suspicions, à des condamnations, ou encore à des mesures de sûreté connexes* ***sont interdits****. »*

[2] *« 2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :*
« a) ***la personne concernée a donné son consentement au traitement de ces données à caractère personnel à une ou plusieurs fins spécifiques****, dans les conditions fixées à l' article 7 et à l'article 8,* ***sauf lorsque*** *le droit de l'Union ou* ***la législation nationale prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée****, ».*

prévoir des cas pour lesquels le consentement de la personne concernée ne suffirait pas à autoriser un traitement de données biométriques. Dès lors, le législateur français pourrait effectivement s'il le souhaitait limiter les cas d'usage de traitement de données biométriques même après l'entrée en vigueur du futur règlement européen.

2. La définition de la notion de « stricte nécessité de sécurité »

Il est ressorti des auditions conduites par votre rapporteur que la notion de « stricte nécessité de sécurité » était insuffisamment précise, en dépit de l'explicitation apportée par la dernière phrase de l'exposé des motifs qui précise qu'elle devrait être entendue « *comme la sécurité des personnes et des biens, ou la protection des informations dont la divulgation, le détournement ou la destruction porterait un préjudice grave et irréversible* ».

Votre rapporteur a donc souhaité préciser cette notion afin qu'elle ne soit entendue de façon ni trop large, ni trop étroite. En effet, une acception trop large de la notion de sécurité annihilerait la volonté du législateur de n'autoriser qu'un usage raisonné des données biométriques. Une acception trop étroite en revanche pourrait conduire à un phénomène d'éviction contre-productif, les usagers ayant recours à des produits et services développés et acquis à l'étranger et échappant de ce fait à tout contrôle par les autorités nationales.

C'est pourquoi votre rapporteur s'est inspiré de la communication de la CNIL en date de 2007 et a proposé de reprendre la **notion d'intérêt excédant l'intérêt propre de l'organisme**. Cela permettrait en particulier d'inclure l'authentification pour les transactions financières dans la mesure où, au-delà de l'intérêt des banques et commerçants, il en irait de la protection des intérêts du citoyen-consommateur.

Sur proposition de son rapporteur, votre commission a donc adopté un **amendement** venant préciser la finalité légitime d'un traitement de données biométriques.

3. La nécessité de prévoir un dispositif transitoire

Conscient des conséquences économiques et organisationnelles lourdes que l'introduction de la limitation des usages des techniques biométriques aurait sur les traitements de données biométriques autorisés avant l'entrée en vigueur de la loi, votre rapporteur a proposé de prévoir une période transitoire afin de permettre aux détenteurs d'autorisations délivrées par la CNIL sous l'empire de la loi de 2004 de se mettre en conformité avec la nouvelle législation.

Lors de l'adoption de la délibération modifiant l'autorisation unique n° AU-007 visant à ne plus autoriser à l'avenir les traitements de données biométriques pour le contrôle des horaires des salariés, la CNIL a prévu une

période transitoire de cinq ans correspondant, selon ses indications, à la « durée de vie » d'un lecteur du contour de la main afin de ne pas pénaliser les organisations qui auraient opté récemment pour un tel dispositif.

La loi n° 2004-801 du 6 août 2004 avait quant à elle prévu en son article 20 un délai de trois ans pour permettre aux organismes de se mettre en conformité avec les nouvelles dispositions législatives.

Étant donné le délai de la procédure parlementaire, votre commission, à l'initiative de son rapporteur, a choisi d'accorder un délai de trois ans aux responsables de traitement pour se mettre en conformité avec la nouvelle législation.

À l'initiative de son rapporteur, votre commission a donc adopté un **amendement** portant article additionnel prévoyant des mesures transitoires.

4. Les conditions de l'efficacité du dispositif : un renforcement des moyens de contrôle

Il n'en reste pas moins qu'une telle limitation de l'usage des techniques biométriques ne serait **efficace qu'à condition de renforcer considérablement les moyens de contrôle**.

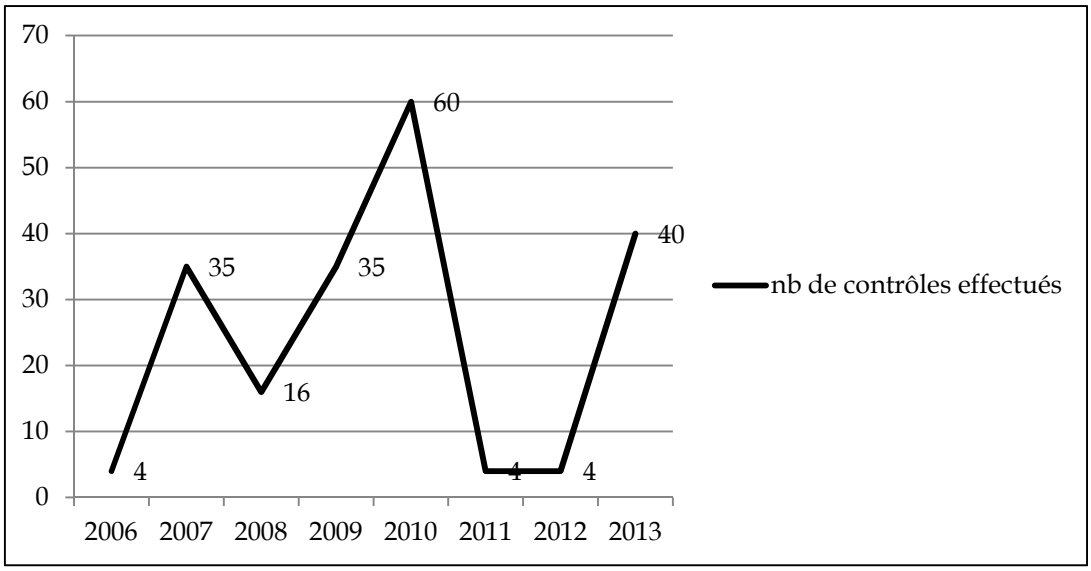
Selon toute vraisemblance, le régime d'autorisation préalable mis en place à partir de 2004 est contourné dans des proportions qu'il est difficile d'évaluer. Ainsi que l'indiquaient à votre rapporteur ses représentants lors de leur audition, la CNIL est amenée, lors de ses contrôles, à connaître de la mise en œuvre de traitements de données biométriques non autorisés. Elle constate par ailleurs que les préconisations contenues dans ses délibérations autorisant la mise en œuvre de certains traitements biométriques ne sont pas toujours suivies. L'obligation, imposée dans certains cas, d'enregistrement des empreintes digitales sur un support individuel détenu par la personne concernée plutôt qu'en base centrale n'est pas, par exemple, systématiquement respectée. Un durcissement des conditions d'utilisation des traitements de données biométriques par une limitation des usages autorisés risquerait d'accroître le nombre de dispositifs « clandestins ».

Or, à l'heure actuelle, dix-huit agents de la CNIL sont affectés à sa mission de contrôle. Si, depuis 2009, un effort accru a été porté à cette mission, l'effectif actuel ne permettrait pas de conduire plus de 450 contrôles par an environ, tous types de contrôle confondus. Ainsi, au cours de l'année 2012, 458 contrôles ont été conduits, dont 285 portant sur des dispositifs relevant de la loi n° 78-17 du 6 janvier 1978 précitée et 173 sur des dispositifs de vidéoprotection[1] ; sur ces 458 contrôles, seulement 4 ont concerné des dispositifs de traitement de données biométriques, dont 2 à la suite de plaintes. En 2013 en revanche, 40 contrôles, soit environ 10 % des contrôles

[1] *Cf. rapport d'activité 2012, Commission nationale de l'information et des libertés, p. 54.*

réalisés, ont porté sur des dispositifs de traitement de données biométriques. Au total, depuis 2006, 198 contrôles ont concerné des dispositifs biométriques, dont 13 % environ sur plaintes, d'après les informations fournies par la CNIL ; ce chiffre rapporté au nombre total d'autorisations délivrées par la CNIL sur la même période, les contrôles auraient donc porté sur 4,5 % des dispositifs.

Évolution du nombre de contrôles de dispositifs biométriques effectués depuis 2006



Source : commission des lois à partir des données fournies par la CNIL

Il convient cependant de remarquer que dans la perspective du règlement européen, la suppression des autorisations préalables permettrait de basculer les efforts vers le contrôle *a posteriori*.

Par ailleurs, la **piste de la certification de procédés industriels, de produits ou de leur implémentation** est probablement une réponse adaptée en présence de technologies évolutives. Votre rapporteur ne peut donc qu'encourager à la poursuite du travail d'ores et déjà entrepris par les pouvoirs publics en concertation avec les acteurs de la filière de la confiance numérique d'élaboration de normes et de standards de haut niveau. À cet égard, votre rapporteur regrette que l'Agence nationale de sécurité des systèmes d'information (ANSSI) n'ait pas été en mesure de donner son avis sur la proposition de loi.

*
* *

La commission des lois a adopté la proposition de loi ainsi modifiée.

EXAMEN EN COMMISSION

M. François Pillet, rapporteur. – La biométrie embrasse l'ensemble des procédés qui identifient un individu à partir de la mesure de l'une ou de plusieurs de ses caractéristiques physiques, physiologiques, voire comportementales : empreintes digitales, ADN, reconnaissance vocale ou iris de l'œil, mais aussi démarche, odeur, dynamique de la signature ou de la frappe sur un clavier. Produite par le corps, la donnée biométrique le désigne ou le représente de façon immuable.

Les catégories pour classer ces techniques évoluent : la distinction entre données « à trace » ou « sans trace » est ainsi bousculée par les progrès réalisés dans le traitement des images et la multiplication des engins vidéo, qui placent désormais la reconnaissance faciale dans les techniques « traçantes ». Ces évolutions peuvent être inquiétantes. Gaëtan Gorce et le groupe socialiste nous invitent à une réflexion particulièrement opportune : il est important que le Sénat se donne une doctrine sur l'usage et la conservation des données biométriques dans la perspective de l'examen prochain du projet de loi sur les libertés numériques.

À l'initiative de la Commission nationale de l'informatique et des libertés (CNIL), le législateur a soumis, par la loi du 6 août 2004, le traitement des données biométriques à un régime d'autorisation préalable. Pour faciliter le travail de la CNIL, l'article 25 prévoit que les traitements identiques peuvent être autorisés par une décision unique : cela concerne par exemple la reconnaissance par le contour de la main pour l'accès au restaurant scolaire. La France s'est ainsi dotée de l'un des régimes les plus protecteurs en la matière, mais sans que le législateur se soit prononcé sur la pertinence des différents usages des techniques biométriques, laissant à la CNIL toute latitude pour élaborer une doctrine.

Or cette dernière est en cours d'évolution. Comme pour toute autre autorisation, l'examen par la CNIL consiste en l'analyse de la proportionnalité eu égard à la finalité envisagée. De 2005 à 2012, la CNIL a distingué les techniques biométriques « à trace », susceptibles d'être capturées à l'insu de la personne, des techniques « sans trace » : contour de la main, reconnaissance vocale, réseau veineux du doigt, iris. À partir de 2013, elle a pris conscience de la faiblesse de cette classification et engagé une réflexion envisageant trois cas : la biométrie de sécurité, indispensable pour répondre à une contrainte de sécurité physique ou logique d'un organisme, imposée à des utilisateurs qui doivent cependant être informés des conditions d'utilisation du dispositif – on peut penser à des exemples comme celui de l'Île Longue ; la biométrie de service ou de confort, reposant sur le libre consentement de l'usager auquel doit être proposé sans contrainte ni surcoût un dispositif alternatif ; les expérimentations, c'est-à-

dire les travaux de recherche fondamentale menés par des laboratoires ou le test de dispositifs avant leur implémentation éventuelle. Adaptant ses exigences aux finalités de chaque traitement, la CNIL ne s'autorise pas à juger de leur pertinence.

L'utilisation de la biométrie se banalise et se répand dans tous les domaines de la vie quotidienne, par exemple pour sécuriser les transactions financières. La proposition de loi peur faire office de première pierre pour construire la réflexion du Sénat. Gaëtan Gorce considère que certains usages, comme dans les cantines scolaires, ne devraient pas être autorisés. Sécurisante par son ergonomie, la biométrie de confort n'est guère rassurante quant à la valeur du consentement des usagers : les parents ont-ils vraiment le choix ?

L'exposé des motifs invite à penser un statut spécifique pour les données biométriques qui ne peuvent bénéficier de la protection de l'article 16-1 du code civil. Le dispositif de la proposition de loi complète l'article 25 de la loi du 6 janvier 1978 qui soumet à autorisation de la CNIL les traitements non étatiques. Les traitements mis en œuvre pour le compte de l'État seraient ainsi exclus du champ de la proposition de loi, qui n'encadrerait que le pouvoir de la CNIL, et non le pouvoir réglementaire. A ce propos, j'attire votre attention sur les nouvelles cartes d'identité, le Conseil constitutionnel n'ayant pas interdit, par sa censure partielle de la loi de 2012, l'usage de la biométrie, mais seulement certains fichiers.

La proposition de loi ne définit pas un statut de la donnée biométrique, elle conditionne l'autorisation de son traitement par la CNIL à une « stricte nécessité de sécurité ». Cette formule pose problème, nous y reviendrons.

Ne sont pas incluses dans le champ de la proposition les activités exclusivement personnelles, comme l'ouverture de sessions sur les nouveaux iPhones, par reconnaissance digitale ou du visage. Cela mérite pourtant que l'on s'interroge.

Quant aux effets de la proposition sur les dispositifs existants, la CNIL estime que toutes les autorisations délivrées jusqu'à présent ne seraient pas reconduites, et que sa nouvelle doctrine ne pourrait être conservée. Enfin, la proposition n'autorise qu'implicitement les expérimentations.

Le problème fondamental est le rôle que nous voulons jouer : le législateur n'a pas saisi en 2004 l'occasion de se prononcer sur les usages légitimes de la biométrie ; j'estime que ce rôle lui revient et qu'il ne peut le laisser à un organisme comme la CNIL, si sérieux soit-il. Or le Gouvernement devrait déposer un projet de loi sur les libertés numériques. Le Conseil de l'Europe s'apprête à réviser la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère

personnel, dite « convention 108 » : son article 6 inviterait le législateur à encadrer le traitement des données biométriques.

Je partage l'objectif de promouvoir un usage raisonné des techniques biométriques, mais avec quelques réserves. Cela peut-il s'articuler avec le règlement européen à venir sur la protection des données à caractère personnel, qui sera d'application directe ? Toute contrainte *a priori* serait supprimée au bénéfice d'un contrôle *a posteriori* renforcé. La résolution législative du Parlement européen du 12 mars 2014 interdit le traitement des données biométriques, en prévoyant des exceptions, en particulier si la personne y a consenti, à moins qu'une disposition nationale y fasse obstacle.

La notion de stricte nécessité de sécurité a semblé insuffisamment précise à de nombreuses personnes entendues lors des auditions. Je souhaiterais qu'elle soit précisée et entendue de façon ni trop large ni trop étroite, ce qui pourrait être contre-productif en incitant les acteurs à acheter des services à l'étranger échappant à la loi française. La notion d'intérêt excédant l'intérêt propre de l'organisme, introduite par une communication de la CNIL de 2007, pourrait y aider. Enfin, pour éviter que certaines dispositions se trouvent hors la loi un dispositif transitoire est nécessaire.

Cette proposition de loi ouvre un débat utile ; j'ai ainsi appris que chaque être humain est unique : ce patrimoine humain doit être protégé. Le Sénat devrait se forger une opinion sur la question et affirmer que l'on ne peut faire n'importe quel usage des données biométriques, même pour des raisons de confort.

M. Gaëtan Gorce. – Merci pour ce rapport exhaustif ; je m'y retrouve, y compris dans les amendements. L'objectif était d'inciter le Parlement à se saisir de ce sujet. Le texte ne concerne que l'accès à des locaux ou des services, alors que l'usage des données biométriques va se développer dans les relations contractuelles : le sujet devrait être examiné en soi. Mon point de vue rejoint celui de François Pillet : tout va bien lorsque l'humain reste maître de la technologie, mais il faut s'interroger et réagir lorsqu'il en devient un rouage.

M. Yves Détraigne. – Je remercie notre rapporteur et l'auteur de cette proposition de loi qui présentent à notre examen une question de plus en plus importante et qui peut menacer la vie privée des individus. Des pays se sont-ils déjà dotés d'une législation dans ce domaine ?

Mme Virginie Klès. – Merci d'attirer notre attention sur ce sujet, et notamment sur la transformation de données « non traçantes » en données « traçantes » par la seule invasion des techniques recourant à la biométrie.

M. Jean-Pierre Sueur, président. – J'avais bien compris la rédaction de la proposition de loi, je comprends moins bien la syntaxe proustienne de votre amendement principal : qu'est-ce donc que l'« accès logique » ?

M. Jean-Jacques Hyest. – Cette proposition de loi se situe dans la continuité des travaux du Sénat sur la carte d'identité, où Virginie Klès et François Pillet s'étaient illustrés. La France a perdu l'avance qu'elle avait en 1978. Il est utile de définir la stricte nécessité de sécurité, même si le président a raison de vouloir une loi bien écrite.

M. François Pillet, rapporteur. – Pour répondre à M. Détraigne : seule la France a commencé à encadrer la biométrie, avec peut-être la Grèce. On remarque d'ailleurs l'influence de notre pays dans la rédaction des textes européens sur le sujet.

M. Yves Détraigne. – Très bien !

M. François Pillet, rapporteur. – Mon amendement, j'en ai bien conscience, reste perfectible – il est loin, en termes de rédaction, de l'article 1382 du code civil… Cependant, si nous en restons à la rédaction actuelle, nous interdisons aussi bien l'accès aux cantines ou aux dojos que, par exemple, l'utilisation de la biométrie pour les transactions financières, qui apporte pourtant de la sécurité aux consommateurs. Les conséquences seraient en outre importantes pour les industries de pointe. Je suis cependant ouvert à toute avancée ; mais ne laissons pas la CNIL seule pour juger de la pertinence d'un système.

Quant à l'objectif « logique », par opposition à l'accès physique, c'est l'accès à des applications informatiques.

M. Jean-Jacques Hyest. – Votre rédaction confond les deux en parlant d'accès physique ou logique à des locaux, équipements, applications ou services.

M. Gaëtan Gorce. – J'avais choisi une rédaction succincte en m'inspirant de la distinction opérée précédemment par la CNIL entre biométries de confort et de sécurité, et de son examen de la proportionnalité : le contrôle de l'accès ne pourrait ainsi utiliser la biométrie que si la sécurité des informations ou des biens le justifie.

Mme Virginie Klès. – Je défends la rédaction du rapporteur : l'accès à une application peut être logique ou physique, comme lorsque l'on touche au disque dur.

EXAMEN DES AMENDEMENTS

Article unique

L'amendement n° 1 est adopté.

M. Jean-Pierre Sueur. – Cet amendement est le fruit d'un effort conceptuel qui mérite d'être poursuivi.

Article additionnel après l'article unique

M. François Pillet, rapporteur. – L'amendement n° 2 crée un dispositif transitoire.

L'amendement n° 2 est adopté et devient un article additionnel.

La commission des lois adopte la proposition de loi dans la rédaction issue de ses travaux.

Le sort des amendements examinés par la commission est retracé dans le tableau suivant :

Auteur	N°	Objet	Sort de l'amendement
Article unique			
M. PILLET, rapporteur	1	Précision – Finalités autorisées pour les traitements de données biométriques	**Adopté**
Article additionnel après l'Article unique			
M. PILLET, rapporteur	2	Institution d'un dispositif transitoire	**Adopté**

LISTE DES PERSONNES ENTENDUES

Commission nationale de l'informatique et des libertés

Mme Sophie Nerbonne, directrice adjointe des affaires juridiques, internationales et de l'expertise

M. Gwendal Le Grand, chef du service de l'expertise informatique

Ministère de la réforme de l'État, de la décentralisation et de la fonction publique

M. Mathieu Jeandron, adjoint au directeur à la direction interministérielle des systèmes d'information et de communication (DISIC)

Entreprises

M. Didier Chaudun, vice-président, Alliance pour la confiance numérique (ACN)

M. Olivier Clémot, *DICTAO*

M. André Delaforge, Natural Security Alliance

M. Laurent Maître, Ingénico

M. Alain Merle, Commissariat à l'énergie atomique (CEA) – LETI

Mme Carole Pellegrino, MORPHO - SAFRAN

M. Pascal Zenoni, THALES

Personnalités qualifiées

Mme Maryse Artiguelong, Ligue des Droits de l'Homme

Mme Meryem Marzouki, chercheure, Centre national de la recherche scientifique (CNRS)

TABLEAU COMPARATIF

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	**Proposition de loi visant à limiter l'usage des techniques biométriques** Article ~~unique~~	**Proposition de loi visant à limiter l'usage des techniques biométriques** Article 1er
Art. 25.— I. — Sont mis en oeuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 : 1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 ; 2° Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en oeuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ; 3° Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en oeuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ; 4° Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ; 5° Les traitements automatisés ayant pour objet : - l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des	Après le II de l'article 25 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, il est inséré un II *bis* ainsi rédigé :	*(Alinéa sans modification)*

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
intérêts publics différents ; - l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ; 6° Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes ; 7° Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ; 8° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes. II. — Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.	« II *bis*. — Pour l'application du 8° du I du présent article, ne peuvent être autorisés que les traitements ~~justifiés par une stricte nécessité de sécurité~~. »	« II *bis*. — Pour l'application du 8° du I du présent article, ne peuvent être autorisés que les traitements ayant pour finalité le contrôle de l'accès physique ou logique à des locaux, équipements, applications ou services 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, à celle des biens ou à celle d'informations dont la divulgation, le détournement ou la destruction porterait un préjudice grave et irréversible. »
III. — La Commission nationale de l'informatique et des libertés se		

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président. Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.		Article 2 *(nouveau)* Les responsables de traitements de données à caractère personnel dont la mise en œuvre est régulièrement intervenue avant l'entrée en vigueur de la présente loi disposent, à compter de cette date, d'un délai de trois ans pour mettre leurs traitements en conformité avec les dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans leur rédaction issue de la présente loi. Les dispositions de la loi n° 78-17 du 6 janvier 1978 précitée, dans sa rédaction antérieure à la présente loi, demeurent applicables aux traitements qui y étaient soumis jusqu'à ce qu'ils aient été mis en conformité avec les dispositions de la loi n° 78-17 du 6 janvier 1978 précitée, dans leur rédaction issue de la présente loi, et, au plus tard, jusqu'à l'expiration du délai de trois ans prévu à l'alinéa précédent.