

Avis n° 98

"Biométrie, données identifiantes et droits de l'homme"

Membres du groupe de travail :

Jean-Claude Ameisen

Sadek Béloucif

Pascale Cossart

Mireille Delmas-Marty

Chantal Deschamps

Chantal Lebatard

Pierre Le Coz

Philippe Rouvillois

Michel Roux

Maxime Seligmann (rapporteur)

Alain-Gérard Slama

Claude Sureau

Mario Stasi (rapporteur)

Personnalités auditionnées :

M. Jean-Louis Bruguière

M. Vianney Dyèvre

M. François Giquel

Sommaire

I – Une approche transformée de l'identité de l'homme

A) La suprématie de la biométrie sur les autres mesures d'identification

B) La disparition de "l'ipséité" au profit de "la mêmeté"

II – Le pouvoir de la biométrie : entre progrès et dérive

A) Les principales finalités de la biométrie

B) Les risques de dérive

III – Vie privée et altérité

IV - Recommandations

L'identification d'une personne s'est depuis toujours fondée sur quelques paramètres morphologiques parmi lesquels la reconnaissance du visage était essentielle. La photographie en a constitué la trace la plus communicable. A la fin du 19ème siècle, certains traits ont même servi pour classer ou prédire tel ou tel comportement.

L'accélération récente du développement des méthodes physiques d'identification de plus en plus sophistiquées, parfois à l'insu des personnes, donne lieu à une tentation collective croissante dont la principale finalité est la sécurité liée à la précision même des paramètres.

C'est cette tension entre ce désir de sécurité qui passe par une identification biométrique sans cesse en perfectionnement et le respect de la dignité des personnes, qui est au coeur de cette auto-saisine du CCNE.

Quel est le prix à payer pour rendre la vie plus sûre ? Quel est le meilleur usage éthique de cette "biométrisation" de l'homme ? La liberté qui se réfugie dans un sentiment de protection individuelle favorisé par l'identification de l'autre, ne constitue-t-elle pas le plus grand leurre qui soit, au moment où la traçabilité technique d'une personne constitue une surveillance déjà inscrite dans les faits ? Certes, l'identification biométrique d'une personne n'a pas pour vocation de la réduire à ses identifiants. Son objectif est de s'assurer qu'une personne qui prétend à telle identité existe bien. Mais, de fait, le glissement de l'identification à celle des comportements et donc de la personnalité, apparaît comme un risque sinon comme une inclination naturelle.

Les trois questions les plus angoissantes sont donc celles du glissement du contrôle de l'identité à celui des conduites, celle de l'interconnexion des données et leur obtention à l'insu des personnes concernées.

I – Une approche transformée de l'identité de l'homme

A) La suprématie de la biométrie sur les autres mesures d'identification

La reconnaissance de son identité, permettant l'affirmation de la singularité du soi, constitue l'un des droits de l'Homme fondamentaux (et en particulier l'un des droits de l'enfant reconnus par la Convention Internationale des droits de l'enfant). Toutefois, la reconnaissance de l'individu par son nom, et éventuellement par sa photographie n'est plus considérée comme suffisante.

Au fil du temps et de l'évolution des moyens et des besoins, les éléments identifiants (nom, prénom accompagnés d'indications relatives au village ou à la région d'origine, à la profession, à des particularités physiques ...) se sont fait plus précis. L'introduction de mesures plus scientifiques permettant une identification plus fiable a progressivement modifié nos relations collectives et individuelles. Nous voulons être reconnus dans la singularité de notre moi, ne pas être confondus avec d'autres mais surtout nous voulons savoir avec certitude si celui à qui nous parlons est bien celui qu'il prétend être.

Aujourd'hui, cette identification passe par un arsenal de paramètres mesurables, de plus en plus nombreux et de plus en plus sophistiqués. Comparés à des bases de données de manière instantanée par des procédés informatiques, ils permettent à la fois de vérifier une identité annoncée et de caractériser, s'il en est besoin, une personne pré-enregistrée. Leur conjugaison confère à l'ensemble un caractère de quasi-infaillibilité et enferme chacun d'entre nous dans un cadre bien défini, la société tendant à s'accommoder de cet enfermement de la personne en une série de données ainsi rassemblées. La pratique a subi une récente accélération avec la montée de la hantise sécuritaire provoquée entre autres par les attentats terroristes. Ce changement d'échelle, cette escalade dans les procédés d'identification représentent, en soi, un sujet de préoccupation.

Les procédés d'identification par la reconnaissance de particularités morphologiques se sont considérablement enrichis : les photographies de la face et les empreintes digitales sont maintenant numérisées facilitant leur stockage et leur accès. A ces techniques classiques, s'est ajoutée une série de procédés plus ou moins fiables et plus ou moins intrusifs : géométrie de la main, réseaux veineux des doigts et du bras, reconnaissance de la rétine et de son réseau veineux, et surtout reconnaissance de l'iris. L'image de l'iris est très complexe mais pratiquement unique pour chaque individu (avec un risque d'erreur estimé à 1 sur 200 milliards) ; elle n'est modifiée ni par l'âge ni par les maladies, ni par les activités professionnelles, et elle n'est pas effaçable. On peut reconnaître l'iris à distance et à l'insu de la personne.

L'utilisation croissante des procédés d'identification par reconnaissance de particularités du comportement (reconnaissance de la voix, de la frappe du clavier, de la démarche) n'a plus seulement pour but de décrire l'individu mais de le définir, de savoir qui il est¹, ce qu'il fait et ce qu'il consomme. A cette utilisation s'ajoute la multiplication des caméras de vidéo-surveillance, la localisation des personnes par l'intermédiaire de leur téléphone portable (ou de la carte Navigo de la RATP) qui, dès lors qu'elles permettent leur parfaite traçabilité, peuvent être considérées comme une mise sous surveillance constante de la liberté d'aller et venir.

¹ Un récent projet européen du 6^{ème} programme cadre (www.humabio-eu.org) a pour but d'étudier de nouveaux paramètres biométriques physiologiques (enregistrements d'électroencéphalogramme, d'électrocardiogramme et d'électrooculogramme), en les combinant entre eux et avec des données identifiantes classiques de manière à obtenir des systèmes d'identification particulièrement performants, en enregistrant ces caractéristiques à l'aide de nouveaux capteurs sans fil, avec le risque d'une obtention à l'insu. Ce projet nous apparaît préoccupant car il a aussi pour ambition de vérifier par ces paramètres physiologiques l'absence de prise d'alcool ou de drogue ou de privation récente de sommeil chez des salariés devant effectuer des tâches telles que transport de fond, pilotage d'avion, manipulation de produits dangereux, tant au départ que pour suivre en permanence leur état de vigilance. L'objectif sécuritaire de cette démarche ne saurait se concevoir bien sûr sans le consentement des intéressés et l'accord de la médecine du travail, mais il doit surtout être mis en balance avec la gravité de l'intrusion dans le champ de la vie personnelle. Ce risque d'instrumentalisation de l'homme à des fins sécuritaires interpelle la médecine du travail qui peut être tentée de transférer sur des masses de données paramétrables la relation avec le salarié, de la même façon que la médecine privilégiant les images et les chiffres a conduit à un risque de déshumanisation de la médecine.

Les méthodes d'identification par analyse de l'ADN prennent une importance croissante, et peut-être démesurée. Certes, les caractéristiques génétiques contenues dans les régions codantes ne sont conservées et utilisées qu'à des fins médicales ou de recherche scientifique, alors que les « empreintes » génétiques utilisées par la Police et la Justice ne concernent que les marqueurs sexuels et des séquences théoriquement non codantes. Les fondements de cette distinction sont peut-être inexacts, et les régions non codantes sont vraisemblablement les plus riches en informations diverses.

Les diverses données biométriques que nous venons d'analyser constituent-elles une véritable identité de l'homme ? Contribuent-elles au contraire à une instrumentalisation du corps et en quelque sorte à une déshumanisation, en réduisant une personne à quelques mesures biométriques ? Cette tentative de réduction biométrique qui ne capturera jamais l'essence de la personne ne peut-elle pas déséquilibrer le regard sur la personne enfermée dans sa "biométrie" au profit de la seule apparence fut-elle scientifiquement déterminée ?

Ne réduisent-elles pas l'homme à une accumulation de données et de critères cartographiques, ceci paradoxalement à l'heure où la biologie, délaissant quelque peu une approche analytique et réductionniste, s'attache à appréhender un système dans sa globalité, en cherchant à intégrer l'ensemble des propriétés d'un organisme ou d'un être vivant (biologie intégrative).

En outre, la généralisation de ces procédés d'identification morphologiques, peut à l'évidence, entraîner une stigmatisation de certaines personnes comme celles vivant avec un handicap et l'exclusion de celles qui ne sont pas aisément paramétrables.

B) La disparition de "l'ipséité" au profit de "la mêmeté"

Cet ensemble de questions invite à une distinction utile, proposée par Paul RICOEUR (*). En effet, le terme « identité » appliqué à un être humain peut désigner en français deux réalités différentes ici en tension. La première concerne son corps dans son objectivité : à travers l'espace et le temps, à travers les lieux et les âges de sa vie, ce corps reste le même, malgré les traces, rides et cicatrices que le temps et les événements lui infligent. Ce premier aspect de l'identité peut être dénommé « mêmeté ». C'est celui que la biométrie permet de cerner : depuis la conception grâce à l'analyse génétique, jusqu'à la mort grâce aux données corporelles identifiantes obtenues de diverses manières - notamment grâce à des particularités morphologiques et à la photographie du visage.

L'autre réalité concerne le vécu d'existence, par un sujet humain conscient et réfléchi. C'est le « soi-même », en anglais le « *self* ». On peut la désigner, pour la distinguer de la précédente, par le terme « ipséité », tiré du latin « *ipse* », c'est-à-dire le soi comme sujet réfléchi. Cette réalité est certes subjective, mais c'est elle qui importe d'un point de vue éthique, car c'est elle qui rend possible l'exercice de la liberté. Notre perception de la dignité humaine est inséparable de cette dimension intérieure et biographique que l'on appelle *l'ipséité*. De ce point de vue, c'est le corps-sujet et non seulement le corps-objet qui est en cause, le corps tel qu'il se vit de l'intérieur et non pas tel qu'il se voit de l'extérieur. C'est à *l'ipséité* que nous rapportons nos expériences affectives et le sentiment intime de demeurer le même du début à la fin de notre vie. C'est en ce sens que Ricoeur dit de *l'ipséité* qu'elle est le "maintien de soi de l'individu à travers les aléas événementiels qui construisent son histoire".

Ce n'est pas non plus dans un corps objectivable mais dans sa chair que l'homme fait l'expérience de sa vulnérabilité, et de sa condition mortelle. Il cherche de diverses manières à protéger son « ipséité », son identité personnelle avec toute la valeur qu'il y attache. Il le fait notamment, en créant et en adoptant dans la vie sociale des espaces d'accès à lui-même, des zones d'intimité. La première d'entre elles est l'intimité corporelle, protégée par des règles de pudeur – règles qui sont levées dans certaines conditions de soins familiaux ou médicaux. Ou encore l'intimité sexuelle, qui s'ouvre au partenariat consenti dans certaines conditions. Au-delà de cette zone corporelle première, on notera de même d'autres zones de protection, car chaque groupe d'appartenance ou d'intérêt crée ses propres limites et délimite une zone de communication interne acceptée et une communication externe contrôlée. A chaque groupe ses « secrets », qui sont en réalité une condition de la libre communication.

(*) Paul RICOEUR, *Soi-même comme un autre*, Ed. du Seuil 1990, pp.39-54 :« La personne et la référence identifiante »

Le groupe social le plus large – en deçà de la commune humanité – est dans nos sociétés celui qu’incarne l’Etat. Il est généralement admis que, en vue des services qu’on attend de lui, l’Etat reconnaisse ses propres membres grâce à des données identifiantes extérieures, qui sont des données corporelles en quelque sorte rendues publiques, celles que nous appelons « état civil ». Elles sont rattachées au nom propre. Elles permettent d’identifier dans l’espace public chaque citoyen par sa « mêmeté » et de le désigner : « c’est bien lui ». Mais respectent-elles toujours l’« ipséité », qui est au fondement de sa liberté ? N’ont-elles pas tendance à la dissoudre dans une collection de données numériques et paramétrées ?

Quand se multiplient et se diversifient ces données, et que celles qui sont relatives à l’intimité et à la fragilité corporelles viennent s’entrecroiser avec celles d’autres zones de la vie sociale, elles même connues par d’autres intervenants à travers d’autres données liées à des comportements divers et recherchées pour d’autres intérêts, on s’interroge légitimement sur l’espace de liberté laissé à la personne, dans son « ipséité ». Là est la question éthique centrale.

II – Le pouvoir de la biométrie : entre progrès et dérive

A) Les principales finalités de la biométrie

A la diversité des procédés d’identification correspond une diversification des finalités. On doit établir une distinction entre les utilisations qui sont faites des données identifiantes selon :

- Qu’elles ont pour finalité la sécurité publique entendue dans son sens large et sont aux mains d’autorités constituées (Justice, Police).
- Qu’elles ont pour but la santé publique
- Qu’elles ont trait à la recherche médicale et scientifique
- Qu’enfin leur usage est d’ordre privé (purement individuel, collectif à l’intérieur d’une entreprise ou commercial par exemple).

Ces utilisations peuvent être considérées comme s'exerçant au profit de la personne ou à son détriment, comme au profit de tiers ou à leurs dépens, ce qui peut amener à opposer au moins en apparence un intérêt individuel à l'intérêt de la société.

Cartes d'identité et passeports recourent de plus en plus souvent aux techniques de la biométrie et de l'électronique, afin d'éviter la fraude et l'usurpation d'identité, et permettre l'authentification. Dans ce domaine, des règles nationales peuvent, dans ce contexte de la mondialisation, être dépourvues de tout caractère opératoire par l'ignorance des législations étrangères, et par la même, écartées.

Plus préoccupante, se révèle l'exigence des autorités américaines du transfert par les Compagnies aériennes Européennes de plus de trente données identifiantes - dont certaines cherchant à savoir ouvertement « qui vous êtes » (préférences alimentaires, utilisation d'un fauteuil roulant, cartes de crédit, etc.).

Les techniques biométriques sont également utilisées dans le cadre de procédures judiciaires. Le juge civil y a recours, en particulier dans le cadre d'une action tendant à la contestation ou à l'établissement d'un lien de filiation*. L'absence assez générale, sauf en France et en Belgique, de contrôles sur les laboratoires pratiquant ces recherches, alors que les offres pullulent sur Internet, est préoccupante.

* La France est l'un des seuls pays où l'expertise biologique en matière de filiation est sous le contrôle d'un juge

Dans le domaine pénal, seules les empreintes génétiques des personnes condamnées pour infraction à caractère sexuel dont certaines atteintes aux mineurs pouvaient initialement être conservées en France. Mais le prélèvement et la conservation d'ADN ont récemment été élargis à « toute personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis un délit », dont la liste exhaustive comporte les « dégradations, détériorations, et menaces d'atteinte aux biens ». Cette extension ne saurait être présentée dans bien des cas comme nécessitée par un besoin de sécurité (est-il indispensable de relever l'ADN des faucheurs d'OGM ?). S'il s'agit d'initier une pratique de prélèvements généralisés à toute une population, il n'est nul besoin de prendre comme prétexte l'infraction à quelque règle que ce soit. En ce domaine plus qu'en d'autres, la finalité des pratiques doit être clairement définie.

La gestion et le contrôle de la couverture sociale des risques de santé nécessitent l'utilisation de données identifiantes avec des outils informatiques adaptés. La carte Vitale est conçue pour améliorer la continuité et la qualité des soins, comme élément important dans le traitement des urgences et comme moyen d'accès au dossier médical informatisé et personnalisé que l'on prévoit de généraliser. La nature des informations identifiantes qu'elle pourrait légitimement contenir et qui ferait d'elle une véritable carte d'identité médico-sociale pose des problèmes délicats. Des procédés de masquage (et de masquage du masquage) devraient pouvoir être autorisés même si cela peut aboutir à une perte de chances sur le plan médical. Cette carte ne saurait en aucun cas être liée à la carte d'identité informatisée dont les seules finalités doivent demeurer celles de la sécurité et de l'ordre public. Le numéro de Sécurité Sociale ne devrait pas non plus servir d'identifiant généralisé, permettant en particulier d'accéder au dossier médical ou à des informations couvertes par le secret médical.

Dans le domaine de la recherche médicale et scientifique, des problèmes assez proches se posent avec une acuité toute particulière pour les collections de données qui prennent, avec l'apparition des banques médicales, une dimension sans précédent, en raison du nombre des informations susceptibles d'être recueillies, et de la grande diversité des usages qui peut en être fait. En effet, ce n'est pas tellement de la biométrie en tant que telle qu'il s'agit, mais de l'intégration des données biologiques dans un système complexe comportant des données d'ordre comportemental, psychologique, etc. Le CCNE, en son avis 77, insistait sur la nécessité d'anonymisation au détriment parfois de données scientifiquement intéressantes.

Les thèmes de l'identification et de la surveillance sont omniprésents dans les usages actuels de la biométrie de la part tant des personnes privées que des entreprises.

Le contrôle de l'accès aux sites qui jusqu'à présent concernait principalement la présence et la localisation physique de l'individu s'étend désormais à l'utilisation des outils informatiques.

Le développement de ces techniques ne se limite pas aux usages impliquant des tiers, dont il y aurait lieu de vérifier l'identité. La biométrie pénètre la vie quotidienne de chacun, offrant une grande variété de procédés, de l'ouverture des coffres au démarrage des véhicules, mais aussi relevant certains aspects de notre comportement (par exemple nature des ouvrages consultés dans une bibliothèque, ou habitudes d'achats dans votre supermarché).

On observe au total une extrême diversité des usages des données identifiantes dans le domaine des activités privées ou commerciales:

- pour soi-même dans la vie quotidienne
- pour des finalités de sécurité générale: c'est le cas des cartes bancaires pour combattre les usages frauduleux qui peuvent en être faits.

- dans les relations d'une entreprise avec ses clients, à la fois pour les identifier dans un souci de sécurité et pour leur faciliter l'accès aux services.
- dans les relations d'un employeur avec ses salariés, qu'il s'agisse de contrôler l'accès aux locaux ou d'organiser des fichiers du personnel, lesquels sont au demeurant interdits.

On est en droit de se demander si une entreprise privée, qui n'est pas soumise à contrôle comme les autorités administratives, peut exiger le recueil de certaines données biométriques comportant un caractère intrusif avec tous les risques que cela comporte, que ce soit au niveau de l'embauche ou pendant la durée du travail (risques d'exclusion, de discrimination ou d'atteinte à la vie privée).

B) Les risques de dérive

Lors du recueil des données, la finalité doit être précisément indiquée, explicitée et justifiée, ce qui exige que soit indiquée avec précision l'autorité ou l'organisme qui procède à son recueil.

L'exigence du consentement est un élément essentiel lors de la collecte des données biométriques. Elle est bafouée lorsque la donnée identifiante est recueillie à l'insu de l'intéressé (photographie de l'iris à distance, enregistrement électrique à distance) ou lorsque le consentement n'est pas demandé comme en Angleterre, lors d'un prélèvement d'un cheveu, d'ongle ou de salive. En France, bien que sa nécessité pour un prélèvement d'empreintes génétiques soit prévue par l'article 16 du Code Civil (et plus particulièrement les articles 16.10 et 16.11), elle a été récemment remise en cause par une loi qui fait du refus de se soumettre à ce prélèvement un délit. C'est la notion même de consentement qui disparaît ce qui devrait normalement conduire à une plus grande prudence et une plus grande rigueur dans la pratique des prélèvements, dans l'utilisation des données identifiantes et dans leur conservation.

Un strict respect de la finalité recherchée est essentiel, et toute confusion entre identification et information sur la personne doit être évitée. En effet, nombre de données peuvent être utilisées à d'autres fins que celles pour lesquelles elles ont été initialement réunies, permettant un contrôle étroit et multiforme des personnes, de leurs déplacements et de leurs activités.

La durée de conservation des empreintes génétiques est en France de 40 ans pour les personnes condamnées, et de 25 ans dans les autres cas. Elle est de 100 ans en Angleterre. Cette conservation sans limites, sans contrôles, et sans possibilité de retrait à la demande de l'intéressé est en contradiction avec les concepts de prescription ou d'amnistie. En outre, si la preuve apportée d'une culpabilité peut justifier la constitution d'une sorte de banque de données identifiantes en forme de casier judiciaire, rien ne saurait justifier la conservation de ces données s'agissant de prélèvements pour des personnes ultérieurement jugées innocentes.

Dès lors, il ne saurait plus être question du respect d'une quelconque finalité elle-même justifiable, mais d'une accumulation, d'un stockage de données "à toutes fins utiles" qui rende possible une recherche discriminatoire à partir de ce stockage, une pratique d'exclusion, ou un regroupement à des fins ambiguës. Ainsi, l'usage de données biométriques qui pourraient être reliées à l'identification de minorités ethniques, ou leur détournement à des fins politiques, sont particulièrement source d'inquiétude. On imagine aisément l'utilisation aux fins de stigmatisation, d'exclusion sinon d'élimination que des régimes totalitaires auraient pu faire ou pourraient faire de tels instruments ainsi mis à leur disposition...

Le fichier des empreintes génétiques de la Police Anglaise porte sur près de 4 millions de personnes, et, dans une récente enquête, le comité Nuffield de bioéthique se demande si la collecte de DNA de tous les nouveau-nés anglais ne serait pas plus équitable... En revanche, le Parlement Européen et un groupe de travail de la Commission Européenne avaient refusé en 2005 la création d'une banque centralisée des données biométriques des passeports de tous les ressortissants de l'Union Européenne en considérant que ce projet n'était pas conforme au principe de la proportionnalité des moyens.

La notion de proportionnalité des moyens est en effet essentielle à prendre en considération puisque intégrer des données personnelles au-delà de ce qui est nécessaire à la finalité déclarée ne saurait en aucun cas être considéré comme éthique.

Cette asymétrie des buts et des moyens met en relief les enjeux réels qui sont ceux d'une surveillance accrue des conduites humaines au nom de leur protection.

La validation des données doit être scrupuleuse, car le recours contre d'éventuelles erreurs risque d'être problématique. De même, le contrôle de l'accès aux données doit être très rigoureux pour éviter toute rupture de confidentialité, tout vol frauduleux et tout détournement de données dites sensibles.

Enfin, la collusion entre données publiques et privées représente un risque majeur, et tout mixage doit être rejeté. Par exemple, le croisement de bases de données les unes administratives, et les autres ayant trait à la santé peut entraîner de graves discriminations dans le domaine des assurances ou de l'emploi en particulier au moment de l'embauche. Il suffit pour s'en convaincre de songer à la systématisation actuelle de l'usage des moteurs de recherche électronique par les employeurs et les recruteurs.

Le contrôle de l'accès aux données et le risque de mixage ne sont pas l'apanage des bases de données informatisées. Ils existent lorsque des données, souvent à la fois publiques et privées, sont stockées dans des puces électroniques, sur support externe et lisibles sans contact, ou implantées dans le corps de l'individu pour des applications des plus variées (suivi des personnes en liberté conditionnelle, sécurité dans les transports, accès à des discothèques...).

La généralisation des RFID (Radio Frequency Identification) qui se substituent au code barre donne une dimension spectaculaire à la biométrie par leur miniaturisation, leurs possibilités infinies d'interrogation à distance et leur usage commercial banalisé par leur faible coût².

Un contrôle rigoureux de l'accès aux données est aussi nécessaire dans le cadre des collections de données médicales ou génétiques, pour lesquelles le CCNE, dans son avis n° 77^{*}, a évoqué le rôle crucial du curateur^{**}.

L'extension de ces pratiques, avec les risques croissants de dérives qu'elles comportent, entraîne immanquablement la nécessité de créer des organismes de contrôle effectifs, tant de la légitimité de recueil des données et des finalités déclarées que du respect de ces finalités, avec exclusion de toute collusion à l'évidence contraire aux libertés. L'existence de ces organismes de contrôle devra s'accompagner de possibilité de recours par les individus concernés, malheureusement bien illusoire quand on connaît le recueil à l'insu.

On observera que la situation ainsi décrite ne se limite bien évidemment pas aux frontières d'une nation et que cette protection devra être internationale pour éviter les dérives et leurs conséquences pour les libertés.

² Michel Alberganti. Sous l'œil des puces. La RFID et la démocratie. Actes Sud, 2007

^{*} Avis n° 77 sur les problèmes éthiques posés par les collections de matériel biologique et les données d'information associées : "biobanques" "biothèques" – Rapport – 20 mars 2003 + Document commun Comité d'éthique français (CCNE) et Comité d'éthique allemand (NER) sur les problèmes éthiques posés par les collections de matériel biologique et les données d'information associées : "biobanques" "biothèques"

^{**} L'exemple de l'Islande illustre le risque d'identification à partir du croisement de bases de données anonymisées. Il existe pour toute la population islandaise trois bases de données toutes anonymisées. Celle des données médicales inclut les individus post-mortem; celle des données généalogiques comporte l'indication de la profession et du lieu de résidence; la troisième concerne les données génétiques. Leur croisement permet d'aboutir à une identification qui pose potentiellement des problèmes de filiation. C'est une des raisons pour laquelle la Cour Suprême d'Islande a déclaré en 2003 son inconstitutionnalité, avec des implications internationales pour les grandes collections prévues en Europe.

III - Vie privée et altérité

Indépendamment de ces dérives, à l'évidence condamnable, la biométrie entraîne par elle-même une exaltation de données individuelles au détriment des valeurs sociétales. Chaque personne doit être tatouée, marquée, au nom d'un intérêt collectif. On passe insensiblement d'une identité- droit de l'individu à une identification-obligation ou devoir social. La sécurité dite collective dicte ses exigences au nom des libertés.

Comment la société réagit-elle à ce processus de sécurisation dans lequel elle s'est engagée ? On observe que si au nom de la sécurité collective, chacun admet que l'autre fasse l'objet de ces marquages qui le rassurent, celui-là qui en cherche le bénéfice répugne à en subir les contraintes. Chacun redoute l'autre; il est favorable à la mise en jeu de toutes les mesures qui permettent de l'identifier et même de l'authentifier, mais lui-même supporte assez mal l'intrusion croissante des appareils de surveillance dans sa vie. Il est conscient sans doute de ce en quoi elles peuvent porter atteinte au respect de sa propre vie privée. Ainsi, notre sentiment inné d'élan vers l'autre est menacé soit de rejet plus ou moins rationnel, soit de compassion pour cet être que j'ai la chance de ne pas être. Le souci de l'autre ne passe pas par la biométrie.

Une société qui passe de la vigilance à la surveillance met en jeu, au prétexte d'une demande croissante de sécurité collective, les libertés individuelles et le droit à l'anonymat et au secret. La collecte des données biométriques identifiantes risque de comporter une atteinte majeure à la vie privée, et pourrait donc aussi ne pas respecter l'article 8 de la convention des Droits de l'Homme qui stipule que « toute personne a droit au respect de sa vie privée et familiale ».

Du fait du paradoxe soulevé entre protection de la vie privée et atteinte à la vie privée, on assiste à une sorte de confiscation consentie de liberté. Subrepticement, notre société, au nom du paradigme sécuritaire, s'habitue à l'usage de ces marqueurs biométriques et chacun accepte finalement et même avec quelque indifférence d'être fiché, observé, repéré, tracé, sans souvent

même en avoir conscience.

La médecine peut, là encore, à son insu, aider à donner des informations d'ordre médical susceptibles d'être utilisées par la police ou la justice. D'une façon générale ce sont toutes les autorités administratives qui sont concernées par l'essor et l'affinement des outils de conversion électronique, à commencer par l'administration hospitalière elle-même.

La question fondamentale est celle de l'interconnexion des dossiers, qui est une tentation normale de tout système informatique. Les moteurs de recherche fonctionnent sur ce principe. Ce n'est pas tant les paramètres de la biométrie qui sont en cause que leur connexion que l'on doit empêcher à tout prix, sauf dérogation admise par une autorité judiciaire.

En résumé, l'utilisation universelle de la biométrie pour définir l'identité des personnes se développe irrésistiblement et en apparence inéluctablement pour des besoins affirmés d'une sécurité accrue et selon des évolutions technologiques constantes présentées comme des progrès. La première interrogation d'ordre éthique résulte de ce caractère ressenti comme inéluctable sans que se soit instauré un débat public et sérieux sur les risques que peut comporter cette évolution et les dérives auxquelles elle expose.

Il est significatif à ce sujet que ceux-là même qui ont recours à ces techniques de plus en plus sophistiquées et performantes affirment, lorsqu'on les interroge, que rien ne justifie qu'ils y apportent eux-mêmes des limites. Toutefois, ils vont jusqu'à inviter eux-mêmes à une prise de conscience collective qu'en l'état seul un débat public peut faire naître, sauf à laisser dans l'indifférence générale le développement de la technologie et son utilisation à des fins sécuritaires empiéter sur la protection de la vie privée et les libertés fondamentales.

C'est la dérive inhérente à la biométrie elle-même qui doit conduire à une réflexion sur sa nature et renforcer l'encadrement qu'une société consciente de ses devoirs vis-à-vis de ses membres doit s'imposer à elle-même.

Il ne s'agit pas là d'un débat théorique ou tout simplement dépassé. Il n'est nullement certain en effet que la sécurité collective soit mieux assurée en un monde où serait encouragée toute forme d'exclusion au détriment d'une solidarité élémentaire. Il est grand temps de redonner son sens véritable à la biométrie et faire ainsi de la technologie un instrument de réel progrès au lieu d'une arme souvent inadaptée et par là même contraire au but qu'elle s'assigne.

En conclusion, le CCNE s'inquiète de la généralisation du recueil d'informations biométriques et des risques qu'elle comporte pour les libertés individuelles. Ces risques sont d'autant plus préoccupants qu'ils sont démultipliés par la montée en puissance de nouvelles technologies destinées au recueil et à la transmission de données personnelles, qui représentent un danger accru pour les libertés. En effet les méthodes modernes de recueil se fondent sur de nouvelles générations de puces électroniques capables de recueillir et de stocker de grandes quantités de données et de les transmettre très efficacement par télémétrie.

Malgré leur apparente neutralité, ces données – notamment celles comportant des paramètres physiologiques ou psychologiques révélatrices de l'identité, des goûts ou de l'état de santé des personnes - peuvent être détournées en vue d'une surveillance abusive des comportements. En se fondant par exemple sur une analyse des préférences alimentaires des voyageurs ou des clients de grandes surfaces, il est possible de tirer des informations concernant les croyances personnelles de consommateurs, ou d'autres éléments susceptibles de servir à des études de marché, à leur insu, sans leur consentement et à l'encontre de leur intérêt, donc dans des conditions éthiquement injustifiables.

Ce risque de détournement est encore aggravé par la possibilité de transmettre de telles données par des techniques performantes de télémétrie qui ne garantissent nullement leur confidentialité et n'offrent aucune protection contre une utilisation illégitime. Le passeport biométrique récemment mis en service dans 27 pays d'Europe et d'Amérique illustre bien les risques d'abus de la

télémetrie: des expertises convergentes réalisées par des sociétés de sécurité informatique et par le groupe Fidis (Futur de l'identité dans la société de l'information) pour le compte de l'Union Européenne ont montré que la confidentialité des données transmises à partir des puces électroniques intégrées au passeport biométrique était illusoire.

La généralisation, la centralisation et la divulgation, même accidentelle, d'informations biométriques comportant des indications d'ordre personnel doit donc impérativement être efficacement encadrée, afin d'éviter qu'elles ne réduisent l'identité des citoyens à une somme de marqueurs instrumentalisés et ne favorise des conditions de surveillance attentatoires à la vie privée.

IV - Recommandations

Compte tenu de cette analyse, le CCNE recommande:

- d'assurer un strict respect des finalités liées au recueil de chaque type de données, en définissant clairement les organismes ou les autorités habilités à y procéder;
- un contrôle étroit, sous la responsabilité des autorités judiciaires et de la CNIL, de tout recours systématique à des identifiants communs, et une interdiction de l'interconnexion des fichiers présentant des identifiants communs mais destinés à des finalités différentes. En particulier devrait être interdit tout regroupement de données susceptibles d'entraîner des stigmatisations, ou des discriminations à l'embauche, dans la mesure où de tels regroupements favorisent une biométrie de l'exclusion en visant préférentiellement les personnes les plus vulnérables. Sans méconnaître les difficultés que rencontre la mise en œuvre effective d'une telle interdiction pour les fichiers détenus par des organismes privés, son respect n'en doit pas moins être rappelé, et son exécution doit au moins être imposée pour tous les fichiers détenus par des organismes publics ;

- le placement des fichiers d'empreintes génétiques sous le contrôle d'un magistrat du siège hors hiérarchie, assisté en tant que de besoin d'autres magistrats ;
- une stricte application des dispositions relatives au consentement préalable au recueil des données, ainsi qu'une limitation effective de tout recueil effectué à l'insu des intéressés ;
- que soit solennellement réaffirmée la légitimité du secret protégeant l'intimité de la personne, et en particulier ses aspects corporels, familiaux ou sexuels ;
- d'engager une réflexion approfondie sur l'usage des puces électroniques et des moyens de transmission télémétriques. Ce thème de réflexion qui va bien au-delà de la biométrie rend nécessaire une Autorité qui puisse établir avec précision la liste des conditions dans lesquelles ces techniques ne devraient en aucun cas être utilisées ;
- de ne pas négliger pour autant la protection des personnes ne figurant dans aucun fichier, et qui pour cette raison ne doivent pas pour autant voir leur statut paradoxalement réduit à celui d'une «mort citoyenne».

Le CCNE estime indispensable la mise en œuvre d'un réel contre-pouvoir face à la généralisation excessive de la biométrie. Pour être performants, des dispositifs capables de protéger les libertés citoyennes devraient s'appuyer sur des instances indépendantes de lutte contre d'éventuelles dérives technocratiques, économiques, policières ou politiques liées à l'exploitation des données biométriques. La CNIL, qui représente en France un exemple d'instance répondant à ces critères, devrait se voir conférer le statut et les moyens permettant de mieux garantir son efficacité et son indépendance. Ces instances devraient également être coordonnées à l'échelle européenne.

Enfin, le CCNE invite à un débat public sur la généralisation abusive du recueil de données identifiantes et leurs implications éthiques. Destiné à favoriser une prise de conscience

collective sur la nature des dérives et la nécessité d'un encadrement effectif, ce débat devrait être organisé en collaboration avec d'autres comités d'éthique, de manière à lui donner la dimension internationale qui convient au traitement d'un problème touchant étroitement aux droits et à la dignité de l'homme.

Le 26 avril 2007

ANNEXE I

DISPOSITIONS FRANCAISES RELATIVES AU PRELEVEMENT DES EMPREINTES GENETIQUES EN MATIERE PENALE

Les articles 706-54 à 706-56 du Code de procédure pénale établissent les règles de fonctionnement du **fichier national automatisé des empreintes génétiques (FNAEG)** destiné à centraliser des empreintes génétiques en vue de l'identification des auteurs d'infraction.

Le fichier des empreintes génétiques est placé sous le contrôle d'un magistrat du Parquet hors hiérarchie nommé par le Garde des Sceaux pour trois ans. Il est assisté d'un comité de trois membres nommés dans les mêmes conditions. Le magistrat et les trois membres ont un accès permanent au fichier. Le magistrat peut ordonner toutes les mesures nécessaires à ce contrôle telles que des saisies ou copies d'informations. Ces pouvoirs s'exercent sans interférer avec ceux de la Commission Nationale de l'Informatique et des Libertés.

LES PERSONNES CONCERNEES

- Le prélèvement des empreintes génétiques est réalisé sur des personnes condamnées mais aussi sur celles à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblables qu'elles aient commis l'une de ces infractions visées à l'article 706-55 du Code de procédure pénale.

"Le fichier national automatisé des empreintes génétiques centralise les traces et empreintes génétiques concernant les infractions suivantes:

1° Les infractions de nature sexuelle visées à l'article 706-47 du présent code ainsi que le délit prévu par l'article 222-32 du code pénal;

2° Les crimes contre l'humanité et les crimes et délits d'atteintes volontaires à la vie de la personne, de torture et actes de barbarie, de violences volontaires, de menaces d'atteintes aux personnes, de trafic de stupéfiants, d'atteintes aux libertés de la personne, de traite des êtres humains, de proxénétisme, d'exploitation de la mendicité et de mise en péril des mineurs, prévus par les articles 221-1 à 221-5, de 222-1 à 222-18, de 222-34 à 222-40, 224-1 à 224-8, 225-4-1 à 225-4-4, 225-5 à 225-10, 225-12-1 à 225-12-3, 225-12-5 à 225-12-7 et 227-18 à 227-21 du code pénal;

3° Les crimes et délits de vols, d'extorsions, d'escroqueries, de destructions, de dégradations, de

détériorations et de menaces d'atteintes aux biens prévus par les articles 311-1 à 311-13, 312-1 à 312-9, 313-2 et 322-1 à 322-14 du code pénal.

4° Les atteintes aux intérêts fondamentaux de la nation, actes de terrorisme, la fausse monnaie et l'association de malfaiteurs prévus par les articles 410-1 à 413-12, 421-1 à 421-4, 442-1 à 442-5 et 450-1 du code pénal;

5° Les crimes et délits prévus par l'article 2 de la loi du 24 mai 1834 sur les détentions d'armes ou de munitions de guerre, l'article 3 de la loi du 19 juin 1871 qui abroge le décret du 4 septembre 1870 sur la fabrication des armes de guerre et les articles 24 à 35 du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions;

6° Les infractions de recel ou de blanchiment du produit de l'une des infractions mentionnées aux 1° à 5°, prévues par les articles 321-1 à 321-7 et 324-1 à 324-6 du code pénal. "

- En outre, le prélèvement des empreintes génétiques est réalisé sur des personnes à l'encontre desquelles il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis un crime ou un délit.

LA NECESSITE DU CONSENTEMENT ET LA SANCTION DU REFUS

- Le consentement est exigé pour les prélèvements effectués sur les personnes suivantes:
 - Personnes condamnées pour l'une des infractions mentionnées à l'article 706-55 (706-54 alinéa 1)
 - Personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions mentionnées à l'article 706-55 sont également conservées dans ce fichier (706-54 alinéa 2)
 - Personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis un crime ou un délit, avec les données incluses au fichier, sans toutefois que cette empreinte puisse y être conservée. (706-54 alinéa 3)
- Toutefois, le **fait de refuser de se soumettre au prélèvement biologique** constitue un **délit** prévu par l'article 706-56, II° CPP (depuis la loi du 9 mars 2004 dite « Perben II »). La sanction est différente suivant que l'auteur a été condamné pour un délit (un an d'emprisonnement et 15000 euros d'amende) ou pour un crime (2 ans d'emprisonnement et 30.000 euros d'amende). Lorsqu'il s'agit d'une personne condamnée pour crime ou pour un délit puni de dix ans d'emprisonnement. (article 706-56)

PRELEVEMENT ET TRANSMISSION DES SCELLES

La collecte et le prélèvement des traces et échantillons biologiques sont assurés par les OPJ. L'officier de police judiciaire qui procède au prélèvement peut requérir toute personne habilitée ayant fait l'objet d'un agrément. Les traces sont collectées par les enquêteurs soit dans le cadre de l'enquête préliminaire ou de flagrance, soit sur commission rogatoire. Pour les personnes visées aux 1^{er}, 2^{ème} et 3^{ème} alinéa de l'article 706-54 (personnes condamnées et soupçonnées) l'officier de police judiciaire chargé de l'enquête procède ou fait procéder au prélèvement biologique. Il peut préalablement vérifier ou faire vérifier par un APJ que l'empreinte n'est pas déjà enregistrée. (article 706-56, I).

Lorsque le prélèvement n'a pas été effectué au cours de procédure d'enquête, d'instruction ou de jugement, il est réalisé, pour les personnes condamnées, sur instruction du Procureur de la République ou du Procureur général, au plus tard dans un délai d'un an à compter de l'exécution de la peine.

(article R. 53-21)

Les scellés sont adressés au service central de préservation des prélèvements biologiques en vue de leur conservation sur décision du Procureur, de l'OPJ ou du juge d'instruction.

(article R. 53-20)

CONTENU DU FICHER (FNAEG)

L'article 706-54 alinéa 5 CPP dispose que « *les empreintes génétiques conservées au fichier ne peuvent être réalisées qu'à partir de segments d'acide désoxyribonucléique (ADN) non codants, à l'exception du segment correspondant au marqueur du sexe* ».

Or, il n'est pas possible d'extraire à partir de segments dits « non codants » d'ADN des informations physiologiques, morphologiques ou héréditaires, hormis le marqueur du sexe. Il s'agit donc, en interdisant l'utilisation de segments « codants », de ne pas faire apparaître dans un fichier automatisé des données sensibles portant sur des caractéristiques physiques ou sur des anomalies génétiques.

L'article R.53-13 CPP précise que le nombre et la nature des segments d'ADN non codants sur lesquels portent les analyses d'identification par empreintes génétiques sont déterminés par arrêté interministériel. C'est ainsi l'article A.38 CPP qui fixe, selon la nomenclature internationale, le tableau des segments pouvant être utilisés.

Il est à noter que le fonctionnement du fichier consiste à la fois en la conservation, sous forme de scellés, des traces et échantillons prélevés, mais aussi en la conservation des résultats des analyses réalisées à partir de ces prélèvements.

CONSERVATION ET EFFACEMENT DES DONNEES

Les empreintes prélevées sur les personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions mentionnées à l'article 706-55 sont effacées sur instruction du procureur de la République agissant soit d'office, soit à la demande de l'intéressé, **lorsque leur conservation n'apparaît plus nécessaire compte tenu de la finalité du fichier**. Lorsqu'il est saisi par l'intéressé, le procureur de la République informe celui-ci de la suite qui a été réservée à sa demande ; s'il n'a pas ordonné l'effacement, cette personne peut saisir à cette fin le juge des libertés et de la détention, dont la décision peut être contestée devant le président de la chambre de l'instruction. (706-54 alinéa 2 et R.

53-13-1 à R. 53-13-6)

En tout état de cause, elles ne peuvent être conservées au-delà d'une durée de **vingt-cinq ans** à compter de la demande d'enregistrement, si leur effacement n'a pas été ordonné antérieurement dans les conditions prévues par les articles R. 53-13-1 à R. 53-13-6. Cependant, si la personne a fait l'objet d'une décision de classement sans suite, de non-lieu, de relaxe ou d'acquiescement exclusivement fondée sur l'existence d'un trouble mental en application des dispositions du premier alinéa de l'article 122-1 du code pénal, le procureur de la République en informe le gestionnaire du fichier et ces résultats sont conservés pendant quarante ans à compter de la date de cette décision. » (R. 53-14, alinéa 2)

Les empreintes prélevées sur les autres personnes ne peuvent être conservées au-delà d'une durée de **quarante ans** à compter, soit de la demande d'enregistrement, soit du jour où la condamnation est devenue définitive ou, si cette date n'est pas connue du gestionnaire du fichier, du jour de la condamnation, lorsqu'il s'agit des résultats des analyses d'identification par empreintes génétiques des échantillons biologiques prélevés sur des personnes définitivement condamnées pour l'une des infractions mentionnées à l'article 706-55. (R. 53-14, alinéa 1)

A l'expiration du délai de quarante ans, il est procédé à la destruction des scellés.
(article R. 53-20)

Les informations transmises au service central pourront faire l'objet d'un traitement informatisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Ce traitement informatisé ne pourra en aucun cas, contenir des résultats d'analyses d'identification par empreintes génétiques.
(article R. 53-20)

Aucune disposition relative au FNAG ou à l'amnistie ou à la réhabilitation n'est prévue pour la destruction des scellés ou l'effacement des données lorsque la personne condamnée a bénéficié d'une amnistie ou d'une réhabilitation.

ANNEXE II

LA SITUATION AU ROYAUME UNI

Les bases de données sont soumises au droit commun et il est expressément admis que figure comme constituant ce droit commun la Convention Européenne des Droits de l'Homme et en particulier son article 8.

Conformément à l'"Human Rights Act" de 1998, la Convention européenne est (plus ou moins) intégrée à la loi nationale britannique. Les pouvoirs publics sont obligés de respecter "les droits issus de la Convention"; la législation postérieure en conflit avec "les droits issus de la Convention" doit être mise de côté; la législation antérieure (c'est à dire les Acts of Parliament) doit être interprétée autant que possible pour être conforme à la Convention; quand il n'est pas possible qu'un Act of Parliament soit interprété comme étant conforme à la Convention, les juridictions doivent l'appliquer: mais dans ce cas précis elles doivent émettre une "déclaration d'incompatibilité" ce qui ouvre la porte à une procédure accélérée au terme de laquelle l'"Act" peut être rapidement amendé (si le gouvernement le souhaite).

La question s'est posée de savoir si la conservation des données biométriques relève du champ d'application de l'article 8 de la Convention Européenne.

La question a été examinée par la "House of Lords" dans sa décision R (S) v Chief Constable of South Yorkshire Police [2004] 1 WLR 2196. En l'espèce, il a été décidé que :

- (i) la simple conservation (contrairement à la diffusion) des données personnelles est conforme à l'article 8 ;
- (ii) Pour la majorité, la conservation de l'ADN pour permettre l'identification d'une personne, sans pour autant permettre d'obtenir d'autres informations sur elles n'est pas conforme à l'article 8 ;
- (iii) Mais (unanimentement), même si la conservation d'échantillons d'ADN concerne les droits énoncés à l'article 8 § 1, la finalité pour laquelle les échantillons étaient stockés en l'espèce nécessitaient une justification.

Le Data Protection Act de 1998 (DPA) restreint l'enregistrement des données personnelles, et impose plus de restrictions à l'enregistrement des données personnelles dites sensibles.

Section 1 :

Le terme « donnée personnelle » signifie une donnée qui a trait à un individu vivant qui peut être identifié

- (a) par ces données ou
- (b) par ces données et d'autres informations qui sont en sa possession, ou dont il va entrer en possession, la surveillance des données, et inclut l'expression d'une opinion sur l'individu et l'indication des finalités de la surveillance des données ou de n'importe quelle autre personne au regard du respect de l'individu.

Section 2 :

Les « données personnelles sensibles » désignent une donnée personnelle consistant en l'information sur

- (a) la race ou l'origine ethnique de l'intéressé,
- (b) ses opinions politiques,
- (c) ses croyances religieuses ou d'autres croyances de nature similaire,

- (d) son appartenance à un syndicat (au sens du Trade Union and Labour Relations Act de 1992),
- (e) sa santé physique et mentale,
- (f) sa vie sexuelle,
- (g) la commission ou la commission présumée de toute infraction, ou
- (h) toute procédure pour toute infraction commise ou présumée commise, l'issue de telles procédures ou la décision de toute juridiction dans lesdites procédures.

Ceux qui traitent les données personnelles sensibles doivent respecter un nombre de « principes de protection des données » qui figurent dans les quatre premières annexes de l'Act. Le traitement mené en méconnaissance de ces principes peut engager la responsabilité civile ou pénale. Cependant, un grand nombre d'exceptions est prévu, atténuant les exigences du respect des « principes de protection des données », ou certaines d'entre elles, dans des cas particuliers. C'est notamment le cas lorsque le traitement est utilisé pour la prévention ou la constatation des infractions, ou le recouvrement des impôts.

Le « Human Tissues Act » de 2004 impose des restrictions au stockage et à l'analyse des tissus humains, à moins qu'un consentement soit donné. La section 45 définit les limites de l'utilisation et de la conservation de l'ADN. Elle prévoit :

(1) Qu'une personne commet une infraction si

- (a) elle est en possession d'un produit du corps humain avec l'intention que
 - (i) l'ADN humain du produit soit analysé sans consentement éclairé, et
 - (ii) que les résultats de ces analyses soient utilisés au-delà des finalités autorisées
- (b) le produit ne relève pas des exceptions expressément prévues, et
- (c) elle ne peut raisonnablement pas croire que le produit fasse partie de ces exceptions

(2) Le produit du corps humain est exclu si

- (a) c'est un produit dérivé du corps d'une personne décédée avant le jour de l'entrée en vigueur de la section et au moins cent ans après le décès de la personne.
- (b) il est placé en dépôt et que la personne qui l'a en dépôt n'est en possession, et n'est pas susceptible d'entrer en possession, d'informations grâce auxquelles l'individu dont provient le produit peut être identifié, ou
- (c) c'est un embryon du corps humain.

(3) Une personne coupable d'une infraction prévue par cette section

- (a) encourt une condamnation à une amende n'excédant pas le maximum légal ;
- (b) encourt une condamnation
 - (i) à une peine d'emprisonnement d'une durée de trois ans maximum, ou
 - (ii) à une amende, ou
 - (iii) aux deux

(4) L'annexe 4 (qui émet une réserve d'interprétation sur « le consentement éclairé » et sur l'usage pour une finalité exclue » dans la sous-section 1 a) s'applique

(5) Dans cette section (et Annexe 4)

- « produit du corps humain » désigne les produits

(a) dérivés du corps humain

(b) composés ou incluant des cellules humaines

- « dépôt » désigne les produits du corps humain prélevés immédiatement avant le jour d'entrée en vigueur de cette section.

« Excepted purposes » [les usages exclus] de l'annexe 4, sont entre autres :

(a) le diagnostic médical ou le traitement de la personne d'où provient l'ADN ;

(b) les médecins légistes ;

(c) en Ecosse, le ministère public ;

(d) la prévention ou la constatation d'un crime ;

(e) les poursuites judiciaires ;

(f) la sécurité nationale ;

(g) l'exécution d'une décision de justice.