

Les numéros personnels d'identification : leur mise en oeuvre, leur utilisation et la protection des données (1991)

Etude préparée par le Comité d'experts sur la protection des données (CJ-PD) sous l'égide du Comité européen de coopération juridique (CDCJ), Strasbourg 1991

L'utilisation croissante de l'informatique dans la société a conduit les administrateurs à recourir toujours davantage à des identifiants. Le PIN (numéro personnel d'identification), s'il est utilisé à l'intérieur d'applications informatiques, est susceptible d'entraîner des atteintes à la vie privée, notamment en raison des risques liés à l'interconnexion de fichiers. Cette étude passe en revue les avantages de l'utilisation des PIN, les dangers pour les personnes concernées ainsi que les garanties devant accompagner leur utilisation.

TABLE DES MATIERES

Introduction

Chapitre 1 : Les PIN - Une définition de travail; secteurs dans lesquels ils sont susceptibles d'être utilisés; leur composition; les tendances actuelles

Chapitre 2 :

- i. Justifications et avantages observés
- ii. Dangers observés pour les personnes

Chapitre 3: Analyse des garanties légales accompagnant l'introduction et l'utilisation des PIN 25

Conclusions et propositions destinées aux décideurs et aux autorités de protection des données

Introduction

Le Comité d'experts sur la protection des données (CJ-PD) n'a pas uniquement élaboré des instruments juridiques en vue d'éclairer, sur la scène internationale, le domaine de la protection des données. Il est vrai que l'ouverture à la signature le 28 janvier 1981 du seul instrument juridique au monde sur la protection des données - la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après dénommée la «convention pour la protection des données») - reste la plus belle réussite du comité. Le comité d'experts a pu utiliser ses bons offices avec autant de succès dans d'autres contextes, notamment pour proposer des lignes directrices concernant les politiques dans certains contextes spécifiques où intervient le traitement de données. Les sept recommandations adoptées par le Comité des Ministres du Conseil de l'Europe pour les divers secteurs relatifs au traitement des données témoignent du travail intense fourni par le comité d'experts dans son approche sectorielle des problèmes de traitement des données (Recommandations no R (81) 1, banques de données médicales automatisées; no R (83) 10, recherche scientifique et statistiques; no R (85) 20, marketing direct; no R (86) 1, sécurité sociale; no R (87) 15, secteur de la police; no R (89) 2, secteur de l'emploi; no R (90) 19, paiement et autres opérations connexes).

Le comité d'experts fait toutefois plus que rédiger des textes juridiques. C'est pourquoi sa contribution au débat sur la protection des données doit plutôt se mesurer par les avis

émis sur les divers problèmes de confidentialité, souvent d'actualité, voire même urgents, qui caractérisent ses sessions plénières semestrielles. Les échanges d'informations sur des sujets aussi divers que le sida, les médias, la génétique, le rôle de l'autoréglementation dans le domaine de la protection des données, etc., permettent de sensibiliser les représentants de tous les gouvernements membres (pour être complet, il convient d'y ajouter les observateurs d'autres organisations internationales ainsi que de pays non-membres du Conseil de l'Europe) aux problèmes de protection des données que soulèvent ces questions. Ils peuvent ainsi comparer les diverses expériences ainsi que les façons d'aborder et de résoudre les problèmes.

Parfois, les échanges de vues ont révélé qu'il était nécessaire d'examiner de plus près un problème donné, par exemple dans le cadre d'un groupe de travail mandaté pour étudier ce problème de plus près et pour présenter d'éventuelles solutions. C'est le type d'approche qui a été suivi pour les questions de protection des données soulevées par les nouvelles technologies. Désireux de ne pas se perdre dans une rédaction laborieuse en jargon juridique pour décrire les problèmes de protection des données nés des nouvelles technologies, le comité d'experts a décidé de publier les informations et les conclusions de son groupe de travail (voir l'étude «les nouvelles technologies - Un défi pour la protection de la vie privée?»).

Il en est de même pour l'introduction et l'utilisation des numéros personnels d'identification (les PIN - personal identification numbers), et les problèmes de protection des données qu'ils entraînent. Au cours d'un échange de vues sur les PIN, le comité a remarqué que le sujet était loin d'être neutre. Les pays membres ont exprimé leur inquiétude plus ou moins vive quant à leur introduction et/ou leur utilisation. Cette attitude est reflétée par les réponses parvenues au comité suite à une demande d'information adressée aux gouvernements des Etats membres du Conseil de l'Europe. Ce questionnaire était destiné à éclaircir les points suivants:

- a. la législation éventuelle sur l'introduction et l'utilisation des PIN;
- b. les raisons pour lesquelles certains pays ont décidé de ne pas instaurer un système de PIN;
- c. les problèmes de protection des données nés dans les divers pays suite à l'introduction et à l'utilisation des PIN.

Le comité pense que la profusion d'informations transmises en réponse au questionnaire, ainsi que ses constatations sur la sensibilité de la question des PIN dans un nombre considérable de pays, méritent une analyse plus détaillée. C'est pourquoi le comité a nommé un petit groupe d'étude composé d'experts d'Allemagne, des Pays-Bas et de la Suède, chargés d'explorer en profondeur tous les problèmes que l'introduction des PIN pose au regard de la protection des données. Ce groupe d'étude, qui s'est réuni les 12 et 13 juin 1989, s'est acquitté de son mandat spécifique par la rédaction d'un rapport sur ces questions en collaboration avec le Secrétariat. Il repose surtout sur les informations transmises par les Etats membres et sur l'expérience de ses propres membres.

Relevons au passage que le comité a composé le groupe de travail pour qu'il dispose de l'expérience d'un pays où les PIN à usages multiples et universels sont considérés

comme une atteinte à la dignité individuelle (Allemagne), d'un pays où ce type de PIN a longtemps été toléré, mais qui prend des mesures en vue de limiter leur utilisation (Suède) et d'un pays où l'on utilise des PIN à usage spécifique, et qui envisage actuellement une réglementation plus approfondie de leur utilisation et de leur diffusion (Pays-Bas). Inutile de dire que les délibérations du groupe d'étude ont largement dépassé le cadre de l'expérience de leurs trois pays. De même, les conclusions présentées à la fin du présent rapport sont destinées à tous les gouvernements, à tous ceux qui participent à l'élaboration des politiques de protection des données et à tous ceux qui sont chargés de veiller à leur application. Nous ne proposons aucun instrument juridique. Nous espérons simplement que les gouvernements et les organismes susmentionnés profiteront de l'identification des problèmes et de la sélection des solutions obtenues par comparaison de l'expérience de chacun. Le Comité d'experts sur la protection des données est convaincu que cette approche sera une nouvelle contribution intéressante au débat sur la protection des données en Europe.

CHAPITRE 1. Les PIN - Une définition de travail; secteurs dans lesquels ils sont susceptibles d'être utilisés; leur composition; les tendances actuelles

Les rédacteurs du présent rapport voient dans les PIN un instrument unique pour identifier une personne dans un fichier administratif. Cela ne veut pas dire que les PIN ne trouvent aucune application en dehors des pouvoirs publics. Ils peuvent constituer un moyen d'accès à toute une gamme de services dans le secteur privé (numéro de compte bancaire, numéro de membre d'un club, numéro d'inscription dans une bibliothèque, voire numéro d'accès personnel au système informatique d'une entreprise privée). Le présent rapport ne s'attache pas à une activité précise ou à un contexte particulier, tels que les diverses utilisations de ces numéros dans le secteur privé. Il se concentre sur les PIN créés par le secteur public à des fins administratives, et parfois utilisés dans le secteur privé, avec le consentement du gouvernement ou dans des circonstances non prévues.

Dans certains pays, les PIN servent d'identifiants universels ou à usages multiples, c'est-à-dire qu'un PIN peut servir à des fins à la fois administratives et privées. Le même numéro peut servir de numéro fiscal, de sécurité sociale, de passeport, de permis de conduire et d'accès à des biens et services dans le secteur privé. Un PIN de ce genre découle d'une conception monolithique de l'administration. Certains PIN ont toutefois un domaine d'application restreint. Ils peuvent être créés pour remplir une fonction administrative déterminée: gérer des dossiers fiscaux, déterminer si une personne a droit à la sécurité sociale, identifier le porteur d'un passeport ou d'un autre document d'identité. Dans ce type d'environnement, une personne donnée se voit attribuer divers identifiants servant diverses fonctions administratives. Le fait de limiter l'usage d'un PIN à une tâche administrative donnée est en accord avec le principe de la séparation fonctionnelle.

Enfin, dans certains cas, un PIN sert à identifier une personne dans un registre de l'état civil ou de la population, à l'exclusion de toute autre application.

L'étude de la situation dans divers Etats membres du Conseil de l'Europe nous informe sur la composition de ces PIN, les fins qu'ils servent et les tendances actuelles dans leur introduction et leur utilisation.

Autriche

L'Autriche n'a aucun identifiant universel malgré les propositions en ce sens faites par l'administration. On n'y trouve que des PIN spécifiques à certains domaines. On notera toutefois que, depuis 1988, le numéro de sécurité sociale peut également servir à certaines applications fiscales.

Belgique

La Belgique attribue un numéro d'identification à toute personne, belge ou étrangère. Ce numéro, conçu au départ en vertu de la loi de 1983 sur le registre national, à progressivement servi d'identifiant pour une foule d'autres applications administratives, au point d'entraîner l'abandon de numéros à usage spécifique tels que les PIN de la sécurité sociale et du domaine fiscal. Cette tendance à l'universalisation du numéro du registre national de la population se poursuit bien que la loi de 1983 subordonne l'utilisation du PIN à l'adoption d'un arrêté royal, après consultation du Comité consultatif sur la protection de la vie privée. Ces précautions internes n'ont pas suffi à limiter ce PIN à son utilisation ou à ses utilisateurs d'origine.

Chypre

Les principaux PIN qui sont utilisés par l'administration sont:

- a. le numéro de sécurité sociale;
- b. le numéro de carte d'identité;
- c. le numéro de permis de conduire.

Le numéro de la carte d'identité est également utilisé à des fins fiscales. Les identifiants sont également largement utilisés dans le secteur privé, principalement par les banques, à des fins de gestion de comptes bancaires et de cartes de crédit.

Danemark

Une loi de 1968 a institué un numéro de dix chiffres composé de la date de naissance, d'un numéro de série et d'un chiffre de contrôle. Les habitants du Danemark sont inscrits au registre central de la population où ils peuvent être identifiés grâce à ce PIN. Ce registre contient des informations sur tous les habitants, destinées à servir les besoins des diverses administrations voire de certains organismes privés dans des circonstances précises. Le PIN est largement utilisé dans le secteur public. Dans le secteur privé, son utilisation est limitée conformément aux dispositions de la loi sur les registres privés - loi sur la protection des données dans le secteur privé du Danemark.

Finlande

En Finlande, les numéros personnels d'identification ont été introduits au cours des années 60. Au départ, les numéros d'identification étaient prévus à des fins de sécurité sociale. Le numéro d'identification se compose de dix chiffres et d'un tiret. Ses six premiers chiffres indiquent la naissance de la personne concernée et les trois chiffres suivants constituent un numéro de série pour établir une distinction entre les personnes nées le même jour. Les chiffres impairs de cette série sont réservés aux hommes et les chiffres pairs aux femmes. Le dernier chiffre est un chiffre de contrôle.

Des dispositions spéciales régissent l'utilisation et l'enregistrement du numéro d'identification. Le numéro d'identification est utilisé conformément à ces dispositions par exemple pour le registre de population, le registre des propriétés et le registre des permis de conduire, ainsi que pour les fichiers de données relatifs aux crédits. L'employeur est également tenu d'informer les autorités fiscales des numéros d'identification de ses employés qui ont des revenus imposables.

Lorsque la loi sur les fichiers de données à caractère personnel a été promulguée, le comité compétent du parlement a appelé l'attention sur le fait qu'une grande utilisation des numéros d'identification est perçue comme constituant une atteinte à la vie privée. A des fins d'information générale, des recherches sur l'utilisation des numéros d'identification dans différents contextes ont été entreprises au service du Data Ombudsman.

La loi sur les fichiers de données à caractère personnel contient des dispositions générales pour les données personnelles et, par conséquent, sur l'enregistrement, l'utilisation et la communication du numéro d'identification. Seules les données personnelles nécessaires à des fins de fichiers de données à caractère personnel peuvent être enregistrées. La nécessité d'utiliser le numéro d'identification doit donc être étudiée au cas par cas.

France

Toute personne née en France se voit attribuer un numéro de treize chiffres composé du sexe, de l'année et du mois de la naissance, du département et du district de la naissance, et du numéro séquentiel dans le registre de naissance. Il est appelé Numéro d'identification au répertoire. Ce numéro est attribué par l'Institut national des statistiques et des études économiques. Divers autres numéros sont utilisés par les secteurs public et privé à des fins déterminées (numéro de carte d'identité, numéro d'enregistrement militaire, numéro de sécurité sociale, numéro de compte bancaire, etc.). Comme nous le verrons plus loin, des dispositions ont été prises pour que l'utilisation du Numéro d'identification au répertoire ne se généralise pas. D'autres secteurs peuvent toutefois obtenir l'autorisation de l'utiliser. C'est le cas de l'administration de la sécurité sociale. Le secteur public aimerait voir étendre l'utilisation du Numéro d'identification au répertoire, car elle estime que la création et la gestion de numéros spécifiques à chaque contexte reviennent cher, exigeant par exemple de réécrire les programmes informatiques. L'autorité française pour la protection des données, la CNIL (Commission nationale de l'informatique et des libertés), encourage toutefois l'administration à adopter des identifiants spécifiques. Grâce à ses efforts, la Direction générale des impôts a créé un numéro fiscal spécial pour remplacer le Numéro d'identification au répertoire sur les déclarations de revenus.

Allemagne

Pour résumer, on n'y trouve aucun numéro unique à usage universel. La façon d'identifier une personne dépend du contexte administratif ou privé. Les tentatives d'introduire un numéro unique ont échoué face à l'opposition du Bundestag et de la Cour constitutionnelle fédérale.

Grèce

En Grèce, une loi de 1986 a institué le numéro de code d'immatriculation unique (EKAM) qui est utilisé sur les cartes d'identité, les actes de naissances les listes électorales et les cartes d'électeur, les passeports, les cartes de la sécurité sociale, les permis de conduire, ainsi que sur les registres des contribuables, des communes et des consulats. Son utilisation dans le secteur public n'est pas universelle. Elle est limitée aux rapports quotidiens entre l'Etat et les citoyens. C'est pourquoi son utilisation est très étendue.

En réalité, les dispositions de cette loi relatives à l'EKAM n'ont pas été appliquées. Le dernier gouvernement, tenant compte des réactions de la presse et de l'opinion publique, a institué un groupe de travail ayant pour mandat l'élaboration d'un projet modifiant ces dispositions.

Islande

La création du registre national de la population en 1953 s'est accompagnée de celle d'un PIN qui devait simplifier la gestion du registre à des fins administratives et statistiques. Ce PIN se compose actuellement de dix chiffres, comprenant la date de naissance (jour, mois, année, siècle), un chiffre de contrôle et deux chiffres arbitraires affectés aux personnes nées le même jour. Depuis 1987, l'utilisation de ce PIN de dix chiffres s'est étendue à d'autres applications dans l'ensemble de l'administration afin d'éviter les problèmes liés à l'identification nominale. Au-delà de son utilisation par le secteur public, ce PIN, qui est affecté à toute personne en Islande au cours de l'année qui suit sa naissance, se retrouve dans le secteur bancaire et sur tous les documents financiers.

Une nouvelle loi sur la protection des données est entrée en vigueur le 1^{er} janvier 1990. Conformément au chapitre 1, paragraphe 4, de cette nouvelle loi, les dispositions de la loi s'appliquent aux données relatives aux affaires privées d'un individu, même anonymes, si celui-ci est identifié par un numéro personnel d'identification. Conformément au chapitre 6, paragraphe 1, de la loi, l'interrelation des registres de données personnelles n'est pas permise. Néanmoins, il est permis d'ajouter à un registre des données concernant un PIN, même si ces données ont été obtenues à partir d'un registre d'un tiers.

Irlande

Il n'existe pas d'identifiant universel à usage multiple en Irlande. Cependant, des numéros à usage spécifique existent dans plusieurs domaines de l'administration publique, par exemple le numéro d'assurance sociale, qui sont utilisés à des fins spécifiques. Il n'y a pas de fondement unique pour souligner la façon dont ces PIN sectoriels sont formulés. Dans le secteur privé, il y a une utilisation croissante d'identifiants personnels, en particulier dans le secteur des services financiers.

Il faut noter qu'il y a eu très peu de discussion sur l'opportunité ou autre d'instaurer un identifiant universel à usage multiple. Si un tel débat devait être entamé, les problèmes de protection des données liés aux PIN seraient sûrement étudiés soigneusement.

Luxembourg

La loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales attribue un numéro d'identité à chaque personne physique (ainsi qu'aux

personnes morales, sur la base de critères différents) résidant au Luxembourg dès la naissances ou à l'immigration, ainsi qu'à toute autre personne physique ou morale inscrite sur un rôle d'une administration publique ou d'un établissement de sécurité sociale luxembourgeois, tenu par une disposition légale ou réglementaire d'employer ce numéro. Le numéro d'identité est composé de onze chiffres représentant la date de naissance, le sexe, un chiffre distinguant les personnes nées le même jour du même mois de la même année, et un chiffre de vérification. L'utilisation de ce numéro est limitée à l'administration interne des services publics ou des organismes de la sécurité sociale, et à leurs relations directes avec le porteur de ce numéro. Le règlement grand-ducal du 7 décembre 1979, tel qu'il a été complété par la suite, détermine les actes, documents et fichiers autorisés à utiliser le numéro d'identité des personnes physiques et morales. Ce règlement contient une disposition malheureuse qui permet aux propriétaires de fichiers habilités à utiliser le PIN de déléguer cette autorisation «à toute personne ou organisme intermédiaire, chargé d'une mission spécifique pour leur [propre] compte». D'autre part, les organismes de la sécurité sociale demandent par exemple aux personnes qui dispensent des soins médicaux de mentionner le numéro d'identité de leurs patients, et aux employeurs de faire apparaître le numéro d'identité de leurs employés dans tous les documents qui leur sont transmis. L'autorité luxembourgeoise pour la projection des données observe cette évolution avec une certaine inquiétude, car le PIN circule bien au-delà du cercle des utilisateurs autorisés par la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales.

Pays-Bas

Aux Pays-Bas, il existe un numéro administratif général depuis 1968. Cependant, jusqu'à présent, il a été utilisé seulement pour les registres de la population des municipalités. Un livre blanc a été publié en 1985 pour suggérer une approche progressive: l'introduction graduelle des PIN dans certains secteurs sur la base d'une législation limitant le risque d'une atteinte excessive à la vie privée. Dans cet ordre d'idées, la loi fiscale prévoit maintenant que les numéros fiscaux figurent systématiquement parmi les données relatives, aux salaires des personnes concernées. Jusqu'en 1989, ces numéros n'ont pu être utilisés qu'à des fins fiscales. Depuis lors, le champ d'application du numéro fiscal a été étendu à tout le domaine de la sécurité sociale. Les propositions du livre blanc visant à intégrer le numéro administratif général et le numéro fiscal ont fait l'objet de vives critiques. Les adversaires de ces propositions ont insisté sur le besoin de prévoir des garanties juridiques et, en particulier, sur le besoin d'une législation sur la protection des données, puisque le PIN doit servir à l'ensemble des services publics. On assiste ainsi aux Pays-Bas à l'introduction graduelle d'un identifiant unique pour l'ensemble des services publics, garantie par une législation adéquate. Le numéro de recensement ne pourra être utilisé dans le secteur privé.

Norvège

Conformément aux dispositions de la loi sur l'enregistrement de la population, tous les habitants de Norvège se voient attribuer un PIN.

Le PIN se compose de onze chiffres. Les six premiers chiffres indiquent la date de naissance: deux pour le jour, deux pour le mois et deux pour l'année. Les trois chiffres suivants sont attribués successivement à chaque naissance de la même journée. Le neuvième chiffre est pair pour les femmes et impair pour les hommes. Les deux derniers chiffres sont des chiffres de contrôle. Outre leur utilisation par les registres de la

population les PIN sont maintenant utilisés par d'autres secteurs de l'administration publique qui en ont besoin pour identifier les citoyens, par exemple à des fins de sécurité sociale ou d'imposition.

L'utilisation du PIN comme moyen d'identification a été aussi élargie à d'autres branches du secteur privé, par exemple les banques et les assurances.

Les organismes publics qui ont besoin d'informations relatives au PIN pour mener à bien leurs fonctions sont autorisés - par la loi ou par des règlements - à demander de telles informations aux citoyens. L'autorisation légale des entreprises privées qui demandent de telles informations dépendra du fait de savoir si la divulgation de ces informations constitue ou non une condition légitime à la conclusion d'un contrat.

Conformément à la loi sur les registres de données à caractère personnel, la création de registres de données personnelles et l'utilisation du PIN dans les registres sont soumises au contrôle de l'inspection des données. Conformément à la législation et aux règlements, l'enregistrement du PIN est interdit pour plusieurs sortes de registres. Pour d'autres sortes de registres, l'enregistrement du PIN est soumis aux conditions énoncées dans la loi ou les statuts, ou à l'autorisation de l'Inspection des données. L'Inspection des données fixe certaines conditions concernant la collecte, l'enregistrement et l'utilisation du PIN au moment de donner son autorisation.

Portugal

L'article 35 de la Constitution portugaise d'avril 1977, amendé en 1982 et en 1989, interdit formellement l'attribution d'un numéro national unique aux citoyens. En fait, une loi de 1973 avait tenté d'attribuer un PIN à toutes les personnes physiques et morales. Ce PIN serait obligatoirement inscrit dans tous les documents et registres officiels concernant les personnes nées après le 1er janvier 1975. Cette loi fut laissée en suspens par la clause de la Constitution de 1977 mentionnée ci-dessus. Bien qu'il n'y ait pas d'identifiant unique au Portugal, on y trouve des numéros à usage spécifique: un numéro de carte d'identité constitué de données non significatives, un numéro détecteur, un numéro fiscal (numéro de série non significatif), un numéro de sécurité sociale, etc. Comme dans bien d'autres pays, on trouve au Portugal une multitude de numéros différents destinés à diverses applications dans le secteur privé.

Espagne

Malgré des tentatives faites au cours des années 70 pour introduire un identifiant personnel universel selon le modèle scandinave, l'Espagne possède encore un système de PIN lié à l'émission du numéro figurant sur le document d'identité du citoyen. Le Décret no 196/76-, tel que modifié par le Décret no 1245/85, déclare que le numéro de la carte d'identité - qui identifie en réalité le lieu d'émission de la carte et non la date et le lieu de naissance du détenteur - est un «identificateur numérique universel». Ce numéro est utilisé pour les relations entre administrations publiques et individus ainsi que pour des règlements d'affaires entre certaines parties du secteur privé (banques, par exemple) et individus. Cependant, le numéro peut comporter l'ajout d'autres chiffres de contrôle par les organismes publics et privés qui l'utilisent. Conformément aux dispositions de la loi no 7/1985, les étrangers résidant en Espagne se voient accorder, en même temps que leurs permis de résidence, leurs permis de travail, etc., un numéro à caractère séquentiel qui doit être utilisé dans leurs relations avec les organismes publics. Depuis 1966, cependant, un numéro de sécurité sociale, spécial et distinct, a été attribué

aux étrangers résidant en Espagne. Ce numéro comprend un code de la province d'inscription, un numéro séquentiel et un ou deux chiffres de contrôle.

En 1990, un nouveau numéro fiscal a été introduit; il se compose du numéro de la carte d'identité et d'un numéro de contrôle non connu de l'individu. Ce numéro est attribué à toute personne au moment de sa naissance.

Suède

En 1947 déjà, la Suède avait instauré un numéro d'état civil pour faciliter et unifier l'identification des personnes d'une autre manière que par leurs noms. Ce numéro est graduellement devenu un numéro d'identification civile largement utilisé dans divers secteurs pour remplacer une foule d'autres numéros spécifiques. Il se compose actuellement de dix chiffres et a reçu l'appellation officielle de numéro personnel d'identification. Ce PIN se compose de la date de naissance (deux chiffres pour l'année, deux pour le mois et deux pour le jour), le numéro d'inscription au registre des naissances (conçu pour indiquer le sexe de la personne et éviter toute confusion entre deux personnes nées le même jour). Dans le PIN suédois, le chiffre 9 indique qu'une personne est née à l'étranger. Cette personne peut être de nationalité suédoise ou non. Le chiffre 9 m peut également vouloir dire que le PIN d'origine d'une personne a été changé. Ce système ne sera plus en fonction l'an prochain. A l'avenir le PIN ne sera pas constitué de manière à révéler qu'une personne est ou non née à l'étranger. Il existe enfin un chiffre de contrôle. Ce PIN est affecté à toute personne inscrite comme habitant d'une paroisse (commune) de Suède.

Ce PIN est utilisé non seulement dans les registres d'état civil, mais également pour diverses applications dans les services publics (fiscalité, services sociaux et de santé, passeport, douanes, élections, enquêtes judiciaires, procédures légales, exécution de jugements, permis de conduire, etc.). On le retrouve également dans divers fichiers du secteur privé, comme pour les employés, le personnel d'entreprises privées, les propriétaires et les locataires, les détenteurs de cartes de crédit, etc.

En Suède, le PIN est donc l'identifiant universel par excellence. La Commission pour la protection des données et la publicité a présenté des propositions en vue de restreindre l'utilisation du PIN. Elle suggère par exemple de renforcer la loi sur la protection des données afin de réduire les applications du PIN. Le Conseil pour l'inspection des données est chargé de superviser l'usage que les maîtres de fichiers font du PIN. Le PIN pourrait également être régi par une loi spécifique interdisant, entre autres, l'utilisation d'un PIN dans un fichier informatique sans l'accord de la personne concernée, ou sans autorisation légale. Le gouvernement examine à l'heure actuelle le rapport de la commission.

Suisse

Bien qu'il n'existe aucun numéro unique et universel en Suisse, le numéro de sécurité sociale (AVS) fait office de numéro personnel d'identité. Ce numéro de sécurité sociale est utilisé par de nombreux services privés et publics dans la gestion de l'assurance maladie, les services du personnel, les registres de la population, etc. Même les autorités militaires l'utilisent. Ce numéro se compose d'informations codées sur le nom de l'assuré, son sexe, son état civil, s'il est Suisse ou non, et d'un chiffre de vérification.

L'utilisation du numéro de sécurité sociale s'est étendue à un point tel qu'une étude en vue de la création d'un nouveau système d'identification des personnes a conclu qu'il serait préférable de s'en tenir à ce numéro.

Turquie

Le certificat de nationalité turque se compose du numéro du détenteur ainsi que de son nom, son prénom, le nom de ses parents et de ses lieu et date de naissance. Ces informations sont reprises dans le registre de l'état civil. Le numéro de la carte de citoyen n'est toutefois pas un identifiant universel.

Royaume-Uni

L'administration britannique utilise un grand nombre d'identifiants à usage spécifique, tels que le numéro national de santé, le numéro national d'assurance, le numéro fiscal, celui du permis de conduire, etc., Ces numéros peuvent être composés de la date de naissance ainsi que d'autres chiffres, ou simplement d'un numéro séquentiel quelconque. Chaque secteur à son système. Rien de surprenant donc à ce que le secteur privé utilise lui aussi une grande variété d'identifiants. Au cours des débats actuels sur l'instauration de cartes d'identité et sur une nouvelle forme d'impôts locaux, on étudie la question des identifiants uniques et de la menace qu'ils pourraient constituer pour les libertés individuelles.

CHAPITRE 2. Justifications et avantages observés; dangers observés pour les personnes

i. Justifications et avantages observés

Etant donné la multiplication des contacts entre l'Etat et les personnes, principalement du fait de l'Etat providence, il est devenu de plus en plus urgent de mettre au point des moyens précis pour identifier les bénéficiaires des biens et services sociaux. Avec l'augmentation démographique de l'après-guerre, le nombre des personnes administrées a également augmenté, et donc la charge financière qu'elles représentent (d'où la nécessité d'établir des registres d'état civil rationnels). Si l'Etat doit pourvoir (sécurité sociale, bourses, enseignement, santé, etc.) et surveiller (forces de police, prisons, collecte des impôts, déplacements des personnes, droit des personnes à manœuvrer divers véhicules ou à diriger une entreprise, etc.), les fichiers administratifs prolifèrent. Etant donné la complexité croissante de la situation, un identifiant unique pour chaque personne faciliterait considérablement la réglementation et la surveillance par l'administration. Celle-ci peut toutefois augmenter son efficacité tant avec des PIN universels qu'avec des PIN à usage spécifique. Et, bien que les PIN soient apparus avant l'informatique (dans nombre de pays, les registres de la population ont existé bien avant l'informatique), l'entrée de l'informatique dans les administrations publiques permet aux PIN de rendre de meilleurs services encore aux fonctionnaires.

Les rapports nationaux qui ont servi à la rédaction du présent rapport mentionnent souvent les économies réalisées grâce aux PIN et l'amélioration de l'efficacité des administrations. Au Portugal par exemple, le décret-loi du 30 novembre 1979 qui institue le numéro fiscal justifie ce dernier par les bienfaits apportés dans l'administration. D'après le préambule, le PIN permet une identification rapide et correcte du contribuable, un contrôle efficace de l'observance des obligations fiscales,

un contact plus facile entre l'administration et les contribuables Le Comité Lindop, dont les conclusions ont amené le Parlement du Royaume-Uni à examiner un projet de loi sur la protection des données (qui devint la loi de 1984 sur la protection des données), reconnaissait lui aussi l'intérêt que présente un système d'identifiants uniques et universels:

«Il est probable qu'avec un seul et unique identifiant par personne, utilisé en toutes circonstances par tous les utilisateurs de données, le coût global pour l'utilisateur serait réduit. De même, le citoyen n'aurait plus à se souvenir des divers identifiants spécifiques à chacune de ses nombreuses activités. » (Rapport du Comité pour la protection des données (1 978), chapitre 29, paragraphe 6).

Le PIN permet également d'identifier les personnes avec précision et garantit l'exactitude des informations à caractère personnel contenues dans les systèmes informatiques. Deux points méritent ici notre attention. Tout d'abord, le PIN permet de ne pas confondre deux personnes portant le même nom. Deux des rapports nationaux au moins (la France et le Luxembourg) signalent que, pour identifier une personne sans ambiguïté, les noms et prénoms sont totalement insuffisants, surtout quand l'identification a des conséquences financières (droit aux allocations, listes de débiteurs insolvables, etc.) ou sociales (par exemple, casiers judiciaires). Dans beaucoup de pays, un grand nombre de personnes portent le même nom, d'abord parce que le nombre de noms utilisés diminue et ensuite en raison des modes qui favorisent certains prénoms à certains moments, etc.

Ensuite, le PIN comporte une autre dimension. Le PIN peut permettre à une administration donnée de vérifier l'exactitude ou la fiabilité des informations d'un fichier administratif. Il s'agit de vérifier les informations présentées par les personnes en vue d'établir leur droit à certains droits, avantages ou privilèges (sécurité sociale, bourses, remboursements, etc.) ou en vue de les dispenser de certaines peines ou charges (taxes, impôts locaux, etc.). La présence d'informations à caractère personnel dans divers fichiers administratifs établis à des fins spécifiques permet aux fonctionnaires de vérifier l'exactitude des données fournies en consultant ces diverses banques de données. L'identifiant universel facilite grandement cette interconnexion ou cette comparaison des fichiers. L'informatique facilite naturellement ce processus. Une personne peut par exemple demander une bourse d'études auprès d'une administration. Elle présente des informations concernant ses moyens financiers qui justifient son droit à une bourse. Une administration consciencieuse vérifie alors en temps réel par consultation, à l'aide du PIN de la personne et de l'ordinateur, le fichier fiscal de la personne, détenu par l'administration des finances. Cette formalité rapide permet ainsi de vérifier l'exactitude des dires du demandeur sur ses revenus, le capital dont il dispose, etc. Ces vérifications des données dans les divers services permettent donc de lutter contre la fraude. Cet aspect de l'identifiant unique est également utilisé pour justifier son existence.

ii. Dangers observés pour les personnes

Il convient de remarquer que, dans certains pays, le débat sur l'introduction ou l'utilisation des PIN a relancé celui de la protection des données. Dans quelques pays, ce débat a mené à l'adoption d'une législation relative à la protection des données. Par exemple, la loi française pour la protection des données du 6 janvier 1978 est née des

débats suscités par le projet SAFARI au milieu des années 70, qui proposait l'interconnexion des fichiers à partir du numéro d'identification au répertoire. L'Allemagne est un autre exemple de pays où la proposition d'utiliser les PIN dans les systèmes informatiques a lancé des discussions qui ont abouti à l'introduction du projet de loi fédéral relatif à la protection des données (devenu loi en 1978). A cet égard, l'article 35 de la Constitution portugaise de 1976 est également intéressant, car il juxtapose l'interdiction de comparer les fichiers (article 35.3) à celle d'affecter aux personnes un identifiant unique (article 35.5), le tout dans le contexte de la reconnaissance des droits du citoyen face à l'informatique.

Que ces facteurs soient justifiés ou non, ils traduisent une inquiétude psychologique et émotionnelle profonde face à l'instauration d'identifiants uniques. A cet égard, on notera que la Cour constitutionnelle de l'Allemagne a déclaré que l'introduction de PIN universels pourrait constituer une atteinte à la dignité individuelle étant donné que ceux-ci permettraient un contrôle sur les personnes par la connexion des fichiers et la constitution de profils de personnes ou de groupes de personnes. Le problème de la dignité des personnes transparaît également dans la crainte du public de voir les gens réduits à de simples «numéros», l'Etat ne traitant plus les personnes avec le respect dû aux êtres humains. Ce type de sentiment général s'accompagne de la crainte de voir surgir petit à petit un «état Orwellien » contrôlant tout et capable de surveiller en permanence les moindres faits et gestes de ses sujets.

L'introduction et l'utilisation des PIN universels font l'objet de réserves importantes. La loi de 1989 relative à la vie privée, en Australie, résulte d'une campagne énergique contre les possibilités de surveillance qu'aurait offertes la carte «Australia card». Cette carte aurait comporté un numéro identifiant le porteur. Ce projet a été abandonné, tandis que la nouvelle loi relative à la vie privée limite considérablement l'utilisation du numéro fiscal. Au Canada, divers commissaires à la vie privée ont lancé des avertissements face à l'extension «insidieuse » de l'usage fait du numéro de sécurité sociale. Dans son rapport annuel pour 1985-1986, le Commissaire à la vie privée a dit que «l'obtention indésirable d'informations est plus facile avec le numéro de sécurité sociale qu'avec toute autre information à caractère personnel». Le Commissaire à la vie privée s'inquiète ici du fait que le numéro d'assurance sociale (NAS), mis en service au milieu des années 60, ait vite dépassé le contexte de la sécurité sociale pour devenir le PIN le plus répandu au Canada, et qu'il permet actuellement de consulter et de comparer les fichiers administratifs qui contiennent des données à caractère personnel, collectées et enregistrées à diverses fins administratives. Toujours au Canada, le rapport de 1987 du Comité permanent pour la justice et le substitut du ministre de la Justice («Une révision de la loi sur l'accès aux informations et de la loi sur la vie privée») a présenté des recommandations énergiques sur la nécessité de limiter l'utilisation faite du numéro de sécurité sociale. Le rapport a noté que ce numéro «est si important et si spécial, et il montre si bien à quel point il est indispensable d'assurer la protection des renseignements personnels, qu'il appelle des mesures de contrôle de son utilisation ». Dans sa réponse au comité parlementaire, le gouvernement fédéral a indiqué qu'il s'assurerait que le NAS ne devienne pas un numéro d'identification universel. En juin 1988, le gouvernement fédéral a restreint l'utilisation du NAS. Toutes nouvelles utilisations du NAS par les institutions gouvernementales fédérales après cette date requièrent l'approbation parlementaire. La politique mise en œuvre en juin 1989 par le gouvernement fédéral requiert que les institutions gouvernementales informent les individus des fins pour lesquelles leur NAS est demandé et qu'il ne peut être refusé un

droit, avantage ou privilège, ou qu'il ne peut être imposé de peine à quiconque refuse de fournir son numéro. Le gouvernement fédéral travaille actuellement en collaboration avec les gouvernements provinciaux en vue de déterminer si l'utilisation du NAS peut être également restreinte dans leurs juridictions.

Au Royaume-Uni, de nouvelles demandes en vue d'utiliser le PIN dans les secteurs public et privé continuent d'affluer, par exemple pour le nouvel impôt local, la cotisation communale et par les agences de crédit. Le Data Protection Registrar a fait des commentaires sur ces demandes, et sur d'autres, et a souligné les dangers que pourrait représenter l'utilisation incontrôlée des PIN.

Les PIN sont donc redevenus d'actualité. La loi relative à la protection des données des Pays-Bas, adoptée en décembre 1988, est née du débat sur les PIN. Le Gouvernement suédois a demandé à sa Commission pour la protection des données et la publicité d'étudier les dangers que l'utilisation des PIN pourrait représenter pour la vie privée.

Combinés à l'informatique, les PIN contribuent sans conteste à augmenter le pouvoir de l'administration. Comme nous l'avons vu ci-dessus, l'interconnexion de fichiers en utilisant des identifiants uniques permet aux organismes publics de vérifier des informations par comparaison avec celles des fichiers de nombreuses autres banques de données. Une telle accumulation de données exclut la personne concernée du circuit de l'information. Un organisme donné ne doit plus contacter la personne pour obtenir ou vérifier des informations déjà fournies à une autre administration. L'administration peut vérifier des informations par comparaison avec des fichiers détenus par d'autres départements. Elle peut également compléter ses informations par emprunt d'informations détenues par d'autres organismes à des fins administratives. L'identifiant unique et universel pour chaque membre de la population constitue la clé de voûte d'un tel accès aux données, et il pourrait fortement augmenter le pouvoir de l'administration.

Si le PIN unique n'est pas limité au secteur public, mais passe au secteur privé, le pouvoir des administrations augmente encore. Cette vision des PIN sous l'angle du «pouvoir» suscite naturellement des questions de libertés individuelles et de surveillance, car l'anonymat du citoyen est anéanti par ce numéro qui permet aux autorités de suivre bien plus facilement ses faits et gestes, d'accumuler des informations à partir des divers fichiers personnels sans qu'il en soit informé et de prendre des décisions qui l'affectent à partir de ces informations disponibles. Cette analyse est valable tant pour les individus que pour les groupes.

Au-delà de ces considérations, il peut également y avoir d'autres risques:

- a. le PIN pourrait contenir des données compréhensibles uniquement par l'organisme auquel il est présenté, voire seulement par un système informatique;
- b. le PIN pourrait contenir des informations délicates voire strictement personnelles (par exemple, certaines personnes n'aiment pas porter un numéro qui révèle qu'elles ont divorcé, qu'elles ont 50 ou 60 ans, etc.);
- c. le PIN pourrait être modifiable, c'est-à-dire que sa composition varierait en fonction des étapes marquantes de la vie du porteur. Il se peut que le sexe du porteur change. Dans ce cas, il faut que l'ancien numéro soit éliminé, ou du moins gardé en sécurité;

d. le PIN pourrait rendre nominales les informations contenues dans les banques de données statistiques si ces données statistiques sont liées au PIN;

e. le PIN pourrait être révélé par son porteur à des organismes fournissant des biens et des services, alors que cette situation n'avait pas été envisagée au moment de sa création. En Suède par exemple, il est noté que la divulgation du PIN est souvent une condition sine qua non pour obtenir des facilités de crédit, de services, la qualité de membre d'une association, etc. Si une personne n'est pas disposée à dévoiler son PIN, elle doit être prête à accepter une réponse négative;

f. ce dernier facteur nous amène à des considérations plus générales et plus importantes, c'est-à-dire la possibilité (qui d'après certains rapports nationaux est déjà une réalité) pour un PIN spécifique de dépasser petit à petit le cadre de ses fonctions pour servir dans d'autres contextes voire devenir d'application générale. Cette situation survient quand l'introduction d'un PIN unique ou spécifique ne s'accompagne pas des garanties nécessaires, ou quand la définition de leur utilisation et des organismes habilités à les utiliser est trop vague.

CHAPITRE 3. Analyse des garanties légales accompagnant l'introduction et l'utilisation des PIN

Les instruments relatifs aux droits de l'homme ne mentionnent pas spécifiquement les PIN. On n'en parle ni dans la Convention européenne des Droits de l'Homme, ni dans la convention sur la protection des données. L'utilisation des PIN à toutefois un rapport direct avec ces deux traités internationaux.

L'utilisation des PIN par les pouvoirs publics peut par exemple, dans certains cas et applications, tomber directement dans le champ de l'article 8 de la Convention européenne des Droits de l'Homme (le droit au respect de la vie privée et familiale, du domicile et de la correspondance). La Cour et la Commission européennes des Droits de l'Homme considèrent que la Convention est un document vivant qui évolue pour s'adapter aux nouvelles situations. Ces deux organismes considèrent par conséquent que la protection des données tombe dans le champ de l'article 8 de la Convention. La Commission a traité au moins trois affaires liées à l'utilisation de PIN par l'administration:

Lindquist contre Suède (no. 10879/84);

Lundvall contre Suède (no. 10473/83);

Kolzer contre Suède (no. 11762/85).

Bien que la Commission ait estimé que ces trois affaires ne constituaient pas une violation de l'article 8 et les ait rejetées, l'utilisation des PIN peut dans certains cas entraîner un point de contestation de cet article.

Quant à la convention sur la protection des données, les principes fondamentaux qu'elle exprime agissent sans nul doute comme une sauvegarde dans l'utilisation des PIN. Ce point de vue repose sur le fait que les PIN sont étroitement liés au traitement des données à caractère personnel. Comme nous l'avons relevé plus haut, ils donnent accès aux fichiers de données à caractère personnel. Même un simple numéro de série sans

signification particulière peut donner accès à un fichier contenant des informations délicates. Il convient donc de garder ces considérations à l'esprit et de considérer que les PIN sont:

- i. des informations personnelles liées à des fichiers de données à caractère personnel;
- ii. des instruments clés dans tout le secteur du traitement des données. Si nous voulons appliquer les clauses de la convention sur la protection des données aux PIN, nous pouvons tirer les conclusions suivantes:
 - les PIN entrent dans la définition des données à caractère personnel telle qu'elle apparaît dans l'article 2.a de la convention;
 - les utilisateurs de données devraient agir loyalement et légalement pour obtenir le PIN d'une personne, conformément à l'article 5.a de la convention. Cela signifie que le PIN ne peut être demandé à son porteur que sur la base d'une réglementation ou d'une autorisation légale. A défaut de telles justifications, il ne peut être obtenu sans le consentement libre et informé de la personne concernée;
 - les PIN devraient servir aux fins pour lesquelles ils sont créés et ne pas être utilisés à des fins non prévues au départ (article 5.b de la convention). On pourrait par exemple douter du respect de ce principe si un PIN spécifique dont l'usage est strictement défini au départ sert à faciliter la comparaison de fichiers, ou s'il est utilisé comme identifiant dans d'autres contextes;
 - le PIN ne devrait pas contenir plus d'informations à caractère personnel que nécessaire pour son application spécifique (article 5.c de la convention);
 - le PIN devrait être exact et pouvoir évoluer en fonction des changements de situation de la personne concernée (article 5.d de la convention);
 - la composition du PIN ne devrait pas révéler des données sensibles du type de celles mentionnées dans l'article 6 de la convention;
 - le PIN devrait être protégé contre l'accès illicite ou la diffusion à des tiers (article 7 de la convention);
 - le porteur du PIN devrait avoir le droit d'accéder aux informations codées à l'aide du PIN, de les faire rectifier et de les faire effacer, tout comme pour les fichiers de données à caractère personnel auxquels le PIN se rapporte (article 8 de la convention).

Pour conclure cette section sur les garanties au niveau international, mentionnons encore le principe 5 de la Recommandation n- R (86) 1 du Comité des Ministres du Conseil de l'Europe relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale. Les rédacteurs de la recommandation ont, à dessein, attiré l'attention des gouvernements sur les dangers qu'entraîne l'introduction d'un numéro de sécurité sociale unique et uniforme. Le principe 5 de cette recommandation déclare que la création et l'utilisation d'un tel numéro devraient s'accompagner des garanties nécessaires. Au cours de la rédaction de cette clause, on a fait remarquer que les identifiants suscitent souvent des craintes. L'exposé des motifs de la recommandation observe également que ce qui au départ ne devait être qu'un numéro utilisé dans le secteur de la sécurité sociale peut rapidement devenir un numéro universel. Les rédacteurs estiment également que les numéros universels ne devraient pas être institués de façon clandestine. Il est intéressant de remarquer que les rédacteurs de la recommandation encouragent les gouvernements à fournir des garanties quant aux données contenues dans les numéros de sécurité sociale ou autres identifiants. Ces informations devraient par exemple être lisibles et se limiter au strict nécessaire.

Garanties prévues dans les législations nationales

La relation qui existe entre l'introduction d'un PIN et son utilisation est confirmée par la mention explicite qu'en font les lois relatives à la protection des données de certains pays (par exemple, la législation française et la législation norvégienne mentionnent spécifiquement les identifiants). En France, l'article 18 de la loi du 6 janvier 1978 déclare que l'utilisation du Numéro d'identification au répertoire à des fins de traitement des données à caractère personnel ne peut être autorisée que par le Conseil d'Etat après avis favorable de la CNIL. Depuis 1978, la CNIL n'a émis que quinze avis favorables concernant l'utilisation de ce numéro. La CNIL a élaboré une jurisprudence très étendue sur l'interprétation à donner à l'article 18 et a, entre autres, essayé de limiter l'interprétation du mot «utilisation». La CNIL considère par exemple que le simple fait de consulter le répertoire national, même sans extraire le numéro (comme dans le cas d'un contrôle d'identité), tombe dans le champ de l'article 18 et requiert donc une autorisation du Conseil d'Etat. Au Danemark, la législation relative à la protection des données de fichiers privés stipule que le PIN ne peut être enregistré par des organismes privés qu'avec l'accord de la loi, ou l'autorisation expresse de la personne concernée, et à condition seulement que cette information soit nécessaire à cet organisme pour satisfaire à des exigences légitimes.

On retrouve également la relation entre la protection des données et les PIN dans le fait que l'on ne mentionne pas la compétence des organismes de protection des données pour intervenir quand l'utilisation des PIN pose des problèmes relatifs à la protection des données. Dans des pays tels que l'Autriche, l'Islande et le Luxembourg, par exemple, les organismes de protection des données ont accepté de superviser l'utilisation des PIN. Même si la Suède n'a en principe aucune disposition interdisant ou limitant explicitement l'utilisation des PIN, le Conseil pour l'inspection des données de ce pays a affirmé sa compétence quand les pouvoirs publics ont tenté de comparer des fichiers à l'aide des PIN. La loi suédoise pour la protection des données prévoit qu'il est en principe nécessaire de demander l'accord du Conseil pour l'inspection des données avant de procéder à une telle comparaison. Conformément à l'article 6, paragraphe 1, de cette loi, le Conseil pour l'inspection des données peut déterminer l'usage d'un PIN dans un fichier et peut même l'interdire complètement. Le Conseil pour l'inspection des données a également établi des dispositions générales concernant l'utilisation des PIN dans les fichiers de clients. Quand des associations décident, conformément à leurs règlements, d'enregistrer les PIN de leurs membres, les personnes concernées doivent admettre que la qualité de membre peut leur être refusée si elles ne sont pas disposées à dévoiler leur PIN. Cependant, si la divulgation du PIN est considérée comme étant une condition déraisonnable, le Conseil pour l'inspection des données est compétent pour en interdire l'enregistrement. La question peut également être portée devant le Conseil national suédois pour la politique à l'égard des consommateurs. Comme nous l'avons vu plus haut, les institutions compétentes pour la protection des données au Canada et au Royaume-Uni s'appêtent à lancer le débat politique sur l'introduction ou l'utilisation des PIN.

On trouve un organisme compétent pour superviser l'utilisation des PIN et publier des directives à ce sujet même dans les pays qui ne disposent d'aucune législation relative à la protection des données. La Belgique dispose par exemple d'un comité consultatif pour la vie privée; ce comité a démontré qu'il est prêt à assurer la réglementation des

PIN, même si par le passé son intervention n'a pu empêcher la diffusion du PIN au-delà de ses objectifs premiers.

A part la législation relative à la protection des données, les lois qui instituent les PIN peuvent également contenir des restrictions quant à leur utilisation et aux personnes ou organismes habilités à les utiliser. C'est par exemple le cas des pays qui disposent d'une législation sur les registres de la population (comme le Danemark, la Norvège et les Pays-Bas) ou qui ont institué des PIN spécifiques à certains domaines (comme le Portugal et la Suisse). En Espagne, le cadre juridique créé par le décret no 196/76, tel que complété par le décret no 1245/1985 pour la gestion des cartes nationales d'identité comportant un PIN, stipule en son article 6 que la gestion des cartes par les autorités publiques «devra respecter le droit à la vie privée», y compris pour réaliser des enquêtes d'identification faites par le ministère de l'intérieur responsable des cartes nationales d'identité.

Conclusions

Conclusions et propositions destinées aux décideurs et aux autorités de protection des données

Comme le démontre l'analyse ci-dessus, le débat sur les PIN n'est neutre ni dans les pays qui disposent déjà d'une large expérience de leur utilisation comme identifiants universels ou spécifiques, ni dans ceux qui discutent leur introduction. L'évaluation précise du coût (problèmes de protection des données et de la vie privée) et des avantages (efficacité de l'administration et économies réalisées grâce à l'introduction des PIN) est indispensable dans les deux cas.

L'analyse des avantages et des inconvénients devrait tenir compte des facteurs suivants:

i. Là où les PIN existent, leur utilisation doit être limitée afin d'atteindre l'équilibre indispensable entre la vie privée et l'efficacité administrative. Cette restriction doit être de nature juridique, exécutée par l'intervention d'un organisme indépendant comme une autorité pour la protection des données, voire intégrée à la législation relative à l'utilisation des PIN par les pouvoirs publics. La législation relative à la protection des données doit expressément mentionner des garanties contre l'utilisation excessive des PIN par les pouvoirs publics. Cette option trouve faveur aux yeux de certains pays. Toutefois, le fait que l'utilisation des PIN ne soit pas expressément mentionnée par la législation relative à la protection des données n'exclut en rien la compétence des organismes de surveillance établis par cette législation. Après tout, les PIN constituent l'élément clé du traitement des données. A partir d'un PIN, il est possible de collecter des données à caractère personnel, de les enregistrer et de les utiliser. D'autre part, les PIN facilitent l'interconnexion de fichiers. A un niveau plus simple, les PIN constituent en eux-mêmes des données à caractère personnel. En résumé, les autorités chargées de la protection des données sont compétentes pour superviser et réglementer l'utilisation des PIN.

ii. Quand il existe déjà des PIN universels ou à usages multiples, ou quand leur introduction est envisagée, il est indispensable de prévoir des garanties. En premier lieu, il convient qu'elles soient établies sur une base juridique. Ce cadre juridique doit définir

leur utilisation avec précision. Quand il n'existe aucune base légale pour demander à une personne de communiquer son PIN, cette dernière doit être informée que son refus n'aura aucune conséquence négative. Ce principe devrait apparaître dans le cadre juridique de l'introduction et de l'utilisation des PIN.

iii. Un cadre juridique pour l'introduction et l'utilisation des PIN universels ou à usages multiples garantit que les PIN spécifiques ne sortiront pas du contexte pour lequel ils ont été créés pour s'étendre à tous les secteurs, et ce sans le débat public nécessaire ni le cadre juridique qui doit accompagner les identifiants universels. Il est donc important de prendre des précautions pour que les PIN spécifiques restent cantonnés à leurs contextes spécifiques. Si le PIN est demandé sans autorisation légale, la personne concernée ne doit pas être obligée de le donner pour un contexte autre que celui défini à l'origine pour ce PIN. Une fois de plus, dans un tel cas, la personne doit pouvoir refuser sans subir des conséquences négatives. Il conviendrait même de déclarer illégal pour tout organisme public ou privé le fait de demander le PIN d'une personne sans autorisation légale.

iv. Les comparaisons de fichiers ou la connexion de bases de données à caractère personnel à l'aide des PIN méritent toute notre attention. Cette utilisation des PIN devrait être surveillée et limitée par des mécanismes spécifiques afin d'empêcher les pouvoirs publics d'acquérir trop de pouvoir. Toute tentative de connexion de fichiers détenus par divers départements de l'administration doit se faire dans la transparence. Il convient de déterminer à l'avance les circonstances dans lesquelles les fichiers de divers départements de l'administration peuvent ainsi être connectés. Cette opération devrait nécessiter une autorisation légale, comme celle de l'autorité chargée de la protection des données.

v. Etant donné que les PIN se rapportent à des personnes identifiées, ils constituent des données à caractère personnel. Ils sont donc soumis aux principes relatifs à la qualité des données. Nous avons déjà mentionné ce facteur pour démontrer que les autorités chargées de la protection des données sont compétentes pour superviser l'utilisation que les organismes publics et privés font des PIN. Nous pensons toutefois que leur introduction et leur utilisation entraînent également l'octroi de droits et de recours aux personnes concernées par la législation relative à la protection des données. Les personnes devraient donc par exemple jouir du droit de faire rectifier la composition d'un PIN quand celui-ci ne correspond plus à leur situation ou état. Si le PIN indique par exemple la nationalité ou l'état civil de la personne, il doit être assorti d'un droit de rectification permettant au porteur de faire modifier ce numéro si des changements interviennent dans la nationalité, le mariage ou le veuvage. La structure des PIN ne devrait pas faire appel à des données sensibles ou révéler ces dernières. Le PIN ne devrait pas indiquer la nationalité, l'origine ethnique, etc. Mieux encore, il convient de s'efforcer de composer des PIN sans faire appel à aucune donnée à caractère personnel. On pourrait par exemple utiliser des numéros de série ou «neutres». Si le PIN est composé de données à caractère personnel, celles-ci ne doivent pas être excessives ou sans rapport avec l'utilisation immédiate à laquelle ce PIN est destiné.

vi. La composition du PIN doit permettre à son porteur de le comprendre. Le codage de ce PIN ne doit donc pas empêcher le porteur de comprendre le sens des chiffres et des lettres, ou références, qui composent ce PIN.

vii. Il convient d'informer les personnes sur les dispositions à prendre pour utiliser leur PIN correctement et pour se protéger contre d'éventuels abus par des tiers.

Dans la présentation des présentes propositions, les rédacteurs se sont limités aux divers types de numéros d'identification. Ils sont toutefois conscients du fait que d'autres identifiants (nom, adresse, etc.) peuvent permettre aux pouvoirs publics de comparer les différents types de fichiers de données à caractère personnel. Ils pensent que ces instruments de connexion de banques de données posent les mêmes problèmes pour les libertés individuelles et les droits des personnes. Les principes présentés plus haut pour les garanties légales et la transparence dans la connexion de fichiers s'appliquent donc également aux identifiants autres que les PIN, tout comme le principe de la séparation des fonctions.

Les rédacteurs sont également conscients des nouvelles techniques utilisées pour identifier les personnes, comme les empreintes génétiques, l'identification par la voix et celle par l'iris. Les rédacteurs en concluent qu'il convient d'exercer une grande prudence avant d'introduire et d'utiliser de tels identifiants. Il convient en particulier de susciter un débat public sur ces sujets afin de trouver un équilibre acceptable entre la protection de la vie privée et les avantages potentiels de ces méthodes.