Secrets d'Etat et vie privée

Poullet, Yves; Havelange, Benedicte

Published in:
Proceedings ¿ Staatsgeheim of transparantie ? ¿ Secret d¿Etat ou transparence ?,

Publication date:
1999

Document Version
le PDF de l'éditeur

SECRETS D'ETAT ET VIE PRIVÉE : OU COMMENT CONCILIER L'INCONCILIABLE ?

Yves POULLET
Professeur à la Faculté de Droit des FUNDP et au DES-DGTIC
Directeur du CRID (FUNDP)
Membre de la Commission belge de la Protection de la vie Privée
(Email : yves.poullet@fundp.ac.be)

Bénédicte HAVELANGE
Collaboratrice scientifique au CRID
Conseiller à la Commission de la Protection de la Vie privée [1]

COLLOQUE DU 20 JANVIER 1999
« SECRET D'ETAT OU TRANSPARENCE » - BRUXELLES

(1) Les auteurs s'expriment à titre personnel et n'entendent en aucune manière engager la Commission de Protection de la Vie privée. La présente contribution a bénéficié du soutien des S.S.T.C. dans le cadre du Programma d'Action Interuniversitaire (PAI) : la societé de l'information qui réunit 4 centres de recherche : CITA et CRID (FUNDP), LENTIC (ULG) et SMIT (VUB).

INTRODUCTION

1. Le titre même du présent exposé sous-entend un antagonisme entre deux intérêts: le secret d'Etat, d'une part, et la protection de la vie privée des citoyens, d'autre part. Or, il nous paraît important de souligner ceci: dans un grand nombre d'hypothèses, secret d'Etat et protection de la vie privée peuvent s'épauler mutuellement.

   La personne fichée a tout intérêt à ce que les données la concernant soient aussi bien protégées que possible contre la diffusion à des tiers non autorisés, ou l'altération accidentelle, ...

   En d'autres termes, si la personne est fichée, il y a certes une intrusion dans sa vie privée, intrusion d'autant plus grave qu'elle est le fait d'un service secret. Mais, si intrusion il doit y avoir, mieux vaut qu'elle ne s'accompagne pas d'une diffusion incontrôlée de l'information recueillie.

   La loi de 1992 impose d'ailleurs des mesures de sécurité technique et de respect de la confidentialité au maître du fichier. D'une certaine manière, la personne concernée est également protégée par le respect strict du secret.

   Il paraît donc important que, dans les débats ayant trait au secret, les aspects de protection de la vie privée soient pris en compte. La proposition que fait le Comité R, à savoir l'inclusion de la vie privée parmi les intérêts que peut protéger une mesure de classification, rejoint cette préoccupation.

   Toutefois, on ne perdra pas de vue que, si la vie privée est un des intérêts que protège la classification, elle n'est certes pas d'une importance primordiale pour la défense ou la sûreté de la nation, et ne jouirait que d'un niveau de classification faible. La protection spécifique de la vie privée doit rester totalement d'application.

   La loi de 1992 vise à la protection d'un droit fondamental, et le fait que les mêmes informations ne présentent pas grand danger pour la sécurité de l'Etat ou sa défense ne peut en rien aboutir à un affaiblissement de ladite protection.

   Rappelons en outre qu'une mesure de classification entraîne l'inapplicabilité de la loi de 1994 sur la publicité de l'administration[2]. En d'autres termes, si des données personnelles sont classifiées, la personne concernée ne pourra en obtenir la consultation.

   Perdant ce moyen de contrôle, la personne concernée doit pouvoir compter sur une application parfaitement rigoureuse des principes protecteurs de la vie privée. On souligne également la nécessité d'effectuer une balance entre l'intérêt de la personne concernée et la nécessité du secret avant de classifier un document.

2. Plusieurs décisions de la Cour européenne des droits de l'Homme consacrent sur base de l' article 8 de la Convention européenne des droits de l' Homme ce devoir de mettre en balance les intérêts respectifs en cause, également lorsqu'il s'agit de juger de la légitimité de prise de renseignements ou de conservation de données personnelles.

---

(2) En vertu del'article 26 du projet de loi relatif à la classification et aux habilitations de sécurité (voir infra).

L'arrêt LEANDER, rendu à propos de la contestation d'un citoyen convaincu d' être fiché par la sûreté de l' Etat de son pays et se voyant opposer le dogme de la sécurité de l' Etat, proclame la nécessité de mettre en balance, d' une part, la protection du droit à la vie privée, droit consacré chez nous par l'article 22 de la Constitution, et, d'autre part, les impératifs de sécurité et d' ordre public qui fondent les services de renseignements et de sûreté. L' arrêt ajoute l'obligation pour réaliser cette balance de l'intervention d' une autorité indépendante.

Nous reviendrons sur cette seconde condition plus loin lorsque nous étudierons à propos de l' accès indirect, le rôle de la Commission de Protection de la Vie Privée.

L' importance de cette balance assigne des limites à la collecte et au mode de collecte des informations des services de renseignements et de la sûreté de l' Etat tant lorsque cette collecte vise un citoyen quelconque que lorsqu' il s'agit d' agents ou de préposés à la sécurité de l 'Etat.

Ce même équilibre doit être trouvé dans l' utilisation qui est faite des données et finalement fixe des limites à la transparence ou à la non transparence des données vis-à-vis des personnes concernées.

3. Ces deux considérations préliminaires nous guideront dans les réflexions qui suivent. Un premier chapitre analyse la façon dont les législations "vie privée", en particulier la directive européenne et notre loi fédérale récente, abordent la question des "traitements" en vue d' assurer la sûreté de l' Etat. Le deuxième chapitre inverse les termes du débat.

La loi organique des services de renseignements et de la sûreté de l'Etat approuvée récemment[3] de même que la loi relative à la classification et aux habilitations de sécurité contiennent des dispositions qui ont trait directement ou indirectement aux traitements de données personnelles. Dans quelle mesure, respectent-elles les exigences des législations de vie privée.

Le troisième et dernier chapitre analyse la question de l' accès des citoyens aux traitements des données détenus par les services susnommés et les limites assignées à la transparence de tels fichiers par le système d 'accès dit indirect.

CHAPITRE LA RÉGLEMENTATION "VIE PRIVÉE" ET LA "SÛRETÉ DE L 'ETAT"

4. Le chapitre analyse successivement la manière dont la directive européenne 95/46 dite directive générale de protection des données aborde les traitements de la défense ou de la sûreté de l'Etat; ensuite, elle opère un rapide tour d' horizon de droit comparé, se concentrant en particulier sur les textes nouveaux émis depuis la directive ou fondé sur elle. Enfin, elle détaille la solution originale du droit belge sur base du texte de loi soumis à la signature royale.

---

(3) Loi organique du 30 novembre 1998 des services de renseignements et de sécurité - Moniteur Belge, 18 décembre 1998.

1. LE POINT DE VUE EUROPÉEN

5. Deux dispositions mentionnent la question particulière des traitements de données à caractère personnel opérés pour des finalités de défense ou de sûreté de l' Etat. A première vue, elles apparaissent contradictoires:

   L'exclusion du champ de la directive pour de tels traitements est proclamée par l 'article 3.2.:
   " *La présente directive ne s'applique pas au traitement de données à caractère personnel mis en oeuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application au droit communautaire, telles celles prévues aux titres V et VI du Traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité physique, la défense, la sûreté de l'Etat (y compris le bien-être économique de l'Etat lorsque ces traitements sont liés à des questions de sûreté de l'Etat) et les autorités de l'Etat relatives à des demandes du droit pénal*". (cfr. en outre le considérant n° 13).

   A l' inverse, l' article 13 dispose que :
   " *Les Etats membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 § 1, à l'article 10, à l'article 11 § 1 et aux articles 12 et 21, lorsqu'une telle limitation est nécessaire pour sauvegarder:*

   a) la sûreté de l'Etat;

   b) la défense;

   c) la sécurité publique;

   d) (...);

   e) un intérêt économique ou financier important d'un Etat membre ou de l'Union européenne;

   f) (...) " (cf. également sur ce point, le considérant n° 43).

6. Comment comprendre cette apparente contradiction ? La directive est - elle applicable ou non aux traitements opérés par la sûreté de l' Etat ou par les services de renseignements ?

   La lecture attentive de la directive conduit à résoudre aisément cette apparente contradiction et à distinguer parmi les fichiers qui ont pour finalité d' assurer la défense ou la sûreté de l' Etat deux types de fichiers ou de traitements: les premiers concement des traitements qui échappent à la directive dans la mesure où ils sont opérés par des institutions qui échappent à toute réglementation européenne, ainsi les traitements opérés par les services de renseignements et de sûreté de l' Etat.

Par contre, certains traitements sont opérés par des organes privés et publics dont les activités sont indiscutablement régis par la directive mais qui occasionnellement devront de gré ou de force collaborer avec les organes premièrement nommés.

Ainsi, le service d' audit d' une banque chargé de détecter des opérations de blanchiment d 'argent sera tenu de transmettre des informations à la sûreté de l' Etat; l' employeur d'une usine d' armement, etc.

Tous ces responsables de traitements sont soumis aux prescrits de la directive et il est dès lors nécessaire que certaines exceptions existent pour de tels traitements contribuant aux missions de sûreté de l 'Etat. Cette nécessité est reconnue par l'article 13 précisément.

Cette précision apportée, qu'il soit clair que les traitements exemptés de l'application de la directive restent soumis au respect de l' article 8 de la Convention européenne des Droits de l'Homme dont la portée a été rappelée çi avant (n°2).

7. L'analyse de l 'article 13 qui est applicable partiellement à certains traitements contribuant à la sûreté de l' Etat ou à sa défense est intéressant dans la mesure où elle apparaît comme une application des principes déduits de l' article 8 de la Convention européenne qui s' impose dès lors à notre législateur.

   L'article 13 crée la faculté pour les Etats de prévoir des exceptions, il ne les impose pas. L'emploi du terme "peuvent" est à cet égard significatif. Ensuite, les exceptions ne doivent être prononcées que dans la mesure où 'de telles restrictions apparaissent nécessaires'.

   Ce rappel du principe de la proportionnalité, consacré à de multiples reprises par la jurisprudence de la Cour européenne de Strasbourg, obligent le législateur national à motiver l' octroi d'une dérogation aux prescrits de la vie privée et à s 'interroger sur les limites d 'une telle dérogation.

   Enfin, les possibilités d 'exception sont précisées : l'article 6 §1, c'est-à-dire le principe de la collecte loyale mais non les autres paragraphes de cet article qui imposent le devoir de qualité des données (pertinence, exactitude, . ..), la nécessité de finalités légitimes et déterminées ainsi que le principe d'incompatibilité; les articles 10 à 12 relatifs aux devoirs d'information et au droit d'accès de la personne concernée; l'article 21 relatif à la publicité du registre des traitements tenus par l' Autorité de contrôle.

2. LE DROIT COMPARÉ

8. Notre tour d' horizon se limite à un bref aperçu de quelques réglementations ou projets de réglementation récents parmi lesquels nous distinguerons les approches suivantes, celle illustrée par le projet de loi néerlandais qui réglemente les traitements de la sûreté de l' Etat et des services de renseignements par une législation séparée; celle de la loi grecque qui ne prévoit aucune dérogation à la loi de protection des données; celle des lois italienne, portugaise et britannique qui prévoit des exceptions partielles selon des modalités diverses.

9. Peu de choses à dire de l'exemple hollandais dont le projet de loi récent en matière de protection des données maintient le système déjà en vigueur sous l 'empire de l'ancienne législation de vie privée.

L' article 2 du projet exclut du champ d' application de la loi de protection des données, les traitements soumis à la loi spéciale: la *"Wet op de inlichtingen- en Veiligheidsdiensten"* (1951) remaniée à plusieurs reprises.

Quelques principes caractérisent cette loi : celui de la proportionnalité et du minimum de mesures d' investigation ; la distinction de 3 degrés de classification des documents détenus par les services de sécurité et cela selon le degré de confidentialité du contenu des documents (cf. infra, la reprise de ce système en Belgique); enfin la responsabilisation des fonctionnaires habilités.

10. L'exemple italien est sans doute proche de celui choisi en Belgique mais il part du principe de la non application de la loi de protection des données contrairement à notre législation.

Selon l 'article 4 al.1, la loi ne s'applique pas aux:

b) "organismes visés aux articles 3 (...) de la loi n° 801 du 24 octobre 1977 ou à l'égard de données couvertes par le secret d'Etat.

c) d'autres organismes publics aux fins de défense ou de sûreté de l'Etat, (...) sur la base de dispositions de lois spécifiques prévoyant expressément le traitement".

A ce principe de non application, l' alinéa 2 du même article introduit une importante nuance *"en tout état de cause, s'appliquent les dispositions des articles 9 (Qualité des données), 15 (Sécurité des données), 17 (Système d'aide à la décision), 18 (responsabilité), 31 et 32 (contrôle par le garante)".*

On ajoutera que l 'obligation de notification au garante est applicable également aux traitements visés à l'article 4 al.1b).

11 Comme la loi belge, la législation portugaise part du principe inverse de la loi italienne. L'article 7 prévoit l'application de la loi mais par la suite certaines dérogations sont prévues.

On les cite

Article 8

Possibilité de traitement de données judiciaires ou relatives à des activités illicites de même que des données sensibles si l'organisme de la sûreté de l'Etat ou le service de renseignements respectent les mesures de sécurité de l'information et les normes de protection des données et si le traitement s' avère nécessaire à l'exercice des fins légitimes de sécurité publiques et pour autant que ne prévalent pas les libertés et garanties du titulaire des données;

Article 10

Possibilité de dispense de l'obligation d'information de la personne concernée, si justification;

Article 11

Possibilité de dispense du droit d'accès de la personne concernée mais alors droit d'accès indirect.

12. Le Data Protection Act britannique est original à plus d' un titre. La Section 29 dispose: *"Personal Data are exempt"* de tout ou partie des prescrits de protection des données à l'exception, ajoute l' article, des dispositions relatives au pouvoir de contrôle du Registrar et du Tribunal.

L'article poursuit en énonçant deux conditions pour l' exemption

- l' exemption doit être requise pour la finalité de sécurité que poursuit le traitement et il faut démontrer que sans cette exemption, la sûreté de l 'Etat ou sa défense subirait un *"real Tort"*;

  l' exemption doit être décrite et définie par un *"public interest immunity certificate"* émanant du Ministre et décrivant à la fois l 'étendue des personnes concernées par le traitement exempt et les moyens utilisés pour la collecte des informations, ceci par une description qui peut rester générale.

On ajoutera que la loi crée pour les personnes concernées par le "certificate" une possibilité de recours devant le tribunal et le pouvoir pour celui-ci d'annuler le "certificate".

3. LA LOI BELGE ADOPTÉE LE 1ER DÉCEMBRE 1998 TRANSPOSANT LA DIRECTIVE ET MODIFIANT LA LOI DU 8 DÉCEMBRE 1992

13. L' article 4 de la loi modifie fondamentalement l' article 3 ancien en disposant au § 4 :
" *Les articles 6 à 10, 12, 14, 15, 17, 17 bis, al. 1, 18, 20 et 31 §§1 à 3, ne s'appliquent pas aux traitements de données gérées par la sûreté de l'Etat, par le Service général du Renseignement et de la Sécurité des Forces Armées, par l'Autorité de sécurité, par les offices de sécurité et par le Comité permanent de contrôle des services de renseignements et son Service d'enquêtes, lorsque ces traitements sont nécessaires à l'exercice de leurs missions".*

L' exposé des motifs voit dans cette disposition une application de l' article 13 de la directive ci-avant commentée. Nous avons déjà souligné que la disposition de la directive bien qu 'ayant un champ d 'application plus limité représente une traduction des principes de la jurisprudence de l' article 8 de la Convention européenne des Droits de l' Homme qui est de toute façon applicable aux traitements en cause.

Quelques remarques à propos du libellé de la disposition belge

premièrement, la loi de protection de la vie privée, sauf exception sur lesquelles nous reviendrons, est désormais d'application pour les traitements de sûreté de l'Etat et de défense nationale.

En d'autres termes, ils ne sont plus exemptés de la loi.

deuxièmement, on note que le champ d'application de l'exception est plus large que celui prévu par la disposition de la loi de 1992 ancienne version.

La formulation précédente exemptait uniquement les traitements de l' Administration de la Sûreté de l'Etat et le Service général du renseignement et de la Sécurité du Ministère de la Défense nationale.

Dorénavant, sont également exemptés les traitements gérés (on s' interroge sur l' utilisation de cette notion existant dans la version de 1992 mais abandonnée par la nouvelle version) par l' Autorité de sécurité définie par une autre loi sur laquelle nous reviendrons comme l'organe de coordination entre sûreté de l'Etat et service de renseignement (article 15 de la loi relative à la classification et les habilitations de sécurité) et par les officiers de sécurité (personnes en charge de la sécurité établies dans chaque département ministériel et dans chaque personne morale titulaire d'une habilitation de sécurité (art. 13 de la même loi relative à la classification).

Troisièmement, on note que les traitements ainsi gérés pour autant que nécessaires à la mission des organes ou institutions ainsi nommés échappent automatiquement et globalement à un certain nombre de dispositions de la loi : ainsi, on relève que ne seront pas d 'application:

les articles 6, 7 et 8 relatifs aux conditions particulières de traitement des données sensibles, de santé ou judiciaires ;

l' article 9 à propos de l' obligation d'informer la personne concernée en cas de collecte de données auprès d 'elle ;

l'article 10 à propos du droit d'accès ;

l' article 12 qui autorise l 'objection à un traitement pour des motifs particuliers et sérieux tenant à la situation de la personne concernée ;

l' article 14 permettant le recours devant le président du tribunal de 1ère instance mais créant aussi une obligation de réagir à charge du responsable du traitement en cas de contestation d'une donnée ;

l' article 15 obligeant à affecter d 'un indice de doute les données contestées ;

l' article 17 qui impose la notification du traitement à la Commission de protection de la vie privée ;

l' article 17bis prescrivant des possibilités de réglementation particulière pour certaines catégories de traitement et mentionnant la possibilité de désignation au sein du responsable du traitement d 'un détaché à la protection des données ;

l' article 18 qui crée un registre public;

l' article 20 qui prévoit un système spécifique d 'autorisations pour certains traitements présentant des risques sérieux d 'atteinte à la vie privée ;

enfin, 'article 31 § 1à 3 qui autorise la plainte de particuliers auprès de la Commission.

14. Le détail de la longue liste d' exceptions laisse apparaître en creux les dispositions maintenues à propos des traitements en cause. On note en particulier que la loi ne prévoit pas de dérogations à l' article 4 nouvelle version de la loi, article considéré comme le noyau dur de la protection relatif à la qualité des données.

Cet article établit les principes de loyauté des traitements, de collecte pour des finalités légitimes, déterminées et explicites, de la non utilisation des données à des fins incompatibles à celle de la collecte originaire, de proportionnalité du contenu et de la durée des traitements aux finalités de la collecte, de l' exactitude et de la mise à jour des données.

Il est clair que le respect intégral de ces principes, sous réserve d'une interprétation lâche de leur portée, soulève quelques difficultés appliqués aux domaines qui nous concernent. Nous reviendrons sur ce point mais relevons dès maintenant que la directive proposait en tout cas des possibilités de dérogations au principe de collecte loyal.

La loi ne prévoit pas non plus de dérogations à l 'article 5 nouvelle version de la loi.

Ainsi, les traitements seront légitimes si et seulement si ils sont soit l' exécution d'une obligation légale (par exemple devoir de communication des officiers de sécurité vis-à-vis de la sûreté de l' Etat dans les cas prévus par la loi relative à la classification et aux habilitations de sécurité *(point c) de l'article 5)*, soit opérés en vertu du consentement de la personne concernée *(point a) de l'article 5 applicable sous réserve de nos critiques ultérieures aux enquêtes de sécurité prévues lors de la nomination d'officiers de sécurité)*, soit nécessaire à la protection de l' intérêt vital de la personne concernée *(point d) de l'article 5 applicable à propos des traitements opérés par les services de renseignements dans le cadre de leur mission de protection de certaines personnes menacées)*, soit nécessaires à l'exécution d'une mission d 'intérêt public ou relevant de l 'exercice de l 'autorité publique dont est investi le responsable du traitement à condition que ne prévalent pas l 'intérêt ou les droits et libertés fondamentaux de la personne concernée *(point e) de l'article 5)*.

C' est à propos de ce dernier type de traitements les plus nombreux dans le secteur étudié que s' appliqueront les principes de la jurisprudence de l' article 8 de la Convention européenne des droits de l 'Homme et que se justifie une pondération des intérêts de la sécurité publique ou de la défense nationale et ceux des personnes concernées de même que la possibilité d' intervention d' une autorité indépendante.

15. D'autres dispositions également importantes restent d'application: l' article 12bis introduit certaines limites à l' utilisation de systèmes d' aide à la décision utilisant des moyens automatisés et oblige à ne point s' en suffire avant de prendre une décision vis-à-vis d' une personne concernée.

La disposition prend tout son sens dans le secteur concerné dans la mesure où souvent de vastes fichiers sont susceptibles d'être analysés automatiquement dans la recherche de suspects potentiels et dans leur classement comme personnes à risque.

Le devoir de prendre des mesures de sécurité adéquates au regard de la nature des données, des flux d 'informations en cause et des risques d 'atteinte à la confidentialité est prescrit par l 'article 16 de la loi.

Son application exige dans un secteur aussi sensible que celui de la sûreté de l' Etat ou de sa défense une attention toute particulière. A cet égard, l'existence du Comité R, les nouvelles mesures introduites par la loi organique et la loi relative à la classification et aux habilitations de sécurité constituent des mesures importantes.

On regrette cependant que leur objectif ne soit pas directement la protection des personnes concernées même si elles peuvent indirectement contribuer à cette protection. Nous reviendrons plus loin à l' intérêt de certaines mesures comme la nomination d 'un détaché à la protection des données.

Outre l' application intégrale du chapitre de la loi sur les dispositions pénales (article 37 et ss.), on ajoute que la Commission de protection de la vie privée dispose vis-à-vis des traitements en cause comme vis-à-vis de tout traitement d 'un pouvoir d 'injonction quant à la communication de certaines informations (article 19 de la loi) que cette même Commission peut prendre d'initiative des recommandations à l'encontre des responsables des traitements (article 30) et peut enquêter auprès de tels services (article 32).

16. De ce bref tour d' horizon, tirons quelques conclusions critiques sur les choix opérés par le législateur belge et ses conséquences :

Fallait-il prévoir autant d'exceptions et les rendre automatiques ?
Ne pouvait-on se contenter d'affirmer que les exceptions ne pouvaient être utilisées que si nécessaires à la finalité des traitements et compte tenu de la nature des données, de la qualité du demandeur, etc.?

L'article 8 de la Convention européenne des droits de l' Homme et l' exemple des législations étrangères attestent que chaque exception ne se justifie pas en soi pour un secteur déterminé mais au regard des caractéristiques d 'un type particulier de traitements opérés au sein de ce secteur.

Ainsi, les enquêtes de sécurité à propos des candidats officiers de sécurité exigent l' information préalable voire le consentement des personnes candidates (c'est-à-dire l 'application de l' article 9 de la loi), comme le reconnaît la loi relative à la classification et aux habilitations de sécurité, application donc d 'un article dont normalement est exempté le secteur de la sûreté et de la défense.

Le même raisonnement n 'est-il pas applicable dans bien d' autres cas (cfr. ci après l 'exemple du droit d 'accès) et n' aurait-il pas dès lors été préférable d' affirmer sur le modèle portugais, italien et britannique que dans des cas justifiés tel ou tel articles ne seront pas applicables, mettant ainsi à charge des organismes de sécurité et de défense nationale le soin d 'établir les motifs pour lesquels ils réclament pour certains types de traitements le bénéfice d' une dérogation.

A l' inverse, on s'étonne de ne pas trouver dans la liste des exceptions possibles, la possibilité de dérogation au principe de collecte par des moyens loyaux c 'est à dire dans des conditions telles qu 'un minimum de transparence existe aux yeux des personnes concernées.

L' utilisation de moyens tels que la vidéosurveillance, les enquêtes auprès de tiers, l'infiltration de groupes clandestins sont certes nécessaires dans certains cas du moins c'est-à-dire lorsque le moyen est proportionné au risque à prévenir et étant donné l' absence d' autres

possibilités d 'obtenir l 'information (cf. à cet égard, l' arrêt Lüdi (15 juin 1992) de la CEDH abondamment cité par l' exposé des motifs de la loi organique).

A nouveau, il ne s' agit pas d'octroyer une exception automatique aux traitements visés mais une possibilité de dérogations à charge pour les responsables de la motiver.

Une troisième réflexion concerne le champ d 'application des exceptions. Comme il a été souligné, l' article 13 autorise des exceptions pour des responsables de traitement en communication avec la sûreté de l' Etat et les services de renseignements, ainsi une banque contactée par la sûreté de l 'Etat pour vérifier si telle personne suspecte a utilisé sa carte de crédit à tel endroit a en principe le devoir d'informer la personne concernée de la communication de la donnée, suite à l' exercice par la personne concernée de son droit d' accès.

La Directive permet dans de tels cas des dérogations à l'application de ses prescrits. Une dérogation est-elle possible en droit belge ? C'est discutable mais en tout cas certainement pas sur base de la nouvelle version de l 'article 3.

La quatrième remarque amplifie une remarque adressée à juste titre par le Conseil d' Etat au projet de loi de protection de la vie privée. Le Conseil d' Etat (p. 193) note que *"l' importance des dérogations affaiblit sérieusement les garanties instaurées par la loi"*.

Cette réflexion l' amène à suggérer que dans son rapport annuel prévu par l' article 32 de la loi, la Commission de protection de la vie privée consacre un chapitre particulier aux constatations et observations adressées à ce secteur particulier.

Notre réflexion élargit ce propos. La loi consacre un dangereux déséquilibre entre les impératifs légitimes de la sécurité de l' Etat et de sa défense et les intérêts de la personne concernée dans la mesure où la loi affaiblit de manière disproportionnée les possibilités de contrôle du respect des prérogatives liées à la protection des données.

Ainsi, la loi dispense les traitements de toute notification à la Commission. Comment dans ces conditions, la Commission peut-elle connaître l' état des traitements au sein des organismes et opérer les investigations nécessaires?

Par ailleurs, l' article 17 bis n'est pas applicable. Or comme le note le Conseil d' Etat (p. 192) une telle dérogation est injustifiable alors même que les traitements en question représentent un risque important pour les libertés des citoyens et que les mesures prévues par cet article comme des garanties supplémentaires en matière de sécurité ou de procédures de motivation voire et surtout l' existence d' un préposé à la protection des données, mesure prévue explicitement par l 'article en cause, eussent été utiles.

- Insistons sur ce dernier point, la nomination d' un contrôleur interne, d' un détaché ou d'un préposé à la protection des données, mesure reprise par la directive sur base de l 'expérience allemande, eût été particulièrement utile dans la mesure où elle aurait facilité le contrôle de la Commission, qui aurait trouvé en cette personne un allié sensible au respect des prescrits de la loi et chargé de veiller à leur respect en première ligne.

Nous reviendrons sur ce point important dans la suite de nos réflexions et en conclusion.

CHAPITRE II : LES RÉGLEMENTATIONS RELATIVES À LA SÉCURITÉ DE L'ETAT ET AUX SERVICES DE RENSEIGNEMENTS FACE AUX EXIGENCES DE LA LOI "VIE PRIVÉE"

1. PRÉSENTATION DES LÉGISLATIONS RÉCEMMENT ADOPTÉES EN LA MATIÈRE - HISTORIQUE DE LA LOI ORGANIQUE

17 Deux lois votées récemment et soumises à la signature royale organisent les services de renseignement et de sûreté et déterminent leurs moyens d' action :

la loi relative à la classification et aux habilitations de sécurité (Chambre des Représentants 1193/11 - 96/97):
cette loi fixe, suivant le critère de gravité des informations contenues, la nature plus ou moins confidentielle des données, détermine sur cette base les personnes habilitées à les traiter et consacre le droit d'investigation de ces services vis-à-vis des personnes, habilitées ou à habiliter comme officier de sécurité;

- la loi organique des services de renseignement et de sécurité (Sénat 1-758/10, 11 et 15, Moniteur belge, 18 décembre 1998) définit les missions de ces deux organismes et dès lors la finalité des traitements opérés par eux ; de même, elle fixe quelques principes à suivre dans les traitements des données y compris lors de la collecte des données.

Si la seconde loi prime certes la première, dans la question qui nous occupe, il est difficile de ne pas les lier et d' essayer d' en opérer une lecture commune.

Plus difficile encore, s' avère la coordination de ces deux lois avec la loi de protection des données personnelles dont elle représente une application sectorielle.

Avant d 'aborder l' analyse du contenu des lois et de leur respect ou non des prescrits de protection de la vie privée, quelques remarques sur l' historique de la loi dite organique illustrent l 'importance du débat.

18 La loi organique des services de renseignement et de sécurité a connu une genèse difficile qu on peut décrire en huit temps.

le premier est la constatation par la jurisprudence de l 'absence de tout fondement légal à l'action de la sûreté de l' Etat et des Services de renseignements généraux et dès lors leur contestation.

Deux arrêts du Conseil d' Etat, le premier dans l' affaire dite Cudell (arrêt n° 54-138) et le second dans l'affaire dite Wicart (30/6/95, arrêt n° 54-139) à propos d' une sanction prise à l' encontre d' un fonctionnaire de la sécurité et une décision du tribunal de 1ère Instance de Bruxelles (24ème chambre) (R.G. 95/14503 Arrêt dit Vlaams Blok (collecte d'informations prise contre des membres d'un parti politique)) rappellent avec énergie la jurisprudence constante

de la Cour européenne des droits de l' Homme pour dénier tout droit de la sûreté de l' Etat et des services de renseignement à la collecte et aux traitements d' informations vis-à-vis de citoyens ou de manière plus large, d' individus :

Considérant que l'article 8 § 2 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales permet l'ingérence de l'autorité publique dans l'exercice du droit de toute personne au respect de sa vie privée, pour autant que cette ingérence est conforme à la loi, qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire notamment à la sécurité nationale et à la sûreté publique, et que les textes qui la prévoient soient accessibles à l'intéressé et rédigés en termes assez clairs pour lui indiquer de manière adéquate quelles circonstances et sous quelles conditions, ils habilitent la puissance publique à s'y livrer, spécialement si l'ingérence présente un caractère secret" (arrêt Wicart).

En réponse à cette critique fondamentale qui ruinait toute l 'action des organismes de sécurité et de défense de l' Etat, le gouvernement met sur la table dessiné à la hâte un avant-projet de loi organique des services de renseignement et de sécurité qui sera soumis fin 95 à la lecture critique du Conseil d' Etat (3ème temps).

L' avis du Conseil d' Etat en date du 27 mars 1996 (publié en annexe des Doc. Parl. de la Chambre des Représentants) est lourd de critiques vis-à-vis du texte gouvernemental.

Si le Conseil d'Etat salue la volonté gouvernementale d'asseoir législativement les prérogatives des organismes en question, il ajoute :
" *Le principal mérite de l'avant-projet est d'ailleurs d'admettre la nécessité de cette intervention"(p. 29).*

Le Conseil d'Etat entre autres critiques dénonce sans ambages l 'absence de juste équilibre que traduit le texte entre les intérêts à prendre en considération:

S'il peut être admis que l'autorité publique se dote de services dont la fonction spécifique consiste à lui fournir les renseignements propres à lui permettre, par les décisions adéquates, de réprimer les atteintes répréhensibles aux intérêts dont elle assume la responsabilité, il reste en effet que la loi doit aussi prémunir la collectivité contre le préjudice que pourraient à la faveur de secret qui les caractérise habituellement, porter ces activités au libre exercice des droits fondamentaux" (p. 31).

Il réclame dès lors que le gouvernement se convainque de la nécessité *"de l'existence de garanties adéquates et suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre" (p. 31 citant l'arrêt Leander de la CEDH).*

A cet égard, la haute autorité réclame la nécessité de précisions dans la loi quant aux limites de l'action des services :

En outre, lorsque sa mise en oeuvre s'opère au moyen de mesures concrètes, échappent au contrôle des personnes concernées comme au public, la loi elle-même, par opposition à la pratique administrative dont elle s'accompagne, doit définir l'étendue du pouvoir d'appréciation attribué à l'autorité compétente avec assez de netteté -compte tenu du but légitime poursuivi - pour fournir à l'individu une protection adéquate contre l'arbitraire (p. 33)".

Ainsi, le Conseil d' Etat met en doute la déclaration d' intention du gouvernement

Chacun des services de renseignement et de sécurité veille au respect et contribue à la protection des libertés et des droits individuels qu'au développement démocratique de la société" en ironisant : " ce qui est assurément une bonne intention, la nécessité de l'exprimer ainsi vient sans doute de ce que le texte en projet ne la réalise guère par ailleurs "(p. 35).

En conclusion, note la haute autorité, la loi en projet est tout à fait dépourvue de règles 'claires et détaillées' ayant trait à la collecte et l'usage des informations (p. 35 C.E. citant l'arrêt Kruslin 24 avril 1990).

Le Conseil d' Etat ajoute par ailleurs l' obligation pour le Gouvernement de saisir pour avis la Commission de protection de la vie privée.

A cette critique fondamentale, le gouvernement adressera une réponse énervée et peu satisfaisante: le projet de loi est déposé sans grande modification le 2 juillet 1996 à la Chambre des représentants et voté lors de la séance du 23 octobre 1997 (Doc. 638 - 95/96).

Le cinquième temps est le passage du texte au Sénat qui modifie profondément le texte de la Chambre et introduit notamment des règles plus détaillées suivant les différentes étapes du traitement des données par les services sus-mentionnés (collecte / utilisation / communication/ conservation).

Par ailleurs, le Président du Sénat, le 12 février 1998, réclame l' avis de la Commission de protection de la vie privée.

L'avis (avis n° 12/98 du 23 mars 1998) de la Commission sera défavorable. On reprend ci après le passage le plus significatif de cet avis :

Le raisonnement suivi par le Gouvernement, conjugué au peu de considération accordé aux remarques formulées par le Conseil d'Etat sur les lacunes du projet en matière de protection des données à caractère personnel, semble indiquer que le but du projet est d'entériner le caractère discrétionnaire de l'action de nos services de renseignement et de sécurité". (Avis, p. 5).

Le texte sera alors revu légèrement par le Sénat. On note également une décision de la Commission parlementaire de concertation entre Chambre et Sénat (Doc. Sénat I. 82-1995 (S.E.) n° 23, 26, 29 et 32). Le vote du Sénat interviendra le 16 juillet 1998.

Dernière étape, le texte amendé par le Sénat sera adopté par la Chambre des Représentants en séance plénière du 19 novembre 1998 et soumis à la sanction royale (Doc. Ch. Représ. 638/21-95/96).

2. ANALYSE DES DISPOSITIONS DES DEUX LOIS AU REGARD DES EXIGENCES DE LA LOI DE PROTECTION DES DONNÉES

19. La loi de protection des données établit un principe fondamental, celui suivant lequel les données ne peuvent être traitées que pour des finalités légitimes et déterminées.

De ce principe en découle un second qui affirme que le contenu des traitements doit être rigoureusement proportionné à l' obtention de ces finalités. L' application de ces deux premiers principes sera étudié au point 2.1.

Ensuite, nous suivrons la démarche proposée par la loi organique étudiant à chaque phase du traitement, collecte des données, utilisation interne et ensuite utilisation externe, enfin conservation des données comment les dispositions des deux lois peuvent être critiquées à l' aune des principes de protection de la vie privée.

2.1. La finalité des traitements et leur proportionnalité

20. *"Conformément à l'article 3 § 4 de la loi du 8 décembre 1992,(...), les services de renseignements effectuent les traitements nécessaires à l'exercice de leurs missions."*

La finalité des traitements opérés par la sûreté de l' Etat et les services de renseignement ressort à suffisance des articles 7 à 11 de la loi organique qui précisent les missions de ces deux organismes.

Cette description des missions obtenue finalement malgré les réticences du Gouvernement prend en compte les exigences de clarté et de précision réclamées par la jurisprudence Wicart et Vlaams Blok et par l'avis du Conseil d'Etat.

Sans doute, peut-on encore déplorer avec le Conseil d'Etat la persistance de certaines délégations du législatif à des pouvoirs subordonnés (cf. les exemples donnés par le Conseil d' Etat, p. 34 et sa conclusion sévère :

> *Il s'impose d'abord d'observer que ces dispositions délèguent l'ensemble du pouvoir de régler la matière y compris les principes essentiels. Ce pouvoir est au surplus attribué, non au Roi ainsi que le requiert l'article 108 de la Constitution, mais à un Comité ministériel qui pourrait lui-même abandonner assez discrétionnairement à un collège administratif, voire même aux services de renseignements et de sécurité, le soin de déterminer les modalités concrètes des enquêtes de sécurité".*

21 L'article 13 de la loi organique reprend au regard des missions préalablement définies une traduction imparfaite du principe de finalité et de proportionnalité. Il dispose que :

> *Dans le cadre de leurs missions, ils (les services de renseignements et de sûreté) peuvent rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de leurs missions et tenir à jour une*

documentation relative notamment à des événements, à des groupements et à des personnes présentant un intérêt pour l'exécution de leurs missions. Les renseignements contenus dans la documentation doivent présenter un lien avec la finalité du fichier et se limiter aux exigences qui en découlent."

Plusieurs remarques à propos de ce texte : premièrement, on note l'emploi du mot 'utile'. Les données (y compris à caractère personnel ?) même non nécessaires à l'accomplissement des finalités peuvent être collectées du moment qu' elles apportent une plus value voire un intérêt pour l' accomplissement des missions.

Les exigences de la loi vie privée sont plus sévères puisque l'article 5 de loi applicable aux traitements de la sûreté de l'Etat et des services de renseignements (cf. supra) exige un lien de nécessité.

Faut-il dès lors interpréter le texte de la loi organique comme une dérogation créée par une loi spécifique à la disposition d'une loi générale ou considérer que la disposition de la loi organique ne s' applique qu'aux traitements de données non personnelles ou à des dossiers non soumis à la loi de protection de la vie privée parce que vu leur défaut de structuration ils ne constituent pas un traitement ?

La question peut également être soulevée à propos du second alinéa qui à propos des renseignements des dossiers de documentation évoque la nécessité d' un simple 'lien avec la finalité du fichier'.

Ainsi, on peut constituer des dossiers épais de coupures de presse à propos d' un événement terroriste dans un lointain pays étranger et noter les points de vue de journalistes belges ou les photos prises à une manifestation en faveur de ces terroristes, manifestation organisée en Belgique.

De telles documentations ont certainement un lien avec les missions de la sûreté de l' Etat mais ce lien est peut-être trop lâche pour considérer comme légitime un tel traitement de ces données.

22. Sans doute, la mission largement exploratoire de l' activité des services en cause exige un certain relâchement par rapport aux exigences strictes de la loi vie privée mais ce relâchement ne peut conduire à justifier toute prise de renseignements.

La légitimité de celle-ci doit être appréciée aux regards des risques réels encourus par la sécurité ou la défense de l' Etat et sans doute doit être motivée de manière interne en tout cas afin que les contrôleurs internes et externes (supra : Chapitre I) puissent évaluer la proportionnalité entre les données collectées et traitées et les risques réels ou présumés encourus par l' Etat ou les citoyens.

Ensuite, des garanties procédurales devraient être prises (Qui décide de la tenue de la documentation? ; nécessité d' un réexamen périodique des traitements) (A cet égard, un parallèle avec les solutions proposées par la Commission à propos de la recherche proactive de la police serait utile).

2.2. Etapes du traitement et règles y applicables

23. Suite aux critiques virulentes du Conseil d'Etat, à savoir l'absence de règles précises et détaillées quant aux modalités des traitements opérées par les services de la Sûreté et du renseignement, le Sénat proposa l'insertion d'articles supplémentaires relatifs aux diverses étapes possibles des traitements.

Notons d'emblée que la notion de traitement que nous utilisons est celle proposée par la loi de protection de la vie privée. Curieusement, le terme "traitement" repris dans la loi organique s'écarte de cette compréhension et ne désigne qu'une étape précise, à savoir l'utilisation interne des données par les services susnommés.

2.2.1. La première étape : la collecte des données

24. Deux dispositions de la loi organique accordent aux organismes visés par cette loi un droit d'investigation 'tous azimuts' à la fois quant aux données à recueillir et quant aux modes de collecte.

L'article 16 de la loi organique énonce:

> *Conformément à l'article 3§3 de la loi du 8 décembre 1992,(...) les services de renseignement et de sécurité peuvent solliciter les informations nécessaires à leur mission, y compris des données à caractère personnel, auprès de toute personne ou organisme relevant du secteur privé".*

Quant à l'article 7, il affirme que *"Dans l'exercice de leurs missions, les services de renseignements et de sécurité peuvent notamment toujours pénétrer dans des lieux accessibles au public (...)".*

Les deux dispositions ci-dessus évoquées reposent sur deux postulats critiquables: le premier concerne la référence à l'exemption générale prévue antérieurement par l'article 3 § 3 de la loi du 8 décembre 1992, exemption dont nous avons vu qu'elle n'était plus d'actualité depuis la réforme de la loi (supra n° 13); la seconde est plus fondamentale encore.

Même s'il n'est plus repris explicitement dans le rapport du Ministre au Sénat, le postulat est largement affirmé et commenté dans l'exposé des motifs du projet de loi :

> " *Les services de renseignements et de sûreté de l'Etat ont comme tout citoyen, le droit, selon l'article 19 du Pacte international relatif aux droits civils et politiques des Nations Unies, de s'informer librement".*

25 A l'application de ce double postulat, la Commission et le Conseil d'Etat répondent de manière péremptoire. Au premier postulat, la Commission même si elle reconnaît (à l' époque, le texte du projet était encore en décision) que la directive exempte les traitements de la sûreté de l'Etat et des services de renseignements ajoute dans son avis (point 1.2.4.) que la jurisprudence de la

Cour européenne des Droits de l'Homme exige cependant certaines limites au droit de ces services de traiter les données :

" *Le projet ne prévoit ni les circonstances, ni les conditions dans lesquelles des données à caractère personnel peuvent être collectées. Ces deux précisions sont pourtant exigées par la Cour européenne des droits de l'homme (...). La Commission estime que ces précisions doivent être apportées en ce qui concerne l'ensemble des activités de renseignements dès lors qu'elles n'atténuent pas l'efficacité de ceux-ci de manière disproportionnée par rapport à la protection supplémentaire dont jouiraient les citoyens".*

Au second postulat, il est répondu de manière plus acerbe encore quant au fondement du raisonnement (Avis C.P.V.P., point 1.2.4., p. 4, cf. également l'avis du Conseil d'Etat, p. 31).

Ce pacte a précisément pour but de protéger le citoyen contre l'arbitraire de la personne publique, et non de justifier l'ingérence de celle-ci dans leur vie privée. (...) Ensuite, le citoyen ne recherche pas systématiquement de l'information alors qu'il s'agit d'une fonction spécifique de renseignement et de sécurité. Là où une réglementation générale de la collecte d'informations apparaîtrait comme une restriction à la liberté du citoyen, elle apparaît au contraire comme une protection de ce dernier lorsqu'elle s'applique à des autorités publiques".

26 Ces critiques péremptoires au droit des services concernés de collecter librement les données obligent à quelques réflexions complémentaires.

Rappelons tout d'abord que la disposition contenue dans l'article 5 de la loi vie privée, relative à l' utilisation de modes de collecte loyaux oblige si l'on désire des techniques de collecte s'écartant de ce principe, une exception de la réglementation par des lois particulières.

Le gouvernement admet la nécessité d'une intervention législative pour les interceptions de télécommunications ou les écoutes téléphoniques où la loi du 30 avril 1994, modifiée par la loi de 1998, ne les autorise à titre exceptionnel que pour les services de renseignements opérant à l'étranger en temps de guerre et dès lors implicitement les refuse dans les autres cas (on rappelle que la résolution du Conseil européen du 17 janvier 1995 relative aux interceptions légales du trafic de télécommunications (C 329/2) et le Mémorandum de Bruxelles du 25 octobre 1995 réclament par ailleurs une base réglementaire pour de telles interceptions).

Il refuse la nécessité d'une telle intervention réglementaire dans les autres cas (vidéosurveillance, enquêtes auprès de tiers, ...) au motif que cette intervention limiterait l'action des services en question et les préjudicierait dans leur lutte contre les atteintes à la sécurité de l'Etat.

Un tel refus est inacceptable. Certaines règles relatives aux modes 'déloyaux' de collecte devraient être prises (Avis du Conseil d'Etat, p. 31), sous peine d' illégalité de ceux-ci, ainsi quant à la proportionnalité entre le risque à prévenir et la mesure prise, quant à l'autorité qui autorise ce mode de collecte, quant aux modalités et à la durée de conservation des informations ainsi traitées.

On citera à ce propos, l' affaire Murray v. U.K. (1994) où la Cour de Justice de Strasbourg estima à propos de la prise par la police de photos d'une militante lors d'une manifestation publique et après son arrestation et ce nonobstant sa relaxation quasi immédiate que *"the taking of her*

photographs was solely related to her voluntary public activities" ne constituerait pas une "interférence" aux droits de la personne concernée à la vie privée.

On note qu'outre les critiques sévères de la doctrine à l'égard de cet arrêt (à ce propos L. Bygraeve, Data Protection Pursuant to the Right to Privacy in Human Rights Treatin, 6, I.J.L.I.T., 1998, p. 265), l' arrêt concerne la prise d'informations relatives à l'expression publique volontaire d'activités (cf. également, l'affaire semblable dite Friedl, non publié en date de 1995 (Series A, n° 305 B) où la Cour admet la non interférence mais note au surplus que la prise de photos était légitime dans la mesure où les autorités s'étaient abstenues de rechercher le nom des personnes présentes sur la photographie).

27. Les deux législations en question prévoient quelques dispositions particulières relatives à la collecte d'informations tantôt en fonction de la source particulière de ces informations, tantôt en fonction de la personne concernée par ces informations.

A propos des sources, l' article 14 de la loi organique prévoit que la collecte auprès des autorités judiciaires, des fonctionnaires et des agents des services publics peut avoir lieu sur base des accords éventuellement conclus, ainsi que des modalités déterminées, par leurs autorités compétentes respectives' (ainsi, p. ex. le collège des procureurs généraux et les autorités en charge des services de sûreté et de renseignement peuvent prévoir les modalités de transmission de l'information entre le parquet et lesdits services).

On rappellera tout d'abord à ce propos que ce fondement légal de collecte doit satisfaire aux principes de "clarté" et "d'accessibilité" des dispositions prévues par la loi, comme rappelé à des multiples reprises par la jurisprudence y compris belge fondée sur l'article 8 de la CEDH (cf. supra).

On ajoute à la suite du Conseil d'Etat (avis, p. 32) que *"l' usager doit pouvoir en prévoir les conséquences pour lui"*.

Ensuite, la disposition de la loi organique susvisée prévoit que dans ces cas les autorités judiciaires ou les fonctionnaires "peuvent" communiquer.

L'expression est étrange puisque s'il s'agit d'une simple possibilité, la même disposition prévoit in fine qu'en cas de refus, ces autorités ou fonctionnaires doivent "motiver" leur attitude, sans expliquer par ailleurs quels motifs peuvent être relevants et la manière dont la motivation pourrait être formulée vu l'absence de toute obligation pour le destinataire de devoir expliquer les motifs de sa collecte.

Peut-être, saurait-il utile que la transmission d'informations entre les parquets, les administrations, d'une part, et les services de renseignement et de sécurité s'opèrent à travers des "personnes spécialement mandatées", des "officiers de sécurité" qui devraient alors pouvoir connaître les motifs de la demande pour, le cas échéant, pouvoir s'y opposer.

L'article 15 prévoit la nécessité de fixer par un arrêté royal pris en Conseil des Ministres, les modalités de collecte auprès du Registre national. L'article 18 évoque la collecte auprès de "sources humaines", sans préciser de quelles personnes il peut s'agir (indicateurs, personnes au sein d'entreprises) pour ajouter que dans ce cas, les services de renseignements et de sécurité veilleront à la sécurité des "informateurs".

Enfin, l'article 17 précise que les services susnommés "peuvent" se faire présenter les documents d'inscription de voyageurs, sans préciser s'il y a obligation de tenir de tels documents et le droit des hôteliers de refuser la transmission de tels documents.

28. En fonction des personnes sur qui porte la collecte des données, on note en particulier les dispositions contenues aux articles 16 et suivants de la loi sur la classification et les habilitations de sécurité.

Ces articles prévoient un droit général de toute personne qui doit faire l'objet d'une habilitation de sécurité, à être informé sur le niveau et l'objet de l'habilitation, sur les types de données à collecter et sur les procédures possibles de collecte.

Ce droit à l'information se double d'un droit de la personne à consentir à la collecte. Ce droit est exprimé du moins au départ c'est-à-dire seulement lors de sa demande d'habilitation. Il ne peut être retiré tant que la personne exerce les fonctions correspondantes à cette habilitation.

Sans doute, faut-il remarquer que ce "consentement" (dans le même sens, avis de la Commission n° 22/96 en date du 4 septembre 1996) ne constitue pas un consentement au sens de la directive dans la mesure où la liberté de le donner n'existe guère là où les conséquences seront souvent la perte d'un emploi ou de la chance d'un emploi.

Sur ce point, on citera deux arrêts de la Cour de Strasbourg, le premier affirme

" *The fact that the information released to the military authorities was not communicated to Mr. Leander can not by itself the conclusion that the interference was not "necessary in a democratic society (...)", as it the very absence of such communication which at least, ensures the efficacy of the personnel procedure (...)"* (cf. arrêt Leander, déjà cité, § 56 à propos de l'enquête opérée à propos d'un charpentier désirant travailler dans un musée de la Force Navale).

Cette position de principe n'interdit pas que l'enquête ne puisse déborder ce qui peut être considéré comme "raisonnable", c'est-à-dire correspondant à la "reasonable expectation" de la personne concernée (à ce propos, le remarquable raisonnement de L. Bygraeve, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, 6 I.J.L.I.T., 1998, p. 261 et s. à propos des arrêts Malone v. U.K. (1984) et Halford v. U.K. (1997).

2.2.2. La deuxième étape : l'utilisation interne des données (ou le 'traitement' selon la qualification de la loi organique)

29. La loi organique ne prévoit pas de dispositions particulières à cet égard. Comme le note l'avis de la Commission (avis, p. 7), *"le projet ne spécifie pas quelles mesures au sein des services concernés peuvent accéder aux données à caractère personnel".*

Rappelons à ce propos que les services de renseignements et de sécurité sont soumis à de nombreuses obligations par la loi vie privée, ainsi l'obligation de prévoir des mesures de sécurité, celle de veiller à l'exactitude et à la mise à jour des données, celle de ne pas prendre de décisions sur le seul fait d'un traitement automatisé, celle enfin de ne pas utiliser des données non pertinentes ou excessives au regard des finalités de leur traitement.

30. La loi relative à la classification et aux habilitations de sécurité contient cependant par rapport à ces prescrits une réponse très partielle et peu spécifique aux données personnelles.

Cette loi prévoit en effet la classification (article 4) de tout document détenu par les services en documents "très secrets", "secrets" et "confidentiels". Le critère de classement est l'importance du dommage causé à la sécurité publique par suite d'une divulgation non autorisée.

Sans doute, regrettera-t-on que parmi les critères énoncés pour procéder à la classification la vie privée des personnes concernées n'aie pas été prise en considération (cf. en ce sens, les critiques du comité R dans son rapport publié aux documents parlementaires).

A cette classification, sont attachées deux conséquences importantes pour assurer la sécurité et la confidentialité des documents et de leur contenu, le cas échéant, à caractère personnel : premièrement, l'accès aux documents classés est réservé aux "officiers de sécurité" disposant de l'habilitation correspondante à leur classement (article 8) et la transmission des documents internes ou externes nécessite l'autorisation de l'auteur de la classification ou de son superviseur hiérarchique (article 10).

2.2.3. La troisième étape : la communication externe des données

31 L'article 19 de la loi organique est particulièrement vague à ce propos puisque la communication a lieu par les services à des tiers "conformément à leurs missions".

On note qu'il n'est pas précisé si le mot "leurs" se réfère aux missions des émetteurs ou des destinataires de la communication ou aux deux. Dans ce dernier cas, il sera nécessaire de vérifier l'habilitation du destinataire à recevoir les données qu'il reçoit.

Une telle formulation vague reçoit la critique virulente de la Commission

" *Le projet sous un libellé apparemment restrictif tend au contraire à permettre une communication tous azimuts faisant fi de la plus élémentaire protection de la vie privée des citoyens".*

A nouveau, la loi aurait pu prévoir l'existence de garanties procédurales, ainsi l'obligation de motiver par écrit la transmission, la nécessité de préciser l'étendue de la transmission et l'obligation d'identifier le destinataire et de s'assurer de son respect des prescrits de confidentialité, propres aux données transmises.

2.2.4. La quatrième étape: la conservation des données

32. L'article 27 prend soin de régler cette dernière étape:

" *les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. ..*", le dernier alinéa ajoute:

" *Le Roi fixe après avis de la Commission de Protection de la Vie Privée les délais pendant lesquels les données sont conservées".*

Dans son avis, la Commission reproche au projet d'avoir ainsi confié au Roi et non à la loi le soin de fixer le délai mais là n'est sans doute pas le noeud du problème tant il apparaît que les deux alinéas dans leur application concrète peuvent se révéler contradictoires.

Que se passera-t-il si la donnée est toujours nécessaire aux finalités mais qu'est dépassé le délai de conservation fixé par le Roi. Pour échapper à la contradiction, il est possible certes de prévoir un délai maximal tellement long que la question ne se pose pas.

Sans doute, au-delà de la fixation de ce délai maximal de conservation, à partir de la dernière utilisation 'significative' de la donnée (c'est-à-dire lors de l'ajout d'un renseignement précis sur la personne 'fichée'), il serait préférable de prévoir qu'à chaque donnée soit attachée la date normalement envisagée de péremption de l'information y contenue et ce en fonction du contexte et de la nécessité de la mission spécifique assignée à ce dossier.

A l'expiration de cette date, la destruction ou l'anonymisation doit être adonnée sauf à prévoir le droit des services en cause de demander la prolongation de la conservation des données auprès d'un organe créé au sein de ces services (le détaché ?) qui veillera à la conciliation des intérêts contradictoires du service et de la personne concernée.

Ce système est semblable à celui existant au sein d'Europol pour les *"analysis files contenant des données à caractère personnel"*.

CHAPITRE III: UNE BALANCE DES INTÉRÊTS PROBLÉMATIQUES: L'ACCÈS "INDIRECT" AUX FICHIERS DES SERVICES DE RENSEIGNEMENT

33. Si secret et protection de la vie privée peuvent faire bon ménage, ils se retrouvent en conflit lorsque c'est la personne fichée elle-même qui souhaite exercer les droits qui lui sont reconnus en cette qualité.

Ainsi, la protection de la vie privée peut se trouver dans de nombreuses hypothèses, confrontée à l'obligation de secret qui s'impose à certains services.

La personne fichée s'est vue reconnaître un droit de contrôle de plus en plus important sur son 'double informationnel', à mesure que celui-ci prenait de l'importance.

Les services de renseignements ont besoin, c'est l'évidence, de traiter de plus en plus d'informations sur les citoyens.

Comment trouver un équilibre entre le droit au respect de la vie privée des citoyens -droit fondamental, rappelons-le- et la nécessité légitime d'assurer la sûreté de l'état dans lequel ils vivent?

De nombreux points de friction existent, qui sont développés ci-dessus

Il faut faire un choix parmi toutes ces questions: nous avons donc opté pour la problématique de l'accès des personnes fichées aux données personnelles traitées à leur sujet par les services de renseignement.

Il nous paraît en effet qu'en cette matière, la procédure existante n'assure pas de manière suffisante l'équilibre des intérêts en présence.

1. LE MÉCANISME DE L'ACCÈS INDIRECT

34. L'article 13 de la loi du 8 décembre 1992 prévoit que l'exercice des droits d'accès et de rectification (dans la nouvelle loi, on y ajoute de manière explicite les droits de suppression ou interdiction d'utilisation de données non pertinentes, incomplètes, conservées trop longtemps) se fait de manière indirecte, c'est-à-dire, via la Commission de la protection de la vie privée, auprès de certains services, cités ci-dessous:

Cela concerne les traitements de données à caractère personnel:

gérés par les autorités publiques en vue de leurs missions de police judiciaire;

gérés par les services de police visés à l'article 3 de la loi organique du 11 juillet 1991 du contrôle des services de police et de renseignements, en vue de l'exercice de leurs missions de police administrative;

gérés en vue de leurs missions de police administrative par d'autres autorités publiques qui ont été désignées par arrêté royal délibéré en conseil des ministres après avis de la Commission de la protection de la vie privée;

rendus nécessaires en raison de l'application de la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux;

gérés par l'administration de la Sûreté de l'Etat du Ministère de la Justice;

gérés par le Service général du Renseignement et de la Sécurité du Ministère de la Défense nationale.

La nouvelle loi modifie quelque peu cette liste: en ce qui concerne plus spécifiquement les services de renseignement, elle mentionne *"la Sûreté de l'Etat, le Service général du renseignement et de la sécurité des forces armées, l'Autorité de sécurité, par les officiers de sécurité et*

par le Comité permanent de contrôle des services de renseignement et son Service d'enquêtes, lorsque ces traitements sont nécessaires à l'exercice de leurs missions" (voir supra).

Les traitements de données gérés par les services de renseignements se voient donc exemptés du respect de dispositions importantes de la loi de 1992.

Ce système est inspiré de la loi française "Informatique et Libertés"[4], qui a mis sur pied le système d'accès indirect pour les traitements *"intéressant la Sûreté de l'Etat, la défense et la sécurité publique"*.

2. LA PROCÉDURE SUIVIE

35. En droit belge, la personne souhaitant exercer le droit d'accès indirect et s'adressant à cet effet à la Commission doit communiquer son identité: c'est la seule condition particulière posée.

La Commission lui demande de fournir également un maximum d'éléments utiles autorisant une recherche motivée: pourquoi pense-t-elle qu'elle est fichée, par quel service, ? ...

La Commission, sur base de ces renseignements, exerce alors le droit d'accès au nom du requérant et demande, le cas échéant, la rectification des données concernées. Lorsque la Commission a effectué l'accès, le requérant est averti de ce qu'*"il a été procédé aux vérifications nécessaires"*, selon la formule de l'article 13 de la loi de 1992.

Cela signifie que, quel que soit le résultat de l'accès effectué par la Commission, même si par exemple, on ne trouve dans le traitement visé aucune donnée concernant le requérant, ce dernier n'est jamais mis au courant de ce que la Commission a pu constater et modifier.

Une chose paraît remarquable dans ce système: c'est le primat de principe accordé à la protection du secret par rapport au droit d'accès de la personne concernée. Dès lors qu'un traitement est géré par un service de renseignements dans l'exercice de ses missions, on considère que l'accès aux données représente un danger pour la sûreté de l'Etat.

Les motifs qui ont poussé le législateur à organiser cette forme d'accès sont l'établissement d'un juste équilibre entre, d'une part, les droits légitimes de chaque personne et, d'autre part, la nécessité de déceler et de poursuivre les infractions, ainsi que la prévention des atteintes à la sûreté de l'Etat[5].

Cet objectif ne nous paraît pas atteint: la loi, même si sa rédaction actuelle est critiquable, pourrait être exploitée mieux pour réaliser cet équilibre.

---

(4) Loi n° 78 - 17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 39. Un autre système existe pour les "Renseignements généraux" : suivant cette procédure, si les informations concernant le requérant ne mettent pas en cause la sûreté de l' Etat, la défense ou la sécurité et moyennant accord du Ministère de l'Intérieur, les données elles-mêmes peuvent être communiquées à l'intéressé. (Décret 91-1051 du 14 octobre 1991 portant application de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (?) aux fichiers informatisés, manuels ou mécanographiques).

(5) Exposé des Motifs, Doc. Parl., Chambre des Représentants, n° 1610/1 - p. 18-19

36. Dans la pratique, l'accès indirect est malaisé à organiser de façon efficace, car le requérant ne sait pas nécessairement lui-même si des données sont traitées à son sujet, ni pour quelles raisons précises.

Le requérant apprend qu'il est fiché par un service de renseignements par exemple lorsqu'on lui refuse la naturalisation, ou l'octroi d'un certificat de sécurité; dans d'autres cas, il peut se douter qu'il est fiché en raison de sa participation à certains groupements ou activités.

Dans toutes les hypothèses, il peut parfaitement se tromper et se croire fiché pour une raison alors qu'il l'est pour une autre, ou pas du tout. Cela rend dès lors la tâche de la Commission difficile, puisqu'elle se base sur des éléments incertains.

Une fois que la Commission réalise l'accès, si elle ne trouve pas les éléments attendus mais d'autres, pouvant justifier le fichage, comment peut-elle en vérifier la pertinence, l'exactitude? Elle n'a aucun moyen de s'informer auprès du requérant, puisque, par définition, ce dernier ne sera informé que de l' accomplissement des 'vérifications nécessaires'.

La Commission ne peut l'interpeller en cours de procédure d'accès pour lui demander des explications sur telle ou telle information : il s'agit en quelque sorte d'une procédure "en double aveugle" ...

Il en va ainsi quel que soit le degré de confidentialité ou de réel danger pour la nation de la divulgation au requérant des éléments en question: la loi de 1992 ne prévoit pas d'appréciation au cas par cas (alors que même la France le prévoit pour les "Renseignements généraux").

L'absence d'une balance des intérêts effectuée au cas par cas ne nous paraît pas constituer une nécessité pour la protection du secret -à la nuance près qu'un système général au lieu du cas par cas simplifie la vie des services concernés. Mais ce système paraît difficilement conciliable avec l'esprit, voire la lettre dans certains cas, des textes fondamentaux en matière de protection de la vie privée (voir ci-dessous).

L' accès indirect tel qu'il est organisé ne permet pas à la Commission d'exercer un réel contrôle, nécessaire dans une société démocratique, sur les pratiques de fichage des services de renseignement.

Enfin, et c'est peut-être plus grave, il crée chez les personnes concernées un sentiment d' injustice et de frustration compréhensible, et ébranle leur confiance dans les institutions (particulièrement la Commission ...).

3. TEXTES APPLICABLES

37. Un tour d'horizon des textes et principes applicables révèle que les impératifs de sûreté de l'Etat et de défense nationale doivent bien sûr être pris en compte et donner lieu à des dérogations; mais il apparaît que, justement, c'est de dérogations qu'il s'agit, à apprécier de manière la plus individualisée possible.

Cela est plus compatible avec le principe de base: la protection de la vie privée est un droit fondamental, et les exceptions qui y sont apportées doivent être justifiées de manière stricte. Une dérogation ne peut devenir un système.

Nous citerons ici brièvement quelques-uns de ces textes[6].

Le principe de la "participation individuelle" est reconnu dans les Lignes Directrices de l' OCDE (1980) régissant la Protection de la Vie Privée et les Flux Transfrontières de Données à Caractère Personnel, ainsi que dans la Convention Européenne pour la Protection des personnes à l'égard des traitements automatisés de données à caractère personnel (1981).

L'article 9 de cette Convention permet de déroger de manière exceptionnelle au principe de participation individuelle *"lorsqu'une telle dérogation, prévue par la Loi de la Partie, constitue une mesure nécessaire dans une société démocratique:*

-a) à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales;

- b) à la protection de la personne concernée et des droits et libertés d'autrui."

La recommandation R(87)15 du Comité des Ministres du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police[7] stipule sous le principe 6 (Publicité, droit d'accès, droit de rectification et droit de recours), entre autres que:

" *L'exercice des droits d'accès, de rectification ou d'effacement ne saurait faire l'objet d'une restriction que dans la mesure où une telle restriction serait indispensable pour l'accomplissement d'une tâche légale de la police ou nécessaire pour la protection de la personne concernée ou des droits et libertés d'autrui. (...)*
Un refus ou une restriction de ces droits devraient être motivés par écrit. (...)"

Il ressort donc, en particulier du dernier paragraphe cité, que les dérogations doivent être indispensables.

Si ces dérogations doivent être motivées par écrit, cela sous-entend en outre une motivation au cas par cas. L'accès indirect devrait dès lors rester un régime d'exception, lié à de strictes conditions limitatives.

38. La jurisprudence de la Cour européenne des droits de l'Homme paraît appuyer cette thèse, quoique de manière plus indirecte.

Ainsi, dans l'arrêt McMichael c. Royaume-Uni, la Cour décida que les ingérences d'une autorité publique dans l'exercice du droit au respect de la vie privée et familiale, ingérences autorisées à certaines conditions par l'article 8 de la CEDH doivent répondre à des exigences procédurales supplémentaires assurant le droit de la défense des personnes concernées.

---

(6) Notons que la directive européenne 95/46 ne s'applique pas au traitement de données à caractère personnel mis en oeuvre pour l'exercise d'activités qui ne relèvent pas du champ d'application du droit communautaire (...) et en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat (...) et les activités de l'Etat relatives à des domaines du droit pénal (article 3). Cela étant, les état peuvent décider d'incorporer certains principes de la directive même dans les domaines de leurs activités qui sont exclues normalement de son champ d'application.

(7) Mais dont l'application peut être étendue aux services de renseignement.

Le paragraphe 87 est formulé comme suit:

Sans doute l'article 8 ne renferme-t-il aucune exigence de procédure, mais il faut que le processus décisionnel débouchant sur des mesures d'ingérence soit équitable et respecte comme il se doit les intérêts protégés par l'article 8".

Dans ce sens, l' arrêt W. c. Royaume-Uni:

" *Il échet (...) de déterminer, en fonction des circonstances de chaque espèce, (...) si les parents*[8] *ont pu jouer dans le processus décisionnel, considéré comme un tout, un rôle assez grand pour leur accorder la protection requise de leurs intérêts."*

Dès lors, si des personnes subissent une ingérence dans leur vie privée ou familiale, elles doivent pouvoir disposer de tous les éléments nécessaires pour se défendre de manière équitable. Cette exigence accorde une garantie procédurale, comme l'article 6 CEDH, mais *"va de pair avec l'objectif plus large consistant à assurer le juste respect, entre autres, de la vie familiale"*[9].

Le droit de se défendre est incorporé dans le droit au respect de la vie privée et familiale[10].

4. DES PROPOSITIONS

38. Si le système belge d'accès indirect paraît peu satisfaisant au regard des arguments cités ci-dessus, faut-il pour autant modifier entièrement les textes qui l'organisent?

Il nous paraît que l'on peut faire l'économie d'une modification globale -qui, au reste, paraît peu imaginable dans le contexte actuel, puisque la nouvelle loi est votée.

Par contre, on peut proposer une relecture des textes existants, et en particulier, de la loi du 11 avril 1994 relative à la publicité de l'administration.

---

(8) Dans le cas d'espèce, il s'agissait d'un problème lié à la vie familiale (garde d'enfants).

(9) Arrêt Mc. Michael c. Royaume-Uni, para. 91

10) Un arrêt plus récent (Mc. Ginley c. Royaume-Uni) énonce aussi, en rapport avec l'accès aux documents (para. 101): *"Dans ces conditions, eu égard à l'intérêt des requêrants à obtenir l'accès aux documents en question et à l'absence apparante d'un quelconque intérêt public à ne pas les communiquer, la Cour considère que l'article 8 faisait peser sur l'Etat une obligation positive à cet égard. Dès lors qu'un gouvernement s'engage dans des activités dangereuses (...), le respect de la vie privée et familiale garanti par l'article 8 exige la mise en place d'une procédure effective et accessible permettant à de semblables personnes de demander la communication de l'ensemble des informations pertinentes et appropriées."*
Quoique dans un contexte différent, on retrouve ici la trace du même souci de la Cour européenne des droits de l'homme. S'il y a ingérence ou atteinte à la vie privée ou familiale, les personnes concernées doivent, sauf exception, être mises en possession de tous les éléments utiles à ce sujet. il est significatif également de voir que la Cour fait, dans ce paragraphe, une balance des intérêts individuels: si l'Etat n'a pas de raison particulière de refuser la communication des documents, il doit en donner connaissance aux intéressés. On ne reconnait pas un droit de l'Etat à les garder secrets pour la simple raison qu'il s' agit de documents concernant des activités menées par l'armée.

L'article 4 de cette loi prévoit que:

" *Le droit de consulter un document administratif d'une autorité administrative fédérale et de recevoir une copie du document consiste en ce que chacun, selon les conditions prévues par la présente loi, peut prendre connaissance sur place, de tout document administratif, obtenir des explications à son sujet et en recevoir communication sous forme de copie. Pour les documents à caractère personnel, le demandeur doit justifier d'un intérêt."*

L'article 6 précise qu'une administration peut opposer un refus à la demande de consultation d'un particulier, pour différentes raisons. Certains motifs de refus sont absolus, d'autres sont relatifs et donnent lieu à une appréciation au cas par cas. S'il s'agit d'un motif relatif, la décision de refus doit être motivée.

Parmi ce type de motifs, on trouve l'ordre public, la sûreté ou la défense nationale, la recherche ou la poursuite de faits punissables, ... Ce sont en principe des motifs qui pourraient être opposés à un requérant par un service de renseignement.

L' exposé des motifs impose une lecture stricte des motifs de refus:

La demande ne peut être rejetée que dans la mesure où l'importance de la publicité n'équivaut pas, dans le cas concret, aux intérêts énumérés à l'article 6. (...) Le fait qu'un des intérêts, prévus dans cet article, est en jeu ne suffit pas pour que l'autorité soit automatiquement relevée de l'obligation de donner des renseignements ou de rendre publics des documents administratifs (...).
Concrètement, le seul fait qu'un document ait trait à la sécurité de l'Etat par exemple, ne suffit pas pour le soustraire à la publicité. Il faut encore que la consultation ou la communication constitue, à ce moment même, un risque essentiel pour la sécurité de l'Etat"[11].

39. Il apparaît donc qu'en invoquant la publicité de l'administration plutôt que la loi de 1992, une personne concernée aurait un accès éventuellement beaucoup plus étendu.

Or, lorsque des demandes concernant cette problématique sont adressées à la Commission d'accès aux documents administratifs, celle-ci les renvoie, selon une jurisprudence constante, à la Commission de la protection de la vie privée. Le raisonnement suivi par la CADA est le suivant:

Les dispositions de cette législation [la loi de 1992] sont plus strictes en matière de publicité des données. Il s'agit d'une législation spécifique qui déroge au principe général de la publicité instaurée par la loi du 11 avril 1994 et qui prévaut sur celui-ci. (...)
En effet, l'article 6, §2, 2° de la loi du 11 avril 1994 relative à la publicité de l'administration stipule que l'autorité administrative fédérale ou non fédérale rejette la demande de consultation, d'explication ou de communication sous forme de copie d'un document qui lui est adressée en application de la présente loi si la publication du document administratif porte atteinte à une obligation de secret instaurée par la loi."[12]

---

(11) Exposé des Motifs -Projet de loi relatif à la publicité de l'administration, Doc. Parl., Chambre des Représentants, n° 1112/1, 92/93

(12) Affaire X/sûreté de l'Etat, S.21.11.1994, 1/CAD/94/12 - Jurisprudence constante.

Nous ne pouvons absolument pas approuver cette jurisprudence: elle fait de la loi de 1992 la cause d'une restriction de la publicité des documents administratifs. Or, ce n'est pas la loi de 1992 qui *"impose une obligation de secret"*!

Elle prend en compte cette obligation et les caractéristiques de certains traitements pour instituer un régime particulier, mais elle ne dispose pas elle-même qu'une obligation de secret pèse sur les services concernés. Raisonner de la sorte revient à faire d'une loi protectrice des libertés une cause de restriction à ces mêmes libertés, ce qui est inconcevable.

40. Notons toutefois que l'accès pourrait désormais être refusé sur base de l'article 26§1 du projet de loi relatif à la classification et aux habilitations de sécurité.

Selon cet article, en effet, *"la loi du 11 avril 1994 relative à la publicité de l'administration ne s'applique pas aux informations, documents ou données, au matériel, aux matériaux ou matières, sous quelque forme que ce soit, qui sont classifiés en application des dispositions de la présente loi."*

Il nous semble que cet article doit également être lu à la lumière des textes cités ci-dessus : il faudrait que l'octroi de l'accès auxdites informations crée un réel danger important pour la sécurité de l'Etat.

La loi de 1994 tend à appliquer un principe constitutionnel ; dans la hiérarchie des normes, elle a donc 'préséance' sur la loi organisant la classification. Dès lors, on pourrait interpréter cet article en ne refusant l'accès qu'aux documents classifiés "secret" ou "très secret", dont la divulgation indue crée un préjudice grave pour la nation.

Une autre possibilité serait que toutes les informations ne soient pas classifiées. Il nous semble que, si la classification doit amener une diminution de la possibilité de contrôle par les personnes concernées, il ne faudrait utiliser qu'avec parcimonie ce mécanisme.

Une classification généralisée renverrait en effet les personnes concernées à la procédure d'accès indirect, avec toutes ses lacunes.

41 En conséquence, nous proposons une position de compromis entre ces différents points de vue; cette position tente de tirer profit au maximum des législations existantes.

Lorsqu'une personne souhaite avoir accès aux données qui la concernent et sont traitées par un service de renseignement, elle devrait en premier lieu s'adresser directement à ce service, en vertu de la loi de 1994. Il s'agirait au départ d'une demande d'accès classique.

Tout problème à ce niveau (absence de réponse d'une administration,...) serait du ressort de la Commission d'accès aux documents administratifs, selon les règles de la loi de 1994 et la jurisprudence en la matière.

Si le service de renseignement saisi de la demande estime qu'il se trouve confronté à un motif d'exception (danger pour la sécurité de l'Etat, ...), il communiquerait au requérant un refus de réponse, et le renverrait alors auprès de la Commission de la protection de la vie privée, qui exercerait dans ce cas la procédure d'accès indirect.

Il en irait de même si un problème se posait lors de l'accès exercé par le requérant lui-même (refus de rectification,...): la Commission jouerait dans cette hypothèse le rôle de médiation qui lui est attribué par la loi [13].

Cette solution nous paraît infiniment plus respectueuse des droits des personnes concernées, sans pour autant exiger un changement législatif. Nous allons jusqu'à penser que cette procédure représente, pour un service de renseignement, l'occasion de remettre en cause ses propres pratiques de traitement de données, ce qui peut être fécond.

La possibilité de voir exercer un contrôle direct par les personnes concernées, et de ne le refuser qu'en cas de danger grave pour la sécurité de l'Etat ou tout autre motif sérieux imposerait aux services de ne garder que des informations réellement pertinentes, à jour, exactes,... ce qui, sauf erreur de notre part, est dans l'intérêt de toutes les parties.

D'autre part, il reste toujours la possibilité de refuser l'accès et de se tourner alors vers la procédure plus discrète d'accès indirect. Les expériences française et néerlandaise vont d'ailleurs dans ce sens, et ne semblent pas montrer que l'on abuse de ces possibilités.

Il est d'ailleurs significatif à cet égard de noter que la Commission Nationale Informatique et Libertés préconise l'abandon total de la procédure de l'accès indirect : il faut donc croire que l'expérience française démontre qu'une procédure d'accès direct n'est pas impraticable (et est même souhaitable).

CONCLUSIONS

42 Individuellement, les exigences de protection des données s'imposent à ceux qui sont en charge de la sûreté de l'Etat et de sa défense.

Ces exigences doivent certes s'accorder aux particularités de la mission impartie à ces personnes et organismes. Ces particularités exigent certes que la transparence de leurs activités, transparence instituée par les législations de la vie privée tant vis-à-vis de personnes concernées que du public en général soient parfois tempérée.

Ces particularités réclament que les multiples limites aux modes de collecte et au traitement des données affirmées par les législations de vie privée soient parfois oubliées au profit de l'efficacité légitime des services en cause.

Mais, à propos des exceptions, il importe précisément pour qu'elles soient et restent légitimes qu'elles soient "prévues par la loi" et soient proportionnées aux nécessités de l'action qui les fondent.

---

(13) Notons d'ailleurs que la loi portugaise transposant la directive 95/46 se tourne vers une procédure d'accès indirect - c'est à notre connaissance, un des rares pays européens à faire le choix de cette procédure - parce que les expériences ont montré que les requérants souhaitaient être appuyés dans leurs démarches auprès des services de police par une instance indépendante.

Ce raisonnement, nous l'avons suivi tout au long de l'exposé, montrant comment la loi vie privée en prévoyant des exceptions globales, automatiques et trop nombreuses ne respectait pas cet équilibre, dénonçant le système actuel de l'accès indirect sans doute légitime dans certains cas mais non dans tous les cas, et finalement réclamant que les étapes du traitement se conforment plus étroitement aux exigences de cet équilibre.

Cet équilibre nous en sommes convaincus ne nuira pas à l'exercice par la Sûreté de l'Etat et les services de renseignements de ces missions mais apportera à ces organismes légitimité et meilleure confiance de la population.

43. Une seconde conclusion nous est également dictée par la jurisprudence de la Cour européenne des droits de l'homme qui voit dans l'intervention possible d'une "autorité indépendante", l'indispensable garantie de la protection de nos libertés.

A nouveau sur ce point, la solution belge est pour le moins défaillante. La loi Vie Privée ne donne pas à la Commission les moyens d'un contrôle effectif sur l'action de la Sûreté de l'Etat et des Services de renseignements.

Sans doute, dira-t-on, le risque est grand d'atteinte à la confidentialité si les pratiques de ces organismes et leurs données faisaient l'objet de délibération dans une Commission qui se doit d'être un 'temple de la transparence' mais bien des solutions pouvaient être trouvées, ainsi, la délégation de cette mission particulière de contrôle à quelques membres et fonctionnaires habilités, leur présence au Comité R dont la mission serait alors élargie à la protection des données enfin leur droit d'intervenir dans la désignation d'un 'préposé ou détaché à la protection des données'.

Nous avons maintes fois insisté sur le rôle que pourrait jouer ce préposé, à la fois dans la conscientisation des fonctionnaires desdits organismes, lors de demandes d'accès et dans toutes les questions posées par certains modes de collecte, les utilisations et la durée de conservation des données personnelles, dans la balance des intérêts à effectuer lors d'une mesure de classification...

L'obligation de sécurité, affirmée par la loi de protection des données, justifie, à suffisance au regard des risques créés par les libertés, la nécessité d'une telle mesure organisationnelle.

Concilier secret d'Etat et vie privée est loin d'être une tâche impossible. Il suffit pour nos autorités de s'en convaincre et de le vouloir.