Secret d'Etat et vie privée

Havelange, Benedicte; Poullet, Yves

Published in:
Droit des technologies de l'information : regards prospectifs

Publication date:
1999

Document Version
le PDF de l'éditeur

SECRET D'ÉTAT ET VIE PRIVÉE : OU COMMENT CONCILIER L'INCONCILIABLE ?°

Bénédicte HAVELANGE* et Yves POULLET**

INTRODUCTION

1. Protection de la vie privée et secret d'État sont-ils inconciliables ? Un examen sommaire de ce que recouvrent ces deux termes semble l'indiquer. Les services de renseignement doivent collecter des informations sur les personnes et groupes dont les activités présentent un danger pour la sécurité de l'État. Qu'ils soient tenus de traiter ces renseignements dans la confidentialité la plus stricte tombe sous le sens. D'autre part, au fur et à mesure que l'exploitation de l'information prenait de l'ampleur — dans tous les secteurs — les citoyens se sont vu reconnaître un pouvoir de contrôle sur l'information traitée à leur sujet, sur leur « double informationnel ». Une personne peut savoir si l'on traite de l'information à son sujet, et si oui, qui, pourquoi et comment. Informée, elle est en mesure de demander une rectification de ces données, voire leur effacement dans certains cas : elle peut faire en sorte que son double informationnel soit aussi ressemblant que possible. Comment ces exigences pourraient-elles être rencontrées auprès de services qui, par définition, ne sont pas tenus à l'ouverture, mais bien au secret ?

Il nous semble qu'en cette matière, tout est question d'équilibre. Les intérêts en jeu doivent être mis en balance, sans que ceux de l'un doivent systématiquement l'emporter sur ceux de l'autre. Notons également que les principes de protection de la vie privée ne sont pas nécessairement un frein pour la gestion de l'information : ces principes imposent en effet que ne soient traitées que des données pertinentes, exactes, à jour. Cela ne rejoint-il pas l'intérêt des services de renseignement ?

° Les auteurs s'expriment à titre personnel et n'entendent en aucune manière engager la Commission de la protection de la vie privée.

La présente contribution a bénéficié du soutien des S.S.T.C. dans le cadre du Programmme d'Action Interuniversitaire (PAI) : « La société de l'information », qui réunit quatre centres de recherche : CITA et CRID (FUNDP), LENTIC (ULG) et SMIT (VUB). Elle a été présentée lors du colloque qui s'est tenu à Bruxelles le 20 janvier 1999, ayant pour thème : « Secret d'État ou transparence ».

* Collaboratrice scientifique au CRID, Conseiller adjoint à la Commission belge de la protection de la vie privée. E-mail : benedicte.havelange@privacy.fgov.be.

** Professeur à la Faculté de Droit et au DES-DGTIC, Directeur du CRID-FUNDP, Membre de la Commission belge de la protection de la vie privée. E-mail : yves.poullet@fundp.ac.be.

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 le devoir de mettre en balance les intérêts respectifs en cause lorsqu'il s'agit de juger de la légitimité de la prise de renseignements ou de conservation de données personnelles. L'arrêt Leander[1], rendu par la Cour européenne des droits de l'homme à propos de la contestation d'un citoyen convaincu d'être fiché par la sûreté de l'État de son pays et voyant opposer à sa demande d'accès le dogme de la sécurité de l'État, proclame la nécessité de mettre en balance, d'une part, la protection du droit à la vie privée[2], et d'autre part, les impératifs de sécurité et d'ordre public qui fondent les services de renseignements et de sûreté. L'arrêt ajoute que pour réaliser cette balance l'intervention d'une autorité indépendante est requise. Cette seconde condition sera étudiée plus loin lorsque, à propos de l'accès indirect, le rôle de la Commission de protection de la vie privée sera envisagé. 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'État tant lorsque cette collecte vise un citoyen quelconque que lorsqu'il s'agit d'agents ou de préposés à la sécurité de l'État. 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 95/46[3] et notre loi fédérale récemment modifiée pour assurer la transposition de cette directive[4], abordent la question des « traitements » en vue d'assurer la sûreté de l'État. Le deuxième chapitre inverse les termes du débat. La loi organique des services de renseignements et de sécurité adoptée récemment[5], de même que la loi relative à la classification et aux

---

1 Arrêt Leander du 26 mars 1987.

2 Droit consacré chez nous par l'article 22 de la Constitution.

3 Directive 95/46 CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.,* n° L. 281/31 du 23 novembre 1995.

4 Loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *M.B.*, 3 février 1999. Cette nouvelle loi intervient par voie de modification de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Le lecteur trouvera une analyse des dispositions de cette loi *in* T. LEONARD -Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution : la loi du 11 décembre 1998 transposant la directive 95/46 /CE du 24 octobre 1995 », *J.T.*, 1999, pp. 377-396.

5 Loi organique du 30 novembre 1998 des services de renseignement et de sécurité, *M.B.*, 18 décembre 1998.

habilitations de sécurité[6] 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 I. LA RÉGLEMENTATION « VIE PRIVÉE » ET LA « SÛRETÉ DE L'ÉTAT »

4. Le chapitre analyse successivement la manière dont la directive européenne 95/46 dite directive générale de protection des données (ci-après, « la directive ») aborde les traitements de la défense ou de la sûreté de l'État ; ensuite, il opère un rapide tour d'horizon de droit comparé, se concentrant en particulier sur les textes nouveaux adoptés depuis la directive ou fondés sur elle. Enfin, il détaille la solution originale du droit belge sur base de la loi du 11 décembre 1998 transposant la directive 95/46/CE (ci-après, « la nouvelle loi »).

A. Le point de vue européen

5. Deux dispositions de la directive mentionnent la question particulière des traitements de données à caractère personnel opérés pour des finalités de défense ou de sûreté de l'État. À 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 œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du 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'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal »[7].

---

6 Loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité, *M.B.*, 7 mai 1999.

7 Le considérant n°13 rappelle les limites de la compétence européenne en la matière.

— Par ailleurs, l'article 13 dispose que : « Les États 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'État ;

b) la défense ;

c) la sécurité publique ;

d) …;

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

f) … » [8].

6. Comment expliquer cette apparente contradiction ? La directive est-elle applicable ou non aux traitements opérés par la sûreté de l'État ou par les services de renseignements. La lecture attentive de la directive conduit à résoudre cette apparente contradiction en distinguant, parmi les fichiers qui ont pour finalité d'assurer la défense ou la sûreté de l'État, deux types de fichiers ou de traitements : les premiers concernent 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'État. Par contre, certains traitements sont opérés par des organes privés et publics dont les activités sont indiscutablement régies 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'État ; 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'État. Cette nécessité est reconnue par l'article 13 précisément.

7. Cette précision apportée, qu'il soit clair que les traitements exemptés de l'application de la directive comme d'ailleurs les autres sont bien évidemment soumis au respect de l'article 8 de la Convention européenne des droits de l'homme, dont la portée a été rappelée à propos de l'arrêt Leander[9]. L'article 13 de la directive qui est applicable selon notre raisonnement à certains traitements contribuant à la sûreté de l'État ou à sa défense apparaît d'ailleurs comme une application des principes déduits de

8 Le considérant n°43 paraphrase sans expliquer outre mesure de telles dérogations.

9 *Cf. supra* n° 2.

l'article 8 de la Convention européenne et s'impose dès lors à notre législateur comme son analyse le démontre.

Premièrement, l'article 13 crée la faculté pour les États de prévoir des exceptions, il ne les impose pas. L'emploi du terme « peuvent » est à cet égard significatif. Deuxièmement, 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, oblige 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. Troisièmement, 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.

B. Le droit comparé

8. Notre tour d'horizon se limite à un bref aperçu de quelques réglementations ou projets de réglementation récents ayant pour caractéristique de transposer la directive européenne. Parmi ces divers textes, nous distinguerons les approches suivantes : celle illustrée par le projet de loi néerlandais[10] qui réglemente les traitements de la sûreté de l'État et des services de renseignements par une législation séparée ; celle de la loi grecque[11] qui ne prévoit aucune dérogation à la loi de protection des données ; celle des lois italienne[12], portugaise[13] et britannique[14] qui prévoient des exceptions partielles et ce, 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

---

10 Wet bescherming persoonsgegevens, Wetsontwerp 25892, Tweede Kamer, nr 7, 2 dec. 1998 disponible à http://www.unimaas.nl/~privacy/wbp.htm.

11 Loi n° 2472-1997 sur la protection de la personne à l'égard du traitement des données à caractère personnel.

12 Loi n° 675 du 31 décembre 1996 portant protection des données à caractère personnel.

13 Lei da proteccao de dados pessoais, Lei n° 67/98 du 26 octobre 1998 disponible à http://www.cnpd.pt/lei_6798.htm.

14 Data Protection Act 1998 (1998 c 29).

veiligheidsdiensten de 1951 mais depuis remaniée à plusieurs reprises. Quelques principes caractérisent cette loi : celui de la proportionnalité et du minimum de mesures d'investigation ; la distinction de trois degrés de classification des documents détenus par les services de sécurité et cela selon le degré de confidentialité du contenu des documents[15]; enfin la responsabilisation des fonctionnaires habilités.

10. La loi italienne part du principe de la non-application de la loi de protection des données[16]. Selon l'article 4, alinéa1, 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'État ;

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

À ce principe de non-application, l'alinéa 2 du même article introduit d'importantes nuances : « 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, alinéa1 b).

11. La législation portugaise part du principe inverse de la loi italienne. L'article 7 prévoit l'application de la loi mais, dans le cadre de l'application de certains articles, certaines dérogations sont prévues. On cite :

— art. 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'État ou le service de renseignement 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 publique et pour autant que ne prévalent pas les libertés et garanties du titulaire des données ;

— art. 10 : Possibilité de dispense de l'obligation d'information de la personne concernée, si justification ;

— art. 11: Possibilité de dispense du droit d'accès de la personne concernée mais alors droit d'accès indirect.

---

15 La loi belge relative à la classification et aux habilitations de sécurité sur laquelle nous reviendrons (*infra*, n°17) reprend cette même classification.

16 La loi belge, au contraire, part du principe de l'application de la loi « vie privée » aux traitements en question.

12. Le Data Protection Act britannique est original à plus d'un titre. La section 29 relative aux traitements de la sûreté de l'État dispose : « Personal Data are exempt » de tout ou partie des prescrits de protection des données à l'exception, ajoute la section, 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'État 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*.

C. La loi belge du 11 décembre 1998 transposant la directive et modifiant la loi du 8 décembre 1992

13. Sous l'empire de la loi de 1992, l'article 3 excluait du champ d'application de la loi les traitements effectués en vue de la sécurité de l'État. L'article 4 de la nouvelle loi modifie fondamentalement l'article 3 ancien en disposant au § 4 : « Les articles 6 à 10, 12, 14, 15, 17, 17*bis*, alinéa 1, 18, 20 et 31 §§1 à 3, ne s'appliquent pas aux traitements de données gérées par la sûreté de l'État, par le Service général du Renseignement et de la Sécurité des Forces Armées, par l'Autorité de sécurité, par les officiers 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 déjà commentée. Nous avons déjà souligné que la disposition visée de la directive a un champ d'application limité et ne s'applique pas aux traitements visés par la disposition en question[17] même si elle 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.

---

17 Hormis sans doute, les traitements détenus par les officiers de sécurité nommés dans les divers organismes extérieurs aux services de la sûreté de l'Etat, du renseignement et de la sécurité des Forces Armées et devant faire l'objet d'une habilitation de sécurité aux termes de la loi organique (*cf. infra*, n° 27).

Quelques remarques à propos du libellé de la disposition belge :

— premièrement, la loi de protection de la vie privée, sauf exceptions sur lesquelles nous reviendrons, est désormais d'application pour les traitements de sûreté de l'État et de défense nationale. En d'autres termes, ils ne sont plus exemptés de la loi comme c'était le cas jusqu'alors.

— Deuxièmement, on note que le champ d'application *ratione personae* des exceptions 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'État et le Service général du renseignement et de la Sécurité du Ministère de la Défense nationale. Dorénavant, sont également exemptés les traitements gérés[18] par l'Autorité de sécurité, organe de coordination entre sûreté de l'État et service de renseignement[19] 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[20].

— 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 sont pas d'application pour tous les traitements préalablement décrits :

. 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 instaurant et précisant le droit d'accès de la personne concernée;
. 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 17 bis prescrivant des possibilités de réglementation particulière pour certaines catégories de traitement et mentionnant la

18 La notion de gestion et de gestionnaire des traitements était utilisée par l'ancienne loi de 1992 mais on s'interroge sur l'utilisation de cette notion abandonnée par la nouvelle version de la loi.

19 Cette autorité est créée par l'article 15 de la loi relative à la classification et les habilitations de sécurité.

20 Conformément à l'article 13 de la loi citée en note précédente.

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, l'article 31 § 10.3 qui autorise la plainte de particuliers auprès de la Commission.

14. Cette 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 offrait en tout cas des possibilités de dérogation au principe de collecte loyale.

La loi ne prévoit pas non plus de dérogations à l'article 5 de la loi dans sa nouvelle version. Ainsi, les traitements seront légitimes si et seulement si ils sont soit l'exécution d'une obligation légale, soit opérés en vertu du consentement de la personne concernée [21], soit nécessaires à la protection de l'intérêt vital de la personne concernée[22], 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[23]. 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.

---

21 Le consentement comme base légitime d'un traitement est prévu au point a) de l'article 5 de la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998. Ainsi dans le cadre d'enquêtes de sécurité prévues lors de la nomination d'officiers de sécurité, le consentement de ces derniers est requis avant de procéder à l'enquête *(cf.* loi sur la classification et les habilitations de sécurité, art.16).

22 C'est la base légitime d'un traitement prévue par le point d) de l'article 5 de la loi. Ce fondement est applicable dans le cas de traitements opérés par les services de renseignements dans le cadre de leur mission de protection de certaines personnes menacées.

23 Comme prévu par l'article 5 e) de la loi.

15. D'autres dispositions également importantes restent d'application : l'article 12*bis* 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 pour faciliter la recherche de suspects potentiels ou pour le classement comme « personnes à risque » de certains individus. 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 désormais prescrit par l'article 16 de la loi de 1992 telle que modifiée par la loi de 1998. Son application exige, dans un secteur aussi sensible que celui de la sûreté de l'État ou de sa défense, une attention toute particulière. À 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 l'objectif de cet ensemble de mesures ne soit pas directement la protection des personnes concernées (même si elles peuvent indirectement contribuer à cette protection), et que d'autres mesures comme la nomination d'un détaché à la protection des données n'aient pas été préconisées[24].

Outre l'application intégrale du chapitre sur les dispositions pénales (articles 37 et ss.) de la loi dite « vie privée », 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

24 Sur cette mesure que constitue la nomination d'un préposé ou détaché à la protection des données, voir *infra*.

opérés au sein de ce secteur. Ainsi, la loi relative à la classification et aux habilitations de sécurité prévoit que lors d'enquêtes de sécurité à propos des candidats officiers de sécurité, l'information préalable voire le consentement des personnes candidates sont requis comme l'exige l'application de l'article 9 de la loi « vie privée ». En d'autres termes, la loi spécifique applique un article de la législation « vie privée » dont cette dernière législation exemptait précisément le secteur de la sûreté et de la défense. Le même raisonnement est applicable dans bien d'autres cas comme nous le montrerons plus tard[25]. 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 article ne sont 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 ?

À l'inverse, on s'étonne de ne pas trouver dans la liste des exceptions pourtant admises par la directive, 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, 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[26]. À 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 de la directive autorise des exceptions pour des responsables de traitement en communication avec la sûreté de l'État et les services de renseignements. Ainsi, par exemple, une banque contactée par la sûreté de l'État 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

25 Ainsi l'exemple du droit d'accès, *infra*, Ch. III ou celui de la déclaration préalable des traitements de la sûreté de l'État à la Commission de protection de la vie privée.

26 *Cf.* à cet égard, l'arrêt Lüdi (15 juin 1992) de la Cour européenne des droits de l'homme, abondamment cité par l'exposé des motifs de la loi organique.

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'État au projet de loi de protection de la vie privée. Le Conseil d'État[27] 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, ce que le gouvernement devait finalement accepter en insérant un alinéa à l'article 32 prévoyant un tel rapport spécifique[28]. Notre réflexion élargit ce propos. La loi consacre un dangereux déséquilibre entre les impératifs légitimes de la sécurité de l'État 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* permettant en cas de traitements présentant des risques particuliers des exigences réglementaires supplémentaires n'est pas applicable. Or comme le note le Conseil d'État[29] 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

---

27 Avis, *op.cit.*, p. 193.

28 Suite à cet avis, le gouvernement devait finalement proposer un amendement repris par le Parlement. À noter que cet amendement n'est cependant pas applicable à l'article 3 § 4 qui précisément concerne l'exception pour les services de renseignement et de sûreté de l'État, qui sont l'objet de nos propos mais par contre s'applique au droit d'accès indirect qui vise ces services. Ainsi a été inséré à l'article 32 §2 un alinéa 2 qui dispose :» A côté de l'information générale relative à l'application de la présente loi et aux activités de la Commission, ce rapport (…) contient de l'information spécifique sur l'application des articles 3 §3 et 6, 13, 17 et 18. ».

29 Avis*, op.cit.*, p. 192.

l'expérience allemande[30], 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, allié d'autant plus précieux qu'il se trouvait placé en première ligne. Nous reviendrons sur ce point important dans la suite de nos réflexions et en conclusion.

CHAPITRE II. LES REGLEMENTATIONS RELATIVES A LA SECURITE DE L'ETAT ET AUX SERVICES DE RENSEIGNEMENTS FACE AUX EXIGENCES DE LA LOI « VIE PRIVEE »

A. Présentation des législations récemment adoptées en la matière – Historique de la loi organique

17. Deux lois publiées récemment 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[31] : cette loi fixe, suivant le critère de gravité des informations contenues dans les traitements opérés à des fins de sûreté de l'État, 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 dite organique des services de renseignement et de sécurité[32] 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 utile de les lier et d'essayer d'en opérer une lecture commune. Cette tâche comme il sera démontré ci-après n'est cependant point aisée. Plus difficile encore, s'avère la coordination de ces deux lois avec la loi de

30 Notons qu'une telle initiative a été prise pour les services de police : la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (*M.B.*, 5 janvier 1999) prévoit en son article 44/2 que « des personnes de contact pour la Commission de la Protection de la Vie Privée sont désignées dans les services de police », ce qui peut certainement être salué comme une mesure très positive.

31 *Cf. supra*, note 6.

32 *Cf. supra*, note 5.

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.

La loi organique des services de renseignement et de sécurité a connu une genèse difficile que l'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'État et des Services de renseignements généraux et dès lors leur contestation. Deux arrêts du Conseil d'État, le premier dans l'affaire dite Cudell[33] et le second dans l'affaire dite Wicart[34] 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[35] rappellent avec énergie la jurisprudence constante de la Cour européenne des droits de l'homme pour dénier tout droit 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 »*[36].

— En réponse à cette critique fondamentale qui ruinait toute l'action des organismes de sécurité et de défense de l'État, le gouvernement met sur la table, rédigé à la hâte, un avant-projet de loi organique des services de renseignement et de sécurité qui sera soumis fin 1995 à la lecture critique du Conseil d'État (3ème temps).

---

33 Conseil d'Etat, 30/6/95, arrêt n° 54-138.

34 Conseil d'Etat, 30/6/95, arrêt n° 54-139.

35 Trib. 1ère inst. Bruxelles 24ème chambre (R.G. 95/14503) décision dite Vlaams Block (collecte d'informations prise au sujet des membres d'un parti politique).

36 Cet attendu est repris de l'arrêt Wicart. Une formulation quasi semblable de l'attendu est présente dans les deux autres décisions citées.

L'avis du Conseil d'État en date du 27 mars 1996[37] est lourd de critiques vis-à-vis du texte gouvernemental. Si le Conseil d'État 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 »[38]. Le Conseil d'État 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 ». 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 »[39]. À cet égard, la haute autorité affirme la nécessité de précisions dans la loi quant aux limites de l'action des services : « En outre, lorsque sa mise en œuvre s'opère au moyen de mesures concrètes, échappant 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 ». Ainsi, le Conseil d'État 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 ainsi 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 »[40]. En conclusion, note la haute autorité, la loi en projet est tout à fait dépourvue de

37 Cet avis est publié en annexe de l'Exposé des motifs de la loi organique, *Doc. parl., Chambre*, 638/1-95/96, pp. 29 et s.

38 Avis CE, *op.cit*., p. 29.

39 L'avis se réfère sur ces points à l'arrêt Léander de la Cour européenne des droits de l'homme déjà cité (Avis CE, *op. cit*., p. 31)

40 Avis CE, *op.cit*., p. 35.

règles « claires et détaillées » ayant trait à la collecte et l'usage des informations[41]. Le Conseil d'État ajoute par ailleurs l'obligation pour le Gouvernement dans une telle matière 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[42].

— 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 susmentionnés (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 de la Commission[43] 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'État 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 »*[44].

— Le texte sera alors revu légèrement par le Sénat[45]. 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[46].

B. Analyse des dispositions des deux lois au regard des exigences de la loi de protection des données

18. La loi de protection des données établit un principe fondamental, celui suivant lequel les données ne peuvent être traitées que pour des

---

41 Avis CE*, op.cit*., p. 35, citant l'arrêt Kruslin de la Cour européenne des droits de l'homme du 24 avril 1990.

42 *Doc. parl., Chambre*, Session 1997-1998, 638/ 17 - 95/96.

43 Avis n° 12/98 du 23 mars 1998.

44 *Ibidem*, p. 5.

45 On note également une décision de la Commission parlementaire de concertation entre Chambre et Sénat (*Doc. parl., Sénat* I. 82-1995 (S.E.) n° 23, 26, 29 et 32).

46 *Doc. parl., Chambre*, Séance du 19 nov. 1998, 638/21-95/96.

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 a). 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.

a. La finalité des traitements et leur proportionnalité

19. « 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'État 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, description obtenue finalement malgré les réticences du Gouvernement, prend en compte les exigences de clarté et de précision réclamées par les jurisprudences Wicart et Cudell, Vlaams Blok, et par l'avis du Conseil d'État. Sans doute, peut-on encore déplorer avec le Conseil d'État la persistance de certaines délégations du législatif à des pouvoirs subordonnés : *« 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 »*[47].

20. 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.».

47 Avis CE, *op.cit*., p. 34.

21. 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 aux services susmentionnés pour l'accomplissement de leurs missions. Or, les exigences de la loi « vie privée » sont plus sévères puisque l'article 5 de cette loi, par ailleurs applicable aux traitements de la sûreté de l'État et des services de renseignements[48], 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 ? De telles interprétations ne peuvent convaincre : la dérogation aurait dû être explicite et quant à une restriction implicite aux seuls dossiers à l'exclusion des traitements, elle contredirait la mission même de la sûreté de l'État qui est de traiter des données de manière efficace et structurée et non simplement d'entasser des informations.

La même apparente contradiction entre la loi organique et celle sur la « vie privée » se retrouve également à la lecture du second alinéa du même article 13 de la loi organique, qui à propos des dossiers[49] 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'État 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'État et sans doute doit être motivée de manière interne en tout cas afin que les contrôleurs internes et externes[50] puissent évaluer la proportionnalité entre les données collectées et traitées et les risques réels

---

48 Sur le contenu de cet article 5 et son applicabilité aux services de renseignements et de sûreté, *supra*.

49 La notion de dossier est ici utilisée de manière plus large qu'en matière de protection de la vie privée où la notion s'oppose à celle de traitement, dans le sens où le dossier regroupe un certain nombre d'informations non structurées et ne facilitant pas l'accès aux données personnelles y contenues.

50 *Cf. supra*, chapitre I.

ou présumés encourus par l'État ou les citoyens. Ensuite, des garanties procédurales devraient être prises : ainsi la détermination de celui qui décide de la tenue de la documentation, la nécessité d'un réexamen périodique des traitements et de leur contenu, *etc*.[51].

b. Etapes du traitement et règles y applicables

23. Suite aux critiques virulentes du Conseil d'État, à savoir l'absence de règles précises et détaillées quant aux modalités des traitements opérés 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.

- 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 renseignements 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[52]; 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'État 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. »

---

51 À cet égard, un parallèle avec les solutions proposées par la Commission à propos de la recherche proactive dans le secteur policier serait utile.

52 *Cf. supra* n° 13.

25. À l'application de ce double postulat, la Commission et le Conseil d'État 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'État 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 fondé sur le droit de l'État de s'informer librement, il est répondu de manière plus acerbe encore et ce en particulier quant au fondement du raisonnement[53]. « Ce pacte (le Pacte international relatif aux droits civils et politiques des Nations Unies) 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 des services de renseignements 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 une utilisation de techniques de collecte s'écartant de ce principe, à instaurer ces exceptions par des lois particulières qui ne peuvent, en tant qu'exceptions, être interprétées que de manière restrictive et doivent faire l'objet de garanties particulières. C'est sur base de ce raisonnement que le gouvernement avait admis la nécessité d'une intervention législative pour les interceptions de télécommunications ou les écoutes téléphoniques : la loi du 30 avril 1994, modifiée par la loi de 1998, n'autorise ces techniques de collecte déloyale qu'à titre exceptionnel et pour les seuls services de renseignements opérant à l'étranger en temps de guerre. Dès lors, implicitement, le Gouvernement refuse dans les autres

53 Avis 12/98 de la Commission de la protection de la vie privée, point 1.2.4., p. 4 ; *cf.* également l'avis du Conseil d'Etat, p. 31.

cas l'interception téléphonique aux services de renseignements et de sûreté[54]. On s'étonne que par contre pour les autres modes de collecte déloyale des informations (vidéosurveillance, enquêtes auprès de tiers, ...), le Gouvernement estime qu'il ne soit pas nécessaire de procéder à une telle intervention réglementaire 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'État.

Un tel refus est inacceptable. Certaines règles législatives relatives aux modes « déloyaux » de collecte devaient être prises[55], sous peine d'illégalité de ces modes de collecte de renseignements, que ce soit 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, *etc.*

Ainsi, à propos de telles limites à la collecte des renseignements, on citera les controverses suscitées par l'affaire Murray v. U.K. (1994) : la Cour de Justice de Strasbourg avait estimé à propos de la prise par la police de photos d'une militante lors d'une manifestation publique que « the taking of her photographs was solely related to her voluntary public activities » ne constituait pas une « interférence » dans les droits de la personne concernée à la vie privée. Cette décision qui limitait le droit de la police à collecter des renseignements par voie de photos appela cependant les critiques sévères d'une partie de la doctrine[56]. Ainsi cette doctrine cite un autre arrêt, dit Friedl, concernant de même la prise d'informations relatives à l'expression publique volontaire d'activités[57] 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.

À 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

---

54 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 conclu sur le même sujet entre l'Europe et les États-Unis réclament par ailleurs une base réglementaire pour de telles interceptions.

55 Avis du Conseil d'État, p. 31.

56 Voir à ce propos, L. BYGRAEVE, « Data Protection Pursuant to the Right to Privacy in Human Rights Treaties », 6, *I.J.L.I.T.*, 1998, p. 265.

57 Arrêt non publié, 1995, Series A, n° 305 B.

compétentes respectives »[58]. 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 de multiples reprises par la jurisprudence y compris belge fondée sur l'article 8 de la CEDH. On ajoute à la suite du Conseil d'État[59] que « l'usager doit pouvoir en prévoir les conséquences pour lui ».

Ensuite, la disposition de la loi organique susvisée prévoit que dans le cadre de ces accords, les autorités judiciaires ou les fonctionnaires « peuvent » communiquer. L'expression est étrange : s'il s'agit d'une simple possibilité, pourquoi la même disposition prévoit-elle *in fine* qu'en cas de refus, ces autorités ou fonctionnaires doivent « motiver » leur attitude ? On ajoutera que la disposition ne détaille pas les motifs de refus qui peuvent être relevants et la manière dont la motivation pourrait être formulée et n'impose aucune obligation au destinataire de devoir expliquer les motifs de sa collecte. Peut-être, eut-il été utile de prévoir que la transmission d'informations entre les parquets, les administrations, d'une part, et les services de renseignement et de sécurité, d'autre part, s'opère 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 (on songe, par exemple, aux « indicateurs » ou aux officiers de sécurité nommés au sein d'entreprises ou d'administrations) pour ajouter que dans ces 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 par les hôteliers les documents d'inscription de voyageurs, sans préciser s'il y a obligation de tenir de tels documents ni l'existence ou non du droit des hôteliers de refuser la transmission de tels documents.

28. En fonction des **personnes** sur lesquelles 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 pour toute personne qui doit faire l'objet d'une habilitation de sécurité, d'être informé sur le niveau et l'objet de l'habilitation, sur les types de données à collecter et sur les procédures

---

58 Ainsi, par exemple, 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.

59 Avis du Conseil d'Etat, p. 32.

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 »[60] ne constitue pas un consentement au sens de la directive de protection des données ou de la loi du 8 décembre 1992 telle que récemment revue, 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'une emploi et que le consentement ne peut faire l'objet d'un retrait.

Sur cette légitimité de l'enquête des services de sûreté à propos de personnes susceptibles d'être confrontées à des informations classifiées et les limites de telles enquêtes, on cite trois arrêts de la Cour de Strasbourg : le premier donne raison aux auteurs de la loi lorsqu'il affirme à propos de la plainte d'un charpentier chargé de travailler sur une base navale militaire et qui avait fait l'objet d'une enquête de sécurité dont les résultats ne lui avaient pas été communiqués malgré sa demande : « The fact that the information released to the military authorities was not communicated to Mr. Leander can not by itself lead to the conclusion that the interference was not « necessary in a democratic society ... », as it is the very absence of such communication which at least, ensures the efficacy of the personnel procedure ... »[61]. Cette position de principe n'interdit pas, selon deux arrêts ultérieurs de la même Cour, 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[62].

- 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[63], « le projet ne spécifie pas quelles personnes[64] au sein des services concernés peuvent accéder aux données à caractère personnel ».

---

60 En ce sens, avis de la Commission de la protection de la vie privée n° 22/96 en date du 4 septembre 1996.

61 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.

62 À ce propos, les arrêts Malone v. U.K. (1984) et Halford v. U.K. (1997) cités et commentés par L. BYGRAEVE, « Data Protection Pursuant to the Right to Privacy in Human Rights Treaties », *I.J.L.I.T.*, 1998, p. 261 et s.

63 Avis n° 12/98, p. 7.

64 Sans doute, serait-il nécessaire sur base du principe de la sécurité des traitements affirmé par l'article 16 de la loi « vie privée » que les personnes qui accèdent aux données soient désignées

Rappelons à ce propos que les services de renseignements et de sécurité sont soumis à de nombreuses obligations par la loi du 8 décembre 1992 telle que revue, comme 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'ait pas été prise en considération[65].

À 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).

- 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 ». À 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

---

sinon nominativement au moins en raison de leurs fonctions et qu'un registre des accès soit tenu par le responsable du traitement.

65 *Cf.* en ce sens, les critiques du comité R dans son rapport publié aux documents parlementaires.

s'assurer de son respect des prescrits de confidentialité, propres aux données transmises.

- 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 nœud du problème, tant il apparaît que les deux alinéas dans leur application concrète peuvent se révéler contradictoires. En particulier, 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[66], il serait préférable de prévoir qu'à chaque dossier 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. À l'expiration de cette date, la destruction ou l'« anonymisation » doit être ordonnée 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[67] qui veillera à la conciliation des intérêts contradictoires du service et de la personne concernée. Un système similaire existe au sein d'Europol pour les fichiers d'analyses contenant des données à caractère personnel.

---

66 Par utilisation significative, on entend la dernière inscription d'un renseignement présentant une valeur informationnelle nouvelle dans le « dossier » de la personne concernée.

67 Nous proposons voir *infra* nos conclusions qu'un « détaché » à la protection des données (selon la terminologie de la directive « vie privée » ou un « préposé » (selon la terminologie de notre loi belge) soit en charge de cet examen périodique.

CHAPITRE III. UNE BALANCE DES INTERETS PROBLEMATIQUE : L'ACCES « INDIRECT » AUX FICHIERS DES SERVICES DE RENSEIGNEMENTS

33. 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. Nous avons voulu développer ici de manière plus approfondie 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.

A. Le principe de l'accès « indirect »

34. L'article 13 de la loi du 8 décembre 1992 modifiée prévoit que l'exercice des droits d'accès et de rectification[68] 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 la sûreté de l'État, 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 (article 3, §4) ;

— 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 ;

68 La loi du 11 décembre 1998 y ajoute de manière explicite les droits de suppression ou d'interdiction d'utilisation de données non pertinentes, incomplètes, conservées trop longtemps.

— 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 le Comité permanent de contrôle des services de police et son service d'enquêtes en vue de l'exercice de leurs missions légales (article 3, §5).

L'article 3, §6 ajoute une exception au profit du Centre européen pour enfants disparus et sexuellement abusés; cette exemption sera applicable après autorisation accordée par le Roi.

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 »[69], qui a mis sur pied le système d'accès indirect pour les traitements « intéressant la sûreté de l'État, la défense et la sécurité publique ».

B. La procédure suivie

35. En droit belge, la personne qui souhaite exercer son droit d'accès indirect et qui s'adresse 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 le concernant.

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[70].

---

69 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 39. Un autre système existe toutefois en France pour les « Renseignements généraux » : suivant cette procédure, si les informations concernant le requérant ne mettent pas en cause la sûreté de l'État, 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 aux fichiers informatisés, manuels ou mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi n° 78 –17 du 6 janvier relative à l'informatique, aux fichiers et aux libertés).

70 La loi du 11 décembre 1998 élargit quelque peu cette possibilité de communication des résultats à l'intéressé, mais cet élargissement ne concerne que les traitements de données à caractère personnel gérés par des services de police en vue de contrôles d'identité.

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'État[71].

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'État.

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'une habilitation 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 notion 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 »).

Il nous semble qu'une balance des intérêts effectuée au cas par cas ne met pas en péril la protection du secret. Il est clair néanmoins qu'une balance des intérêts globale représente une charge de travail moins lourde pour les services concernés, qui peuvent se contenter de renvoyer toutes les demandes d'accès à la Commission. 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).

---

71 Exposé des Motifs, *Doc. parl.*, Ch. Repr., n° 1610/1, pp. 18-19.

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 (en particulier, l'utilité de l'intervention de la Commission est mise en doute).

C. Textes applicables

37. Un tour d'horizon des textes et principes applicables montre que les impératifs de sûreté de l'État et de défense nationale sont bien sûr pris en compte et sont à l'origine de dérogations accordées aux services concernés ; mais il apparaît que, justement, c'est de dérogations qu'il s'agit, à apprécier de manière la plus individualisée possible. 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[72].

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'État, à la sûreté publique, aux intérêts monétaires de l'État 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[73] 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*

72 On renvoie, pour ce qui est de la directive européenne 95/46 à ce qui est exposé *supra*, aux n^{os} 5 et s.

73 Mais dont l'application peut être étendue aux services de renseignement.

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 au droit d'accès direct peuvent être autorisées si elles sont *indispensables* (cette condition devant s'apprécier au cas par cas, puisqu'une dérogation doit être *motivée*). 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[74], 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 Convention européenne de sauvegarde des droits de l'homme doivent répondre à des exigences procédurales supplémentaires assurant le droit de la défense des personnes concernées. 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[75]:

« Il échet (...) de déterminer, en fonction des circonstances de chaque espèce, (...) si les parents[76] 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'exige 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 »[77]. Le droit de se défendre est incorporé dans le droit au respect de la vie privée et familiale[78].

---

74 Arrêt McMichael c. Royaume-Uni, 25 janvier 1995, n° 51/1993/446/525.

75 Arrêt W. c. Royaume-Uni, 8 juillet 1987, série A n° 121-A.

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

77 Arrêt McMichael c. Royaume-Uni, paragraphe 91.

78 Un arrêt plus récent (arrêt McGinley et Egan c. Royaume-Uni, 9 juin 1998, n° 10/1997/794/995-996) énonce aussi, en rapport avec l'accès aux documents (paragraphe 101) : « Dans ces conditions, eu égard à l'intérêt des requérants à obtenir l'accès aux documents en question et à

D. Des propositions

39. 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.

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. (...)*

---

l'absence apparente d'un quelconque intérêt public à ne pas les communiquer, la Cour considère que l'article 8 faisait peser sur l'État 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'État n'a pas de raison particulière de refuser la communication des documents, il doit en donner connaissance aux intéressés. On ne reconnaît pas un droit de l'État à les garder secrets pour la simple raison qu'il s'agit de documents concernant des activités menées par l'armée.

Concrètement, le seul fait qu'un document ait trait à la sécurité de l'État 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'État »[79].

40. Il apparaît donc qu'en invoquant la publicité de l'administration plutôt que la loi de 1992 pour fonder une demande d'accès à des données traitées par un service de renseignements, un requérant aurait un accès éventuellement beaucoup plus étendu. Or, lorsque des demandes concernant cette problématique sont adressées à la Commission d'accès aux documents administratifs (la « CADA »), 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 »[80].

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.

41. Notons toutefois que l'accès pourrait désormais être refusé sur base de l'article 26§1 de la loi relative 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. » Dès lors, il suffit d'invoquer la classification pour refuser l'accès aux documents.

---

79 Exposé des motifs, projet de loi relatif à la publicité de l'administration, *Doc. parl*., Ch. repr., n° 1112/1, 92/93.

80 Affaire X / sûreté de l'État, S.21.11.1994., I/CAD/94/12. Jurisprudence constante.

Il nous semble toutefois que cet article doit également être lu à la lumière des textes cités ci-dessus ; en effet, la loi de 1994 tend à appliquer un principe constitutionnel et ne peut être ignorée dans l'application des autres lois. Une lecture respectueuse des deux lois doit conduire à n'appliquer une mesure de classification que dans les cas strictement nécessaires, en gardant à l'esprit que ladite mesure prive les personnes concernées de l'exercice d'un droit constitutionnel.

42. 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'État, ...), 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.

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'État ou tout autre motif sérieux imposerait aux services de ne garder que des informations réellement pertinentes, à jour, exactes, ... ce qui 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, sauvegardant ainsi le secret, si nécessaire.

CONCLUSIONS

43. Individuellement, les exigences de protection des données s'imposent à ceux qui sont en charge de la sûreté de l'État et de sa défense. Ces exigences doivent certes s'accorder aux particularités de la mission impartie à ces personnes et organismes. Ces particularités exigent 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 fonde.

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'État et les services de renseignements de ces missions mais apportera à ces organismes légitimité et meilleure confiance de la population.

44. 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. À 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'État et des services de renseignement. 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'État et vie privée est loin d'être une tâche impossible. Il suffit pour nos autorités de s'en convaincre et de le vouloir.