1 ÉTHIQUE ET ANALYSE : LA RELATION AVEC LE DECIDEUR

Guy Rapaille, Patrick Leroy, Dirk Peeters

La présente contribution reflète les réflexions personnelles des auteurs et n'engagent pas les institutions auxquelles ils appartiennent.

« Nothing is more important to national security and the making of conduct of good policy than timely, accurate, and relevant intelligence. Nothing is more critical to accurate and relevant intelligence than independent analysis"
Dennis C. Blair 22 Janvier 2009,
The Senate Select Committee on Intelligence (USA)

INTRODUCTION

Le renseignement est un concept ancien[1]. Il existe depuis que l'homme vit en société. L'historienne Rose Mary Sheldon, témoigne que « *[...] l'histoire du renseignement dans le monde antique montre comment, même en des temps plus primitifs, les systèmes de renseignement contribuaient à façonner la politique de défense et la politique étrangère des nations [...]* »[2]. Seul détenteur de la violence légitime[3], l'Etat utilise aujourd'hui ses services de renseignement intérieur ou

1. Ben Israël, I., *Philosophie du renseignement*, Editions de l'Eclat, 2004, p. 26.
2. Sheldon, R.-M., *Renseignement et espionnage dans la Rome antique*, Editions Les Belles Lettres, 2009, p. 48.
3. Weber, M., *Le savant et le politique*, in une édition électronique réalisée à partir du livre de Max Weber (1919), Paris : Union Générale d'Éditions, 1963, 186 pages. Collection : Le Monde en 10-18. P.67 http://dx.doi.org/doi:10.1522/ela.wem.sav

Ils doivent tout d'abord se connaître car il y va de la bonne relation entre client et fournisseur du renseignement. Du côté du client, il s'agit de savoir qui peut produire quoi, comment et dans quel délai. Du côté du fournisseur, il s'agit de connaître les exigences du client. Mais ils doivent surtout se reconnaître, c'est-à-dire donner un sens à la relation client-consommateur/fournisseur. C'est ce caractère dialogique qui va définir l'identité d'agent de renseignement, et l'identité d'un homme ou d'une femme politique ou d'un militaire (le décideur) comme acteur à part entière du cycle du renseignement. Les uns sont les donneurs de sens des autres.

LE CONSOMMATEUR DE RENSEIGNEMENT

Un « client-consommateur » de renseignement est généralement un décideur politique, une personne qui a le pouvoir d'influencer ou de déterminer les politiques et les pratiques au niveau international, national, régional, ou local. Mais il peut s'agir aussi d'un décideur militaire à des niveaux de commandement militaires divers, qu'ils soient stratégique (les prises de décision seront le fait du Ministre de la Défense et du Chef de la Défense), opérationnel (les prises de décision seront le fait de l'Etat-major et des commandants des composantes Air, Terre, Mer et Médicale) ou tactique (les prises de décision seront le fait des commandants d'unités déployées).

La globalisation mondiale a provoqué l'irruption d'acteurs non étatiques (multinationales, organisations internationales, Organisations non gouvernementales,...), gros « clients-consommateurs » de renseignements, fournis généralement par des agences de renseignement privées, puisqu'ils n'ont pas directement accès aux renseignements provenant des services officiels qui, d'ailleurs, n'opèrent pas avec des finalités liées à la logique du marché. Qu'ils soient politiques, militaires ou économiques, les « clients-consommateurs » expriment une demande à l'adresse des « fournisseurs » que sont les services de renseignement, mais qui donnent aussi un sens à l'activité de ces services, c'est-à-dire à la fois une direction et une signification à leurs activités.

Le « client-consommateur » est donc, comme l'exprime la CIA[6] : « *an authorized person who uses intelligence or intelligence information directly in the decision-making process or to produce other intelligence.*»

Le citoyen pourrait-il être considéré comme l' « *ultime client* », dans nos sociétés démocratiques ? Même s'il n'est pas décideur ? Qu'est en droit de savoir le citoyen, dont une part des impôts sert à financer les Services de renseignement ? Dennis Blair, en janvier 2009, affirmait : « *Therefore, there is a special obligation for the leadership of the Intelligence community to communicate frequently and candidly with the oversight committees, and as much as possible with the American people.[...]* »[7].

Tout ne peut être diffusé au grand public. Il y va de la sécurité de certaines opérations, des agents, des sources, etc... Certaines divulgations prématurées ou inappropriées peuvent aussi mettre en péril la sécurité intérieure du pays ou

6. Central Intelligence Agency, *A consumer's guide to intelligence*, Washington, DC – CIA, 1994.
7. Statement of Dennis Blair before the Senate Committee on Intelligence, United States Senate January 22, 2009.

extérieur de façon plus ou moins puissante et active selon que la menace intérieure ou extérieure sera plus ou moins importante, ou perçue comme telle, par un instinct de survie, de sa population, de ses structures, de son système politique.

Par ailleurs, la place et les missions qui sont dévolues aux services de renseignement sont également en relation avec le rôle que l'Etat dont ils dépendent estime devoir et pouvoir exercer pour la défense et la promotion de ses intérêts et dans les relations internationales. Certains services déploient plus d'activités que d'autres même si les Etats dont ils émanent sont de dimension comparable en termes de superficie, population, niveau de vie, richesses produites, ... selon la conception que s'est forgée chaque Etat pour la défense et la promotion de ses intérêts considérés comme vitaux.

La Belgique, comme la France, présentent une étonnante absence de culture en matière de renseignement. C'est un problème culturel et historique affirme Eric Denécé[4] citant le Général Christian Quesnot : « *Les politiques [...] estiment, souvent à tort, que les avantages que les services de renseignement procurent sont inférieurs aux inconvénients qu'ils suscitent* »[5]. C'est moins le cas dans les pays anglo-saxons où tant les décideurs politiques que les citoyens, à de rares exceptions, ont conscience de l'utilité des services pour le bien commun.

Nous aborderons, dans ce travail, la question de la relation entre les décideurs politiques et les services de renseignement, par le biais de l'analyse. Cette fonction majeure au sein de ceux-ci produit ce qui doit (devrait) permettre aux décideurs de prendre la décision adéquate. Nous montrerons que les relations entre ces deux acteurs génèrent des cas de conscience, des problèmes éthiques et poserons l'hypothèse que ceux-ci peuvent être résolus par la (ré-)instauration d'un climat de confiance. Nous conclurons en proposant une réflexion sur la communauté du renseignement.

LA RELATION ANALYSE/DÉCIDEUR : UN PROCESSUS DIALOGIQUE

Si les services de renseignement existent, c'est qu'ils répondent à un besoin, que ce besoin soit réel ou qu'il relève de la conception que l'Etat en question s'est donné de ses besoins. Aujourd'hui, au sein de ces services de renseignement, un langage managérial apparaît, à tort ou à raison. On parle désormais de « *produits finis* », de « *clients* », de « *services à produire* ». Quoi qu'il en soit, si les services de renseignement existent, travaillent, produisent, c'est qu'un client a exprimé plus une demande qu'un besoin. Il convient donc, comme dans toute logique commerciale qu'une compréhension mutuelle s'instaure : La relation entre le fournisseur du renseignement et le consommateur du renseignement est dialogique. Non seulement, ces deux acteurs du renseignement doivent se connaître, mais aussi se reconnaître.

---

4. Dénecé, E. et Arboit, G., *Les études sur le renseignement en France*, Centre français de recherches sur le renseignement, rapport de recherche n° 9, novembre 2009, p. 7.
5. Quesnot, C. (Général), « Perception, utilité et usage de la fonction connaissance et anticipation par le président de la République, chef des Armées », *les Cahiers de Mars*, n°198, décembre 2008, p. 31.

provoquer des crises diplomatiques. Le célèbre principe du *need to know* est une évidence. Cependant, dans nos démocraties, le citoyen n'est-il pas en droit de savoir, d'être éclairé sur les actions entreprises par les services de renseignement qui exécutent la politique décidée par les autorités qui sont elles-mêmes amenées à rendre des comptes au Parlement élu par ledit citoyen ? La question reste ouverte et dépasse largement le cadre de cette réflexion. Il n'en demeure pas moins qu'il existe – et qu'il existera toujours peut-être – une tension entre la nécessité d'assurer la discrétion et le secret du travail de renseignement et la légitime curiosité du public et des médias concernant précisément le travail de renseignement. Quant à l'intervention des organes de contrôle externes, quelles que soient leur forme, leur compétence, leur prérogative, qu'il soit simplement permis faire référence à une conclusion formulée par Tristan d'Albis[8] : « *le contrôle externe des Services de renseignement, loin d'être une sanction, serait pour eux, tant un gage de modernité qu'un signe indubitable de reconnaissance* ».

L'ANALYSE DANS LES SERVICES DE RENSEIGNEMENT

L'analyse dans le renseignement aborde des domaines souvent extrêmement sensibles et traite des données qui, régulièrement, sont volontairement fausses, trompeuses[9]. La Loi belge du 30 novembre 1998 organique des services de renseignement et de sécurité envisage cette situation puisqu'elle fixe l'ingérence parmi les menaces contre lesquelles doivent lutter les services de renseignement. Les « *moyens illicites, trompeurs ou clandestins* » sont au cœur même du travail des services et en constitue une particularité[10]. Dans le cadre du travail d'analyse, le doute est une vertu. La validité des données à la disposition des analystes est à remettre en cause constamment. La tromperie est une règle, souligne Rob Johnston. Les analystes dans notre profession doivent être entraînés à prendre cela en compte dans le processus analytique. Le secret, et les comportements inhérents à cette exigence, sont aussi une variable à prendre en compte.

Plusieurs auteurs spécialisés ont tenté de définir l'analyse en tant que composante du cycle du renseignement. L'approche de Sherman Kent est basée sur les trois fonctions de l'analyse, soit l'élément descriptif, le rapportage et l'estimation.

Bruce Berkowitz et Allan Goodman[11] définissent l'analyse comme un processus d'évaluation et de transformation de données brutes en descriptions, explications et conclusions pour un client.

D'autres enfin insistent sur l'apport personnel de l'analyste dans le processus en fonction de sa nature, son histoire, son environnement socio-économique,

---

8. D'Albis, T. et Miquel, P-A, « Au service de l'Etat », *Magazine des Anciens Elèves de l'ENA, dossier Le Renseignement*, 2006, octobre, n° 365,2-3 cité dans le *Rapport d'activités 2006* du Comité Permanent de Contrôle des Services de renseignement et de Sécurité (Belgique).
9. Johnson, R., *Analytic culture in the US Intelligence Community – an ethnographic studie*, Center for the study of Intelligence (CIA),Washington, 2005, p. 34.
10. *« tentative d'influencer un processus décisionnel par des moyens illicites, trompeurs ou clandestins »* Loi Organique du 30 Nov 98, article 8g.
11. Johnson , R., *op. cit.*, pp. 35-36.

entre autres, qualifiant l'analyse non pas seulement comme le produit de la connaissance, mais comme un processus cognitif en soi.

Les méthodes utilisées et la psychologie de l'analyste en tant qu'individu interagissent dans le processus analytique. On pourrait dès lors définir l'analyse dans le renseignement comme un processus sociocognitif, se produisant dans une sphère professionnelle habituellement secrète, par lequel un ensemble de méthodes est utilisé pour réduire un problème (ou une question) complexe à un ensemble d'hypothèses simples.

PROBLÈMES ÉTHIQUES DANS LA RELATION AVEC LE CONSOMMATEUR DE RENSEIGNEMENT

L'interaction Producteur/Consommateur ou la satisfaction des besoins

Deborah G. Barger [12] exprime clairement l'évolution de la relation « producteur-consommateur » depuis les événements du 11 septembre 2001. Trois dynamiques ont rapidement changé la perception par les services de ce que les consommateurs de renseignement attendent : « *qui sont les clients aujourd'hui, que veulent-ils et pour quand le veulent-ils* » ? La liste des clients potentiels a crû exponentiellement, générant des types de produits différents, affirme-t-elle. C'est le cas en Belgique aujourd'hui, par exemple, à la suite de la relation croissante des services de renseignement avec le Parquet fédéral, illustrée surtout dans le cadre de la lutte contre le terrorisme. L'attente du Procureur fédéral diffère de celle des décideurs à qui nous avons l'habitude de fournir nos produits. En France, précise Bernard Besson [13], un juge d'instruction n'a que faire des us et coutumes du monde du renseignement : « *Cela ne cadre pas avec mon code de procédure* » disent-ils.

Abstraction faite d'éventuelles techniques de marketing qui entendent influencer quelque peu ce processus, le monde de l'entreprise impose de calquer dans une large mesure la production sur les besoins du client. Les besoins et les attentes du client constituent les critères qui dictent le choix des produits mis sur le marché. Il peut s'agir dans ce cadre d'un besoin futur du client, qui semble justifier l'existence d'une marque et qui peut déboucher sur un produit innovant, ainsi que sur les recherches et le développement y relatifs. De même, au sein du secteur public, les produits et les services doivent correspondre aux besoins existants ou, éventuellement, futurs du client. Les administrations publiques disposent en effet de fonds publics pour leur fonctionnement. En contrepartie, ce fonctionnement est censé apporter une valeur ajoutée suffisante à la société. Les services proposés par un service public diffèrent sans nul doute à cet égard. Les autorités se démarquent du secteur privé par leur impossibilité de déterminer dans tous les cas et avec certitude qui est « le client ». « Le client » peut ainsi être un simple citoyen, un décideur politique, ou encore la société dans son

12. Barger, D.G., *Toward a Revolution in Intelligence Affairs*, Rand Corporation, 2005, p. 20 et suivantes.
13. Intervention de Bernard Besson au cours du séminaire sur l'Etique et le renseignement - Paris, le 5 mai 2008.

ensemble, voire des parties de celle-ci. La valeur ajoutée des services fournis par l'administration publique, aussi appelés « produits », fera l'objet d'une évaluation au regard de la perception que l'on a du « client ».

Le premier dilemme auquel l'analyse est donc confrontée est l'attente du décideur politique ou militaire et aujourd'hui judiciaire. Le décideur aura habituellement une tendance à accepter les produits analytiques qui soutiennent sa politique et ignorera les analyses en contradiction avec sa politique, affirme Robert M. Clark [14], ou tout simplement parce que ce qui lui a été fourni, réduit son champ de manœuvre ou les options qui s'offrent à lui. C'est également le cas du décideur militaire.

Bien évidemment l'éthique du service de renseignement et l'éthique individuelle de l'analyste imposent la fourniture d'une analyse objective. Le renseignement n'est pas un substitut de la politique ou de la sphère décisionnelle militaire, c'est un partenaire. Le décideur prendra dans ce cas la responsabilité de son choix, à charge peut être pour le Service de Renseignement de lui fournir une évaluation des conséquences de son choix.

Il pourrait arriver également que le décideur impose, dans l'étape « planning » (Plan directeur) du cycle de renseignement, soit des sujets de recherche, soit un niveau de priorité qui ne correspondent pas à la réalité du terrain, soit carrément exige la suppression d'une matière du Plan directeur. Ceci poserait problème pour plusieurs raisons. Tout d'abord, le respect strict du Plan directeur ainsi altéré empêcherait la collecte d'informations sur des matières dont la réalité par rapport à la menace est pourtant évidente. Ensuite, dans les relations entre les services, notamment dans le cadre de la Loi sur du 10 juillet 2006 relative à l'analyse de la menace qui a créé l'Organe central pour l'analyse de la menace [15], le critère de la pertinence ne pourrait plus être respecté car le service ne posséderait pas d'éléments suffisants pour répondre à cette exigence légale. La surévaluation politique ou militaire d'une menace exigée par le décideur serait moins problématique. Cependant, les rapports rédigés par l'analyse ne reflèteraient pas la réalité voulue par le décideur. Ici aussi, le dialogue devrait permettre de résoudre ce dilemme.

L'interférence entre politique et renseignement ne concerne pas seulement l'analyse mais aussi l'entourage du décideur, précisent Olivier Forcade et Sébastien Laurent [16]. Si l'interférence est faible, le renseignement sera vraisemblablement étranger à toute contingence partisane. Le contenu sera apparemment objectif. Si l'interférence prend la forme de pressions politiques au risque de dénaturer complètement l'analyse, il conviendrait alors que l'entourage du décideur, ou les techniciens du renseignement relayent auprès de lui l'analyse objective produite par les services. La proximité du dispositif de renseignement de l'échelon décisionnel est à ce niveau la solution à ce dilemme.

---

14. Clark, R.M., *Intelligence Analysis, a target centric approach*, Editions CQ Press Washington, 2006, p. 285.
15. Organe de Coordination pour l'Analyse de la Menace.
16. Forcade, O. et Laurent, S., *Secrets d'Etat : pouvoirs et renseignement dans le monde contemporain*, Editions Armand Colin , Paris, 2005, p. 49 et suivantes.

Un deuxième dilemme auquel est confronté le producteur de renseignement est la carence en informations brutes ou de sa capacité analytique (rapport d'analyse creux) face à la satisfaction des besoins du consommateur.

Il est éthiquement impensable de voir l'analyste jouer le rôle de collecteur d'information brute (*raw intelligence*), car il n'aurait pas le recul suffisant dans son rôle d'analyste par rapport à l'information brute. C'est ce que l'on pense actuellement dans la plupart des services de renseignement. David T. Moore[17] estime pourtant que l'avenir du renseignement passe par ce double rôle « collecteur-analyste » joué par le producteur de renseignement, par une méthode plus agressive de recherche d'informations, tant classifiées que non classifiées. L'analyste sait ce qu'il veut, comment il le veut, pour quand il le veut. Il possède ses propres critères de recherches. Nous ne sommes sans doute pas encore prêts à implanter cela au sein des services de renseignement en Europe.

Fausser un produit d'analyse en comblant les manquements analytiques par des éléments supposés, créés, dans le but à tout prix de satisfaire le « consommateur » n'est pas la réponse adéquate au dilemme non plus. Il serait aussi tentant pour l'analyse, afin de masquer les faiblesses du rapport, d'indiquer le peu de changement dans l'évolution du cas ayant généré la demande du « client-consommateur ». Mais au risque de lui faire prendre une mauvaise décision. Ceci pose l'exigence d'intégrité de l'analyste, de sa relation à lui-même.

L'objectivité s'exprime généralement en termes de neutralité, impartialité, désintéressement, ou impersonnalité. Il s'agit d'une prise de distance d'un individu vis-à-vis de lui-même pour se rapprocher d'un objet, étant admis que l'objectivité et la subjectivité sont mutuellement exclusives. L'individu objectif est censé, au moment de porter un jugement, abandonner tout ce qui lui est propre (idées, croyances ou préférences personnelles) pour atteindre une espèce d'universalité... On peut prétendre que, comme dans le milieu journalistique, l'objectivité est un idéal jamais atteint. En effet, elle dépend non seulement de la manière dont les informations sont exploitées et de l'importance relative qui leur est accordée. Il est, en outre, difficile pour tout rédacteur de s'abstraire d'un certain nombre d'influences liées à son milieu, son éducation, son pays d'origine, etc. Elle suppose aussi une connaissance parfaite et complète du sujet et de tous ses paramètres explicatifs, condition qui est, la plupart du temps impossible à satisfaire en pratique. Une contrainte supplémentaire réside dans l'expérience que doit acquérir un analyste. Celui-ci ne sera réellement efficace et surtout fiable qu'après une formation théorique et une pratique de l'analyse de plusieurs années. Force est de constater qu'en Belgique des jeunes analystes formés et qui commencent réellement à « produire » quittent les services de renseignement pour des fonctions équivalentes dans le secteur public ou privé.

Probité et liberté sont certainement les deux qualités majeures d'un analyste. Il doit être probe vis-à-vis de lui-même, vis-à-vis de la hiérarchie directe ou de ses subordonnés, vis-à-vis des fournisseurs d'informations brutes (HUMINT, SIGINT, ...), vis-à-vis des « clients-consommateurs » de renseignement, car

17. Moore, D.T., *Critical Thinking Analysis*, Joint Military Intelligence College, Washington DC, 2006, p. 93.

la clé du succès, c'est la confiance. Et il doit être libre de préjugés, libre de travailler sur des hypothèses, libre constructions de l'esprit et non des vérités révélées ou espérées par le consommateur de renseignement, libre de ses opinions personnelles, politiques ou idéologiques et libre de pressions éventuelles.

Producteurs de renseignement et clients-consommateurs s'adressent des reproches qui naissent de l'incompréhension mutuelle :

Le 1er reproche qui est adressé à l'analyse par les consommateurs est que les rapports contiennent des analyses très affinées sur des développements futurs possibles et ne réduisent pas les incertitudes. Les clients-consommateurs n'apprécient pas les hypothèses. Ou encore le renseignement fourni réduit leur choix d'options. Un reproche peut naître d'une controverse à la suite de la diffusion dans le public d'un renseignement incomplet créant une ambigüité. Le client-consommateur, politique dans ce cas-ci, craindra que le débat public n'incite le choix du « *worst case scenario* ». Une ambiguïté pourrait apparaître aussi à la suite d'une analyse plus faible, qui contient trop d'incertitudes sur les développements futurs. L'approximation rendra la vie du client-consommateur politique plus difficile.

Un autre reproche pourrait apparaître à la suite de la remise d'un rapport insipide. Comme nous exprimons ci-dessus, la tentation sera grande d'une démonstration par le producteur de renseignement de son « savoir » pour combler les carences du rapport.

Le producteur de renseignement n'est pas en reste. Un reproche assez courant adressé aux « clients-consommateurs » est qu'ils ont peur de l'incertitude, dès lors que le producteur de renseignement émet le plus souvent des hypothèses, ou alors, en cas d'un début de politisation des services, que les consommateurs utilisent le renseignement comme un instrument de persuasion vers le public. Dans le même ordre d'idée, les producteurs de renseignement estiment que les consommateurs voient le renseignement comme un moyen de rendre la politique bonne aux yeux du citoyen plutôt qu'un moyen de faire de la bonne politique. Enfin, deux grands classiques : l'incapacité ou l'absence de volonté du politique de favoriser l'approche à moyen et long terme des services et l'absence de guidance et de *feed back* du politique vers les services, important pourtant dans le cadre du cycle du renseignement[18].

Un constat général s'impose : le manque de dialogue, le manque de connaissance du rôle et des besoins des deux parties.

La position d'un client-consommateur, dans son monde, mérite d'être examinée, comme la position d'un analyste dans son monde mérite également d'être examinée. L'un, est vulnérabilisé par sa position, les erreurs sont impardonnables dans la jungle politique. L'homme politique doit agir, vite. L'analyste est sans doute plus « contemplatif ». Il évite les certitudes et aime plutôt conseiller la prudence. La relation des acteurs à la notion de temps sera examinée ci-après.

Quelques exemples illustrent ce premier point : Les rapports des services de renseignement américain et britannique concernant l'éventuelle présence d'armes

18. Caprini, M., "Controlling and overseeing intelligence services in democratic states", in H. Born and M. Carpini, *Democratic control of intelligence services*, Ashgate, 2007.

de destruction massive en Irak en 2003 constituent à cet égard l'exemple le plus documenté de ces dernières années. Cette supposée présence a justifié l'invasion du pays par les troupes américaines et britanniques. Des enquêtes de contrôle effectuées par après ont montré que les rapports des services de renseignement américain et britannique avaient souffert d'interventions politiques[19]. Les enquêtes relatives aux rapports de renseignement sur les armes de destruction massive en Irak démontrent par ailleurs la volonté affichée par les décideurs politiques d'approuver les seules analyses qui viennent à l'appui de leurs idées, au détriment de celles qui en divergent.

Nous observons ce même phénomène - qui est, répétons-le, source de tensions entre les décideurs politiques et ceux qui fournissent le renseignement - dans le domaine de l'extrémisme politique.

Bien que le fonctionnement des services de renseignement fasse l'objet d'un contrôle démocratique fort étendu dans les pays occidentaux, de nombreux hommes politiques cultivent une certaine méfiance à l'égard des rapports rédigés par les services de renseignement en ce qui concerne l'extrémisme politique. *Grosso modo*, l'intérêt porté par les services de renseignement à des organisations d'extrême gauche semble susciter la méfiance de politiciens davantage gauchistes. Le même schéma s'applique au spectre politique de droite. L'explication réside certes dans le questionnement de ces hommes politiques par rapport aux frontières posées par le service de renseignement. En d'autres termes, quelle est la conception de l'extrémisme développée par ce dernier[20] ?

Citons à titre d'exemple la récente polémique apparue aux Etats-Unis d'Amérique à la suite de la publication d'une évaluation de la menace par le Department of Homeland Security (DHS). Celle-ci illustre à merveille les différentes réactions à l'égard d'un produit du renseignement, dictées par l'orientation politique du destinataire.

Dans ce rapport d'avril 2009, rédigé par l'Office of Intelligence and Analysis, le DHS évoque la menace que pourraient représenter à l'avenir les milices d'extrême droite présentes aux Etats-Unis et dont l'action s'articule autour de divers thèmes tels que l'immigration illégale, le rôle trop actif joué par le gouvernement fédéral, l'avortement et la limitation de la détention d'armes à feu[21]. Selon le DHS, la crise économique actuelle, combinée à l'élection du premier président afro-américain, représente un formidable terreau pour le recrutement par les milices radicales d'extrême droite aux Etats-Unis. Celles-ci sont dès lors en passe de représenter la principale menace pour la sécurité intérieure du pays.

---

19. United States Senate, Select Committee On Intelligence, *Report On the U.S. Intelligence, Community's Prewar Intelligence Assessment on Iraq*, July 7, 2004. U.K. House of Commons, "Review of Intelligence on Weapons of Mass Destruction", *report of a Committee of Privy Counsellors*, July 14th, 2004. *The Guardian*, "We got it wrong on Iraq WMD, intelligence chiefs finally admit", April 8th, 2005.

20. Peeters, D., et Segers, J., « Services de renseignement et extrémisme », in M. Cools et al., *La Sûreté. Essais sur les 175 ans de la Sûreté de l'État*, Bruxelles, Politeia, 2005, pp.281-302.

21. Department of Homeland Security, Office of Intelligence and Analysis, "Rightwing Extremism:Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment.", April 7, 2009.

Les milieux conservateurs de droite ont violemment réagi à la parution de ce rapport. Selon ces milieux conservateurs, le rapport entend stigmatiser les groupes qui s'insurgent contre l'avortement, contre l'immigration et contre l'étendue du pouvoir exercé par le gouvernement fédéral.

Mentionnons à cet égard la parution, deux mois plus tôt, d'un rapport similaire rédigé par le Missouri Information Analysis Center (MIAC), et qui évoquait la possibilité que certains groupes conservateurs de droite soient liés au terrorisme intérieur[22]. Ce rapport a provoqué lui aussi une vague de protestations parmi les conservateurs de droite sur tout territoire des Etats-Unis. Ainsi le responsable de la Missouri Highway State Patrol en a-t-il appelé publiquement à une réflexion sérieuse concernant les procédures d'élaboration de ce type de rapport, voire à une remise en question à l'avenir de l'autorisation accordée au MIAC de rendre de telles analyses publiques[23]. Le fait de considérer, dans les rapports précités, les milices d'extrême droite comme étant la principale menace potentielle aux Etats-Unis constitue sans nul doute un revirement par rapport aux analyses effectuées par le DHS sous l'administration du président George W. Bush et qui portaient sur les menaces intérieures. Sous cette présidence, les rapports du DHS - ainsi que ceux rédigés par le Federal Bureau of Investigation (FBI) - présentaient l'extrémisme écologique et de gauche comme les principales menaces pour le pays. En janvier 2009, le DHS publiait un nouveau rapport en ce sens[24].

Force est de constater qu'un changement dans l'administration à la présidence des Etats-Unis se solde très rapidement par la parution d'analyses fort divergentes sur le même sujet. Il est malaisé de l'expliquer: est-ce le résultat d'une autocensure des analystes du renseignement, y a-t-il eu des pressions politiques, ou s'agit-il d'un parti pris idéologique des responsables du service de renseignement ?

En Belgique, la loi organique des services de renseignement et de sécurité du 11 novembre 1998 définit l'extrémisme de la manière suivante: « *les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'Etat de droit* ». La loi considère l'extrémisme comme un des sept phénomènes susceptibles de menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, le potentiel scientifique ou économique.

Tout lecteur qui s'attarde sur ce passage de la loi comprendra aisément que cette définition entend seulement fournir un cadre général à la notion d'extrémisme et est donc sujette à interprétation. C'est précisément cette possibilité d'interprétation qui peut mener à controverse et semble susciter une certaine méfiance de la part des hommes politiques et du grand public.

---

22. Missouri Information Analysis Center, "MIAC Strategic Report. The Modern Militia Movement.", February 20, 2009.
23. WorldNetDaily, "Homeland Security on guard for 'right-wing extremists'", April 16, 2009. WorldNetDaily, "State drops warnings over 'militia' members.", April 16, 2009.
24. Department of Homeland Security, "Leftwing extremists Likely to Increase Use of Cyber Attacks over the Coming Decade.", January 6, 2009.

Le débat qui s'est développé en Belgique autour de la *Proposition de loi relative aux méthodes de recueil de données des services de renseignement et de sécurité* illustre de manière éclatante cette tendance. Pour les uns – dont certains liés à des mouvements d'extrême gauche – la proposition de loi représente une menace permanente de l'état de droit en raison notamment de ce qu'ils considèrent comme une absence de contrôle de ces méthodes[25].

La préservation du secret, source principale du dilemme éthique ?

Nous sommes entrés depuis plus d'une décennie dans l'ère de l'information avec comme conséquence l'avènement des sources ouvertes. Les experts en renseignement tant français qu'anglo-saxons s'accordent à dire que près de 85 % du renseignement utile provient de ce moyen de collecte (OSINT). Les 15 % restants proviennent d'opérations clandestines, du traitement des informateurs et représentent, par conséquent, la notion de secret au sein des services – le Secret-défense en France par exemple –, selon certains auteurs, dont ils se plaisent à souligner le paradoxe.

Pourtant, cette décennie est aussi la décennie pendant laquelle les espions sont sortis de l'ombre, que ce soit de leur plein gré ou non, a affirmé un haut responsable du SCRS (Service de renseignement canadien), lors de la conférence Global Futures Forum à Vancouver en 2008. Le public en connaît maintenant plus que jamais sur le monde du renseignement et la transparence est probablement aussi plus grande que jamais.

Le Secret d'Etat, la Raison d'Etat sont une part des méthodes de fonctionnement et de l'activité des Etats, dont dépendent les services de renseignement dans le monde, que cela soit à des fins diplomatique, politique, économique ou industrielle, que l'Etat soit démocratique ou totalitaire. L'histoire regorge d'exemples, nous ne citerons, pour mémoire, que l'affaire Dreyfus. En mai 2009, les médias rappelaient le travail effectué par le Parlement européen sur les vols secrets et les prisons secrètes de la CIA en Europe, en soulignant les tentatives infructueuses de la présidence portugaise de la commission temporaire de faire la lumière sur ces activités secrètes. Le Parlement européen s'était élevé contre le « *lourd silence de la plupart des gouvernements concernés* »[26]...

D'un point de vue juridique, le droit belge ne définit pas comme telle la notion de secret, mais la jurisprudence a toujours a toujours interprété le terme « secret » dans le sens commun, c'est-à-dire celui du dictionnaire. L'article 458 du Code pénal (qui sanctionne la violation du secret professionnel) est d'application générale et vise aussi les membres des services de renseignement qui de plus sont tenus par des dispositions spécifiques prévues soit par la loi organique des services de renseignement et de sécurité, soit par la loi relative à la classification et aux habilitations, attestations et avis de sécurité.

Au-delà du secret généré par la partie clandestine des opérations menées par les services de renseignement, il y a sa protection. La loi organique du

25. *De Standaard*, "BIM, een continue bedreiging voor de rechtsstaat." (La loi-BIM, une menace permanente pour l'état de droit), 1er juillet 2009. De Morgen, "De nieuwe BIM-wet, met de B van Bedreigend." (la nouvelle loi BIM, avec un B (un M) de Menaçante), 8 juillet 2009.
26. *Le Soir*, 20 mai 2009.

30 Novembre 1998 qui régit les deux services de renseignement belges précise en son Article 11§3 que *« le SGRS a pour mission de protéger le secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et l'accomplissement des forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que le Ministre de la Défense gère. »*

Le maniement de l'information doit répondre à certains impératifs en matière de discrétion. Les lecteurs des romans d'espionnage et les fans de films du même genre reconnaîtront l'importance de notions telles que le « *besoin d'en connaître* », la « *règle du tiers service* » ou encore le « *danger source* ». Le concept du « besoin d'en connaître » se réfère à la nécessité de compartimenter l'accès à l'information. En d'autres termes, cette dernière n'est accessible qu'aux seules personnes qui peuvent justifier d'un intérêt pour cette information et de la nécessité d'en prendre connaissance. La « règle du tiers service » stipule que toute information transmise par un service de renseignement à un autre demeure la propriété du service d'origine. En conséquence, le destinataire de l'information ne peut l'utiliser qu'avec l'autorisation de son propriétaire, et dans le respect des conditions posées par ce dernier. Cette règle majeure qui gouverne l'échange d'informations entre les services n'est très souvent que peu, voire pas du tout comprise par les non-initiés. Le « danger source » attire l'attention sur le risque encouru par la source de l'information, susceptible d'être identifiée en cas de mauvaise gestion de cette dernière, avec toutes les conséquences que cela implique. Dans des cas extrêmes, la sécurité physique de la source peut être menacée. Il s'agit là d'un concept qui ne nécessite la plupart du temps que fort peu d'explications et qui peut généralement être appréhendé par ceux qui n'appartiennent pas à la communauté du renseignement. Nous retrouvons en effet cette notion dans d'autres milieux tels que celui du journalisme, par exemple.

Outre ces concepts généraux d'application au sein de la communauté du renseignement, la plupart des pays disposent d'une base légale organisant le maniement de l'information confidentielle. La loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité prévoit en son article 3 la classification des informations, documents ou données, le matériel, les matériaux ou matières, sous quelque forme que ce soit, dont l'utilisation pourrait porter atteinte à toute une série d' intérêts comme l'intégrité du territoire national la sécurité intérieur et extérieure de l'Etat, entre autres.

Par classification, il faut entendre l'attribution d'un niveau de protection par ou en vertu de la loi, ou encore par ou en vertu des traités et des conventions liant la Belgique. Peuvent faire l'objet d'une classification : les informations, documents ou données, le matériel, les matériaux ou matières, sous quelque forme que ce soit, dont l'utilisation inappropriée peut porter atteinte à l'un des intérêts suivants: la défense de l'intégrité du territoire national et des plans de défense militaire, l'accomplissement des missions des forces armées; la sûreté intérieure de l'Etat, y compris dans le domaine de l'énergie nucléaire, et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations

internationales de la Belgique; le potentiel scientifique et économique du pays; tout autre intérêt fondamental de l'Etat; la sécurité des ressortissants belges à l'étranger; le fonctionnement des organes décisionnels de l'Etat.

La classification comprend trois degrés : TRES SECRET, SECRET, CONFIDENTIEL. Le degré TRES SECRET est utilisé lorsque l'utilisation inappropriée peut porter très gravement atteinte à un des intérêts précités. Le degré SECRET est attribué lorsque l'utilisation inappropriée peut porter gravement atteinte à un des intérêts précités. Le degré CONFIDENTIEL est attribué lorsque l'utilisation inappropriée peut porter atteinte à l'un des intérêts précités. L'utilisation susvisée comprend notamment la prise de connaissance, la détention, la conservation, l'utilisation, le traitement, la communication, la diffusion, la reproduction, la transmission ou le transport.

Ainsi, compte tenu de cette classification, une autorité en Belgique n'est autorisée à prendre connaissance d'informations classifiées que si elle dispose d'une habilitation de sécurité d'un niveau au moins identique au degré de classification de celles-ci.

Pour les services, l'attribution de degrés de classification et la mise en œuvre des principes du « besoin d'en connaître », de la règle du « tiers service », et du « danger source », visent uniquement à limiter et à contrôler l'accès à l'information « sensible » dans le but de protéger cette information ainsi que sa source. Pour certains, il s'agit incontestablement d'un obstacle à la nécessité de transparence et au contrôle démocratique. Cependant, on ne peut ignorer la nécessité d'une certaine ouverture et d'un contrôle démocratique des activités des services de renseignement. Le maniement correct de cette nécessité et la recherche d'un juste équilibre constituent un défi permanent pour tout service de renseignement d'un état démocratique. L'époque des services « secrets » œuvrant incognito dans l'ombre est depuis longtemps révolue.

Olivier Forcade et Sébastien Laurent[27] précisent que le secret est bien constitutif de la démocratie. Constituée sur le principe de la publicité et de la transparence, la démocratie n'a pu, et ne peut toujours progresser qu'en acceptant une part d'ombre et de secret.

Comment combattre, de plus, le spectre du terrorisme dans ce qu'il a de plus irrationnel sans une part de travail clandestin ? Les mêmes auteurs ont rappelé avec intérêt un arrêt de la Cour des droits de l'homme (1978) des plus clairs en cette matière : « *les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'Etat doit être capable pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire.* »

Pour John B. Chomeau et Anne C. Rudolph[28], pourtant, la source principale du dilemme éthique est la préservation d'un secret dans une société démocratique, ouverte. Ce dilemme éthique réside tout d'abord, disent-ils, par une notion

27. Forcade, O. et Laurent, S., *op. cit.*, pp. 213 et suivantes.
28. Chomeau, J.B. et Rudolph, A., "Intelligence Collection and Analysis, dilemma and decisions", in J. Goldman, *Ethics of Spying*, The scarecrow Press, Inc. Lanham, Maryland, Toronto, Oxford 2006 p.114 et suivantes.

peu claire de qui est notre « *clientèle* » et puis, plus particulièrement par les circonstances qui appellent une nécessité de classification du renseignement. L'éthique s'affronte au traditionnel secret, au *need to know*, à la méfiance et aux techniques de *deception*[29].

Comme nous l'exposions plus haut, le secret, la clandestinité de certaines opérations vont croître en fonction de la situation dans laquelle se trouve le pays, situation de crise, de guerre, de paix, ou encore en fonction du régime politique qui le dirige, démocratie, dictature.

Cela revient-il à dire que plus le régime est démocratique, plus la transparence semble de rigueur ? Sans doute, mais ce n'est pas aussi simple. Même en temps de paix, il convient d'assurer la protection de toute une série de données dont l'utilisation inappropriée pourrait porter atteinte, comme le précise la loi[30], à la défense de l'intégrité du territoire national et dans plans de défense militaire, à l'accomplissement des missions des forces armées, à la sûreté intérieure et extérieure de l'Etat, etc... C'est le secret défini par Michel Senellart, « *l'horizontalité du cryptogramme* », « *le sceau du secret* », à côté des mystères (arcana) et des machinations et stratagèmes[31].

Ce débat secret/transparence est un débat sans fin. Le dilemme se situe dans la détermination de ce qui doit impérativement être gardé secret et ce qui peut être présenté au public. Dans nos sociétés démocratiques, le rapport à la confidentialité, au secret est compris du public. Le projet de loi sur les méthodes particulières de recherches pour les services de renseignement belges prévoit cependant une exception pour les professions telles que journalistes, avocats. Pour certaines professions, leur obligation du secret suscite la confiance[32] nous rappelle Daniel Bérésniak. Depuis toujours, le notaire, le médecin et le prêtre, sont des détenteurs de secrets, mais aussi des personnes de confiance. Guillaume-Gustav De Valk a raison de souligner cependant que si tout est classifié, alors rien ne l'est. Moins il y a de secrets, plus ce qui doit être réellement protégé le sera sérieusement. Aussi, il est impératif de revoir aujourd'hui notre volonté de classifier, de surclassifier certains renseignements, par souci plus de publicité et de transparence.

A l'heure où nous rédigeons, les députés français examinent le projet de loi de programmation militaire (LPM) 2009-2014 lors d'un débat qui sera dominé par la question du secret-défense. Le texte du ministre de la défense, Mr Hervé Morin, durcit, en fait, les règles en vigueur pour sa protection[33]...

En Belgique, le Comité permanent « R » a déjà fait le constat que les services pouvaient avoir tendance à surclassifier des renseignements par rapport aux critères définis par la loi du 11 décembre 1998 relative à la classification et

---

29. Deception : *« action de tromper et d'induire en erreur. Partie intégrante des mesures actives. La déception peut être pratiquée aux niveaux politique, stratégique, opératif et tactique. »* Jacques Baud , Encyclopédie du renseignement et des Services secrets, Lavauzelle, 1998, p. 162 et suivantes.
30. Loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (Belgique).
31. Senellart, M., *Les arts de gouverner. Du regimen médiéval au concept de gouvernement*, Editions du Seuil, 1995, p. 249.
32. Bérésniak, D., *Secrets, pourquoi on parle, pourquoi on se tait*, Editions Grancher, 2004 , p. 145.
33. http://tempsreel.nouvelobs.com/depeches/politique/20090607.FAP6675/secret_defense_lundi_et_mardi_a_lassemblee.html

aux habilitations, attestations et avis de sécurité et à proposer la création d'un mécanisme permettant soit la rectification d'une classification abusive ou d'une déclassification plus large après l'écoulement d'un certain laps de temps. Ici aussi, il n'existe pas de solution-miracle et tout est question d'équilibre entre la nécessité de protéger un secret et une certaine ouverture destinée à accroître la confiance du public.

De nombreux services de renseignement se sont depuis un certain temps déjà attelés à la mise en œuvre d'une stratégie et d'une politique de communication. Des services de renseignement européens tels que l'AIVD néerlandais, le BfV allemand, le CNI espagnol, le BIS tchèque, pour n'en citer que quelques-uns, disposent de leur site Internet créé par des professionnels et par le biais duquel ils tiennent le public informé de leur fonctionnement. Le Bundesamt für Verfassungsschutz (BfV) allemand, par exemple, publie sur son site quantité de rapports périodiques sur des phénomènes que ce service est habilité à suivre. Nombre d'autres services publient leur rapport annuel ainsi que des brochures de sensibilisation.

La Sûreté de l'Etat belge (VSSE) est, parmi les services de renseignement européens, celui qui jusqu'à présent a le moins œuvré au développement d'une stratégie de communication. Il lui faut dès lors rattraper son retard.

Le développement de canaux de communications afin d'informer le public du fonctionnement et des activités du service constitue un défi pour la VSSE. En effet, peu de pays européens - mis à part quelques anciens états communistes d'Europe centrale et orientale - enregistrent une aussi grande méfiance à l'égard de leur service de renseignement. Celle-ci est la conséquence d'une détérioration notable de l'image de ce service au siècle passé, dans le milieu des années quatre-vingt et au début des années nonante.

Mathieu Magherman, dans une thèse de 2007, se penche sur le degré d'ouverture et de communication de la communauté du renseignement belge - qui compte la VSSE et le Service Général de Renseignement et de Sécurité (SGRS) militaire - à travers les ans[34].

Dans son étude, Magherman fait état des timides tentatives effectuées par la VSSE depuis la seconde moitié des années nonante du vingtième siècle afin d'améliorer sa communication avec le monde extérieur. Le nombre restreint de sources écrites relatives au service de renseignement civil belge qu'il lui a été permis de consulter pour écrire son rapport montre bien combien ce service oeuvrait dans l'ombre à l'époque. Comme nous l'avons mentionné, les années nonante témoignent d'un début de changement à cet égard. Depuis lors, la direction du service s'ouvre toujours davantage aux media. Il n'est toutefois que peu question, pendant cette période qui suit la Guerre froide, d'une véritable politique de communication structurée. Chaque administrateur général en poste développe sa propre vision en la matière, que traduit le degré de communication du service. Selon Magherman, le manque de communication vers l'extérieur durant les dix dernières années de la Guerre froide a fait de la VSSE une cible facile pour nombre de théories du complot autour de divers dossiers controversés

34. Maghermann, M., *La Grande Muette: Why the Sûreté de l'Etat has been lagging behind in openness*, King's College, London, 2007.

à cette époque. Elle a de même contribué à ternir son image, une atteinte qui s'est poursuivie jusqu'à nos jours.

Magherman conclut qu'il appartient aux responsables politiques d'un service de renseignement d'imposer à ce dernier une politique en matière de communication et de la diriger. Lorsque le service décide lui-même de la portée et de la direction de cette communication, lacunes et inconsistances apparaissent car il ne peut se défaire de sa tradition du secret.

La mesure dans laquelle un service de renseignement peut aller de l'avant et apporter plus de clarté quant à la nature de son travail et quant à son rôle dans la société, est indissociable de la mesure dans laquelle est discutée la présence d'une culture du renseignement. Autrement dit, on ne peut faire l'économie d'un débat de société sur le sujet, et d'une connaissance minimale du rôle d'un service de renseignement de la part du public, de la presse et de la classe politique. Pourtant, on ne peut que constater la mise en veilleuse d'une telle culture du renseignement en Belgique.

Il s'ensuit à nouveau une méfiance à l'égard des services de renseignement, comme évoqué dès le premier problème éthique (l'interaction producteur-consommateur). La pensée sous-jacente est ici que le soi-disant besoin du maintien du secret est utilisé abusivement soit pour camoufler ses propres manquements ou son inefficacité, soit dans le but de poursuivre des agenda cachés.

Le facteur temps

« I believe we should get more information before news media does »[35]

Cette évaluation de Deborah Barger amène deux réflexions. L'adaptation des Services de renseignement aux nouveaux modes de communication et la rapidité de transformation de l'information brute en un produit utilisable par un décideur.

Les événements du 11 septembre ont, nous l'avons déjà écrit, changé les exigences des « clients/consommateurs » de produits issus de l'analyse, mais aussi des pratiques opérationnelles. Nombre de services se sont réorganisés, restructurés, fusionnés. Nous nous dirigeons vers une révolution dans les pratiques du renseignement, comme elle le souligne par le titre de son ouvrage.

Les jeunes générations se sont habituées à la rapidité offerte par les moyens de transmissions. L'avènement technologique tel que les blogues, *Facebook* et autres serveurs internet propulsent plus que jamais les services de renseignement dans l'ère de la communication. Tout comme les réseaux terroristes, du reste.

Il ne faut pas confondre rapidité de transmission du renseignement et le temps nécessaire pour le confectionner. Pour un service de renseignement et par conséquent pour l'analyste qui doit fournir le renseignement au client-consommateur, le temps est une notion importante, surtout en fonction du type de produit demandé.

Il existe plusieurs types d'analyse qui correspondent à des exigences différentes.

L'analyse à court terme qui se confond de facto avec l'analyse opérationnelle.

35. Barger, D.G., *op.cit.*, p. 20.

C'est une analyse qui permet l'évaluation rapide de dossiers opérationnels. Elle permet éventuellement de réorienter une enquête ou une recherche d'information en cours.

L'analyse à moyen terme qui est une analyse de moyen terme (souvent associée à une analyse opérative). Elle permet d'étudier un phénomène plus large sur un laps de temps plus long. L'analyse à long terme qui est souvent associée à l'analyse stratégique. Elle doit permettre à l'autorité politique ou militaire d'avoir une meilleure perception des risques à venir. Une bonne analyse stratégique doit donner le temps aux autorités de développer des politiques préventives afin de diminuer les risques potentiels et d'éviter l'essor de menaces précises.

Le client-consommateur n'a pas toujours la même perception du temps. Ce qui fait défaut, dans tous les services de renseignement, c'est ce temps. Une des conclusions du séminaire organisé à ROME par la Sherman Kent School, début avril 2004, révélait que la crise incite les décideurs politiques à exiger, quasi exclusivement, des analyses en temps réel, analyses qui alimentent leurs cabinets.

Tout ce que nous faisons aujourd'hui dans les services de renseignement publics relève de la compétition propre au secteur privé. « *If we are not timely, we are not relevant* » affirme un expert américain. C'est une quasi obligation pour assurer la survie de nos Services. D'autant que les « décideurs-consommateurs » de renseignement créent parfois leur propre réseau d'informations pour palier généralement ce qu'ils qualifient, à tort, de carence des Services.

Le dilemme auquel les analystes sont confrontés est la satisfaction en temps et en heure des exigences du « client-consommateur » dans cette compétition ouverte aujourd'hui, entre services de renseignement public et privé, compétition alimentée par leur comportement « clientéliste ».

Revenant à cette relation dialogique décrite plus haut, il se pourrait que les « clients-consommateurs » perdent leur crédit auprès des services de renseignement publics, dès le moment où ils favoriseraient une forme de connaissance alternative. par une société réseautée, grâce à Internet entre autres. Cette connaissance alternative pourrait, à la longue, influer sur l'accueil réservé par les Clients-consommateurs aux produits fournis par les Services de renseignement publics et par conséquent, porter atteinte à l'objectif premier desdits Services : l'aide à la décision, dans le cadre d'une communauté du renseignement.

CONCLUSIONS

Nous avons posé la question de la relation entre les décideurs politiques et les services de renseignement, par le biais de l'analyse. Nous avons montré que les relations entre ces deux acteurs génèrent des cas de conscience, des problèmes. Plusieurs dilemmes ont été identifiés. L'hypothèse que ceux-ci pouvaient être résolus par la (ré-)instauration d'un climat de confiance semble se confirmer, même si certains d'entre nous, dans le monde du renseignement considère cela comme une utopie. Des recherches pourraient être poursuivies à l'avenir, en Belgique, sur la promotion de la notion de communauté du renseignement qui doit servir à insuffler la confiance dans la relation producteur/consommateur, mais en

évitant le piège de la politisation, qui doit servir à répondre à cette exigence de dialogue basée sur la compréhension mutuelle, la conscience de la suffisance des moyens, des possibilités des acteurs pour arriver aux fins qui sont prescrites, dans le respect des lois et d'un cadre moral et éthique.

Nous pourrions déjà la définir non comme une simple force, mais plutôt comme une communauté, une communion d'acteurs dans un ensemble défini (communauté internationale ou OTAN ou UE ou Belgique ou forces armées belges, ...), mus « *[...] tant par la différenciation fonctionnelle que par la solidarité organique nécessaire au bon fonctionnement de cette koinonia* »[36]. Et elle ne devrait pas se limiter justement pas à une articulation entre les services de renseignement et le pouvoir exécutif, le pouvoir législatif et les ministres de tutelle. Il s'agit, dans ce cas, plutôt d'un « *dispositif de renseignement* » comme défini par Sébastien Laurent[37], qui relève plutôt d'une architecture politique et administrative.

C'est à cette condition que les services de renseignement et les politiques construiront un esprit de confiance mutuelle, pour gagner la confiance des citoyens, dont les Anglo-saxons estiment qu'ils sont les « *ultimes clients* » des services.

BIBLIOGRAPHIE

Livres

– Barger G, Deborah, *Toward a Revolution in Intelligence Affairs,* Rand Corporation 2005

– Baud Jacques, *Encyclopédie du renseignement et des Services secrets,* Lavauzelle, 1998

– Ben Israël, Isaac, *la philosophie du renseignement,* Editions de l'éclat, 2004

– Beresniak Daniel, *Secrets, pourquoi on parle, pourquoi on se tait,* Editions Grancher, 2004

– Caprini, M., "Controlling and overseeing intelligence services in democratic states", in H. Born and M. Caprini, *Democratic control of intelligence services,* Ashgate, 2007

– Chomeau John B. et Rudolph Anne, « Intelligence Collection and Analysis, dilemma and decisions », cité dans Goldman Jan, *Ethics of Spying,* The scarecrow Press, Inc. Lanham, Maryland , Toronto ,Oxford, 2006

– Clark, Robert M, *Intelligence Analysis, a target centric approach?* Editions CQ Press Washington, 2006

– Forcade, Olivier et Laurent, Sébastien, *Secrets d'Etat : pouvoirs et renseignement dans le monde contemporain,* Editions Armand Colin, Paris, 2005

– Johnson, Rob, *analytic culture in the US Intelligence Community – an ethnographic studie,* Center for the study of Intelligence (CIA), Washington, 2005

36. Senellart, M., *op. cit.*, p. 86.
37. Laurent, S., *Politiques du renseignement,* Presses universitaires de Bordeaux, Pessac, 2009, p 300.

– Laurent, Sébastien, *Politiques du renseignement*, Presses universitaires de Bordeaux, Pessac, 2009,

– Moore, David T, *Critical Thinking Analysis*, Joint Military Intelligence College, Washington DC, 2006

– Peeters, Dirk et Segers, Joris, *Services de renseignement et extrémisme*, in Marc COOLS *et al.*, sous la dir. De, *La Sûreté. Essais sur les 175 ans de la Sûreté de l'État*, Bruxelles, Politeia, 2005

– Sheldon, Rose Mary, *Renseignement et espionnage dans la Rome antique*, Editions Les Belles Lettres, 2009

– Senellaert, Michel, *Les arts de gouverner. Du régime médiéval au concept de gouvernement*, Editions du Seuil, 1995

– Weber, Max, *Le savant et le politique*, édition électronique réalisée à partir du livre de Max Weber (1919), Paris : Union Générale d'Éditions, 1963, 186 pages. Collection : Le Monde en 10-18.

Articles

– Central Intelligence Agency, *A consumer's guide to intelligence*, Washington, DC – CIA, 1994

– Denece, Eric et Arboit, Gérald, *Les études sur le renseignement en France*, Centre français de recherches sur le renseignement, rapport de recherche n° 9, novembre 2009

– Quesnot, Christian (Général), *Perception, utilité et usage de la fonction connaissance et anticipation par le président de la République, chef des Armées*, les Cahiers de Mars, n°198, décembre 2008

Ouvrages académiques

– De Valk, Guillaume Gustav, *Dutch Intelligence – Towards a qualitative framework for Analysis*, Rijksuniversiteit Groningen, 2005

– Magherman Mathieu, *La Grande Muette : Why the Sûreté de l'Etat has been lagging behind in openness* , King's College, London, 2007.

Documents officiels

– *Rapport d'activités 2001* du Comité Permanent de Contrôle des Services de renseignement et de Sécurité (Belgique)

– *Rapport d'activités 2006* du Comité Permanent de Contrôle des Services de renseignement et de Sécurité (Belgique)

– Department of Homeland Security, Office of Intelligence and Analysis, *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment.*, April 7, 2009. (USA)

– Department of Homeland Security, *Leftwing extremists Likely to Increase Use of Cyber Attacks over the Coming Decade.*, January 6, 2009 (USA)

Documents parlementaires belges

– Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (Belgique)

– Loi Organique du 30 Nov 1998 des services de renseignement et de Sécurité (Belgique)

Documents parlementaires étrangers

– Statement of Dennis Blair before the Senate Committee on Intelligence, United States Senate Janunary 22, 2009 (USA)

– United States Senate, Select Committee On Intelligence, "Report On the U.S. Intelligence

– Community's Prewar Intelligence Assessment On Iraq", July 7, 2004., (USA)

– U.K. House of Commons, "Review of Intelligence on Weapons of Mass Destruction.

– Report of a Committee of Privy Counsellors, July 14th, 2004., (UK)

Medias

The Guardian, "We got it wrong on Iraq WMD, intelligence chiefs finally admit.", April 8th, 2005.

– De Standaard, "BIM, een continue bedreiging voor de rechtsstaat.", 1er juillet 2009.

– De Morgen, "De nieuwe BIM-wet, met de B van Bedreigend.", 8 juillet 2009.

– Le Soir, 20 mai 2009

Internet

– http://tempsreel.nouvelobs.com/depeches/politique/20090607.FAP6675/secret_defense_lundi_et_mardi_a_lassemblee.htm

– WorldNetDaily, "Homeland Security on guard for 'right-wing extremists'", April 16, 2009.

– WorldNetDaily, "State drops warnings over 'militia' members.", April 16, 2009.