

UN SERVICE DE RENSEIGNEMENT PEUT-IL OU DOIT-IL COMPTER SUR VOTRE COLLABORATION?

La loi du 30 novembre 1998 organique des services de renseignement et de sécurité¹ donne aux services de renseignement civils mais aussi militaires une série (plutôt limitée) de possibilités légales pour accomplir leurs missions. Le présent article traite de l'une de ces compétences: dans quelle mesure la Sûreté de l'Etat et le Service général du Renseignement et de la Sécurité des Forces armées (SGRS) peuvent-ils demander ou recevoir spontanément des données de particuliers ou de personnes travaillant dans les services publics?

QUESTIONS?

La réponse à cette question n'est pas évidente du tout. Selon la situation, il faudra prendre toute une série de règles en considération. Il faut en effet distinguer les paramètres suivants:

- Chez qui les informations sont-elles demandées? S'agit-il d'un acteur public ou privé? La personne est-elle tenue au secret professionnel ou à un autre devoir de discrétion?
- Quelles sont les données demandées? S'agit-il de données à caractère personnel ou s'agit-il d'informations qui ne peuvent être rapportées à une personne identifiée ou identifiable?
- Comment et où sont conservées ces données? Ont-elles été stockées dans un ordinateur ou figurent-elles dans un fichier?
- Dans quel cadre les informations sont-elles demandées exactement? S'agit-il par exemple d'une enquête de sécurité? Ou la demande a-t-elle une autre enquête pour cadre?
- Qui est le destinataire des informations? Est-ce le service de renseignement militaire ou civil? Dans quelques cas très spécifiques, cette distinction sera également importante lors de la réponse à apporter à la question de savoir si vous pouvez ou devez

communiquer certaines informations à un membre d'un service de renseignement.

La problématique sera abordée pas à pas. En première instance, on fait la distinction entre les acteurs privés et publics. Ensuite, on examine deux importants régimes légaux qui impliquent normalement une limitation voire une interdiction de communiquer des données. Il y a d'une part la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (LVP)². D'autre part, il y a les nombreuses dispositions créant un secret professionnel ou un devoir de discrétion. Nous examinerons ensuite à quelles conditions la communication de données est autorisée pour enfin déterminer quand il est obligatoire.

Au fil du texte, nous reprendrons régulièrement plusieurs exemples. Il est évident qu'il s'agit d'exemples hypothétiques qui ont pour seul objectif d'accroître la lisibilité du texte.

ACTEUR PRIVÉ VERSUS ACTEUR PUBLIC

Il faut faire une première grande distinction entre le secteur public et le secteur privé. Cette distinction est créée par la loi sur les services de renseignement elle-même.

NOTES

1 M.B. 18 décembre 1998.

2 M.B. 18 mars 1993.

L'article 14 règle la situation du secteur public, l'article 16 celle du secteur privé.

Article 14

Dans le respect de la loi, sur la base des accords éventuellement conclus ainsi que des modalités déterminées par leurs autorités compétentes, les autorités judiciaires, les fonctionnaires et les agents des services publics peuvent communiquer d'initiative au service de renseignement et de sécurité concerné les informations utiles à l'exécution de ses missions.

A la requête d'un service de renseignement et de sécurité, les autorités judiciaires, les fonctionnaires et les agents des services publics peuvent, dans le respect de la loi, sur la base des accords éventuellement conclus ainsi que des modalités déterminées par leurs autorités compétentes, communiquer au service de renseignement et de sécurité concerné les informations utiles à l'exécution de ses missions.

Lorsque les autorités judiciaires, les fonctionnaires et agents des services publics estiment ne pas pouvoir communiquer aux services de renseignement et de sécurité les informations qu'ils demandent, ils en communiquent les raisons par écrit endéans le mois de la demande.

Article 16

Conformément à l'article 3, § 3, 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, les services de renseignement et de sécurité peuvent solliciter les informations nécessaires à l'exercice de leurs missions, y compris des données à caractère personnel, auprès de toute personne ou organisme relevant du secteur privé.

La notion de 'service public' de

l'article 14 doit être comprise dans le sens le plus large possible et recouvre notamment, en plus de toutes les institutions des autorités fédérales, communautaires, régionales, provinciales et communales, tous les organismes d'utilité publique³. L'article 14, et non l'article 16, sera applicable à la communication d'informations par exemple par La Poste, BIAC ou Belgacom.

On entend par autorités judiciaires tant les magistrats du parquet que les juges d'instruction⁴. Mais les articles 14 et 16 ne sont pas les seuls qui régissent de manière générale de communication d'informations aux services de renseignement. L'article 18 de la loi du 30 novembre 1998 est également une de ces dispositions.

Article 18

Dans l'exercice de leurs missions, les services de renseignement et de sécurité peuvent avoir recours à des sources humaines. Dans ce cas, ces services doivent veiller à la sécurité des données qui concernent les sources humaines et des informations qu'elles communiquent.

Ces 'sources humaines' (ou informateurs⁵) ne peuvent être autres que des acteurs publics ou privés. Quelle plus-value a alors cette disposition par rapport aux articles 14 et 16? Les sources humaines de l'article 18 font-elles l'objet de moins de limitations? Cela peut difficilement avoir été l'intention. On ne peut en effet pas accepter que des informations qui ne peuvent être communiquées, par exemple en raison d'un secret professionnel (voir plus loin), aboutissent quand même dans un service de renseignement sous l'appellation 'informations provenant d'un informateur'?

Il est quand même exclu qu'un fonctionnaire ne respecte pas les 'accords conclus ainsi que les modalités déterminées par (son) autorité compétente' (voir ci-après) et communique plus de données que convenu en tant qu'informateur? L'article 18 avait clairement une autre finalité. On voulait rendre légalement possible de garder secrète la source des informations⁶.

INTERDICTION DE COMMUNIQUER DES INFORMATIONS

Tant la LVP que nombre de réglementations imposant un secret professionnel ou un devoir de discrétion interdisent en principe que certaines données soient communiquées à des tiers. Le service de renseignement reste-t-il alors nécessairement privé de ces informations?

Informations, données à caractère personnel traitées et non traitées

Les données communiquées par des particuliers peuvent consister en des données à caractère personnel⁷ ou en des données qui ne concernent pas une personne identifiée ou identifiable⁸. Dans la suite du texte, nous désignerons cette dernière catégorie par le terme 'informations'.

S'il s'agit de données à caractère personnel, il faut se demander si ces données sont traitées de manière automatisée ou si elles figurent dans un fichier au sens de la LVP et constituent donc des 'données à caractère personnel traitées'. Si ce n'est pas le cas, la LVP n'est pas applicable – tout comme pour les 'informations' – et tant l'acteur public que l'acteur privé peuvent sans problème communiquer ces données à un membre d'un service

3 Voir par ex. Doc. Parl., Chambre 1995-96, 638/1, p. 14.

4 Doc. Parl., Sénat, 1997-98, 758/9, pp. 2-3.

5 Doc. Parl., Sénat, 1997-98, 758/3, p. 11.

6 Doc. Parl., Sénat, 1997-98, 758/3, p. 11.

7 Par exemple l'identité et l'adresse d'un titulaire de boîte postale à La Poste ou les données relatives aux passagers dont dispose une compagnie aérienne.

8 Par exemple les plans des lieux qui doivent être observés.

de renseignement sur la base de cette réglementation⁹. Mais que se passe-t-il si on demande à un hôtelier de sortir de son ordinateur la liste des numéros de téléphone composés depuis une chambre déterminée?

Données à caractère personnel traitées par des particuliers

La LVP pose des exigences strictes à tout traitement de données à caractère personnel. Le traitement qui est important ici est la 'communication de données à caractère personnel à un tiers'. Cet acte ne peut être posé que s'il est à la fois admissible et légitime¹⁰.

L'admissibilité de ce traitement ne constitue pas de problème. L'article 5, e), stipule que: "Le traitement de données à caractère personnel ne peut être effectué que (...) (...) lorsqu'il est nécessaire 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 ou le tiers auquel les données sont communiquées". La communication de données à caractère personnel à des services de renseignement est donc admissible si elle est nécessaire à l'exécution de leurs missions légales¹¹.

La légitimité de la communication d'informations est plus délicate. L'article 4, § 1er, 2°, stipule ce qui suit: "Les données à caractère personnel doivent être (...) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées (lisez: communiquées) ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables." En d'autres termes, la personne qui enregistre des données à caractère personnel doit préalablement décrire dans quelle finalité elle le fait. Si elle le fait dans la finalité A, elle ne peut utiliser ces données pour la finalité B, à moins que la finalité B soit très proche de la finalité A. Elle ne peut pas non plus communiquer ces données à un tiers qui veut les utiliser pour la finalité C, à moins une fois encore que les finalités A et C soient 'conciliables'¹².

La finalité de l'enregistrement des numéros de téléphone par l'hôtelier consiste à pouvoir facturer les services fournis au client. Communiquer cette liste de numéros de téléphone à un membre d'un service de renseignement pour servir par exemple la sûreté de l'Etat n'est bien entendu pas conciliable avec cette finalité.

Conclusion: sous réserve d'un éventuel recours à la figure de l'état de nécessité, les données ne peuvent être communiquées^{13 14}.

On ne peut bien entendu pas exclure qu'un acteur privé (ou public) ait tenu compte, lors du libellé de la finalité de son fichier, de la possibilité que des services de police et de renseignement puissent être intéressés par ces données et que l'une de ses finalités formulées soit conciliable avec la communication d'informations à un service de renseignement¹⁵. Dans ce cas, les données peuvent bien entendu être communiquées. Mais, selon toute vraisemblance, cela ne vaut que pour une minorité de fichiers.

Il est donc important d'examiner si l'on a voulu créer, par l'article 16 de la loi du 30 novembre 1998, une exception générale à l'interdiction de la LVP de communiquer des données à caractère personnel traitées à un tiers (en l'espèce un service de renseignement) si c'est inconciliable avec la finalité du traitement¹⁶. Nous pensons que l'on ne peut accorder une telle portée à l'article 16. Nous nous basons pour cela sur une analyse des travaux parlementaires.

Ce n'est qu'au Sénat qu'il a été proposé d'insérer par voie d'amende-

9 Il faut bien entendu examiner si d'autres règles (comme par ex. le secret professionnel) n'entraînent pas une interdiction de la communication des informations.

10 De Bot, D., "Verwerking van persoonsgegevens", in *Recht en praktijk*, Antwerpen, Kluwer, 2001, p. 111 et suiv.

11 Les travaux parlementaires relatifs à la modification de la LVP font explicitement référence aux articles 7 et 9 de la loi organique des services de renseignement comme 'mission d'intérêt public' au sens de l'article 5, e) de la LVP (Doc. Parl., Chambre, 1997-98, 1566/1, p. 32).

12 Voir pour un exemple dans lequel la police est parvenue à utiliser les données à caractère personnel enregistrées par une banque pour sa finalité non-identique mais conciliable: Gent, 28 mars 2002, *Tijdschrift voor Strafrecht*, 2002, p. 326 et De Hert, P., "De waarde van de Wet van 8 december 1992 bij de bewijsbeoordeling in strafzaken", *Tijdschrift voor Strafrecht*, 2002, p. 310.

13 La police et la justice sont d'ailleurs confrontées à la même limitation. Cela peut sembler très étonnant mais c'est la conséquence du fait que notre LVP, à la différence d'une série d'exemples étrangers, ne stipule pas de manière générale que l'appareil judiciaire peut demander à certaines conditions des données pour une finalité

judiciaire, quelle que soit la finalité initiale du premier traitement (De Hert, P., l.c., p. 310).

14 Un traitement ultérieur pour une autre finalité n'est toutefois pas interdit (De Bot, D., o.c., 120-121). Une modification de la finalité est permise moyennant le respect de toutes les exigences de légitimité de la loi. En d'autres termes, la loi n'empêche pas qu'un hôtelier décide à un moment donné de communiquer les données relatives au téléphone pour une autre finalité, tant que cette finalité est décrite clairement, est portée à la connaissance de l'intéressé et qu'une nouvelle déclaration relative à ce traitement est faite. Il n'est donc pas requis que les données à caractère personnel soient une nouvelle fois recueillies. L'une dans l'autre, ces possibilités semblent plutôt théoriques ici.

15 Une telle finalité pourrait être libellée comme suit: "Enregistrement des données a également lieu dans le but de communiquer ces données aux autorités judiciaires et administratives qui le demandent et qui veulent utiliser ces données pour préserver la sûreté de l'Etat ou dans le cadre de la lutte contre la criminalité."

16 L'article 13 de la directive européenne 95/46/CE du 24 octobre 1995 permet au législateur national de créer une telle exception dans l'intérêt de la sûreté de l'Etat.

ment un article qui traite du recueil d'informations auprès de particuliers¹⁷. L'article de loi ne fait toutefois pas référence à la LVP à ce moment. La justification du projet de texte est intéressante: "Le présent texte de l'article 10quinquies vise donc à confirmer à l'égard du secteur privé la légitimité [nous soulignons] d'une éventuelle sollicitation de la part des services de renseignement et de sécurité, notamment si celle-ci concerne la communication de données à caractère personnel tombant sous le champ d'application 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"¹⁸.

La demande par le service de renseignement peut être légitime, sans que pour autant la communication par le particulier le soit. Ce n'est en effet pas parce qu'un service de renseignement peut recueillir certaines données qu'un particulier peut lui communiquer ces données. Le contrôle de l'admissibilité et de la légitimité d'une communication d'informations doit en d'autres termes avoir lieu deux fois: une fois dans le chef de celui qui veut communiquer les informations et une fois dans le chef de celui qui veut obtenir les informations.

Le fait qu'on n'a pas voulu adapter l'article 16 à la situation existante ressort d'ailleurs de la suite des discussions. Une référence à l'article 3, § 3 de la LVP a été ajoutée à l'article 10quinquies par amendement. La justification est la suivante: "La loi relative à la protection de la vie privée détermine déjà quels renseignements les services de renseignements et de sécurité

peuvent recueillir dans le secteur privé. L'article 10quinquies est donc, en fait, superflu [nous soulignons]. Si l'on veut malgré tout le maintenir pour des raisons de clarté, il faut renvoyer clairement aux dispositions en vigueur prévues par la loi relative à la protection de la vie privée"¹⁹.

Une fois revenu à la Chambre, l'article 16 a été repris sans modification et le rapporteur a ajouté: "Etant donné que les informations détenues par le secteur public ne sont pas suffisantes, les services de renseignement doivent être en mesure de solliciter des informations ou de collecter des données à caractère personnel auprès du secteur privé. Dans un souci de concordance entre les deux lois, il s'imposait d'invoquer l'article 3, § 3, 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 afin de justifier la légalité d'une éventuelle demande [nous soulignons] émanant des services de renseignement. Telle est la portée de l'article 16"²⁰.

Même si ce passage aurait pu être plus clair, la conclusion reste pour nous que la loi sur les services de renseignement n'octroie pas d'autorisation générale aux acteurs privés pour communiquer des 'données à caractère personnel traitées' à des services de renseignement.

Le secret professionnel de particuliers

Aucun problème ne se pose sur ce plan: l'article 16 de la loi sur les services de renseignement ne peut jamais être lu comme s'il contenait

une autorisation de communiquer spontanément ou sur demande des données qui sont couvertes par un secret professionnel ou un devoir de discrétion à un service de renseignement.

Nous renvoyons uniquement au cas spécifique du détective. Dans cette section nous retenons qu'il est normalement tenu à un devoir de discrétion: les informations qu'il recueille ou obtient à l'occasion de la mission ne peuvent être communiquées qu'au client²¹. La conclusion (provisoire) est donc que ni la Sûreté de l'Etat ni le SGRS ne peuvent obtenir communication de ces données.

Données à caractère personnel traitées par des autorités publiques et secret professionnel

Pour approcher au plus près la portée exacte de l'article 14 de la loi sur les services de renseignements, les questions sur l'application de la LVP et des règles relatives au secret professionnel sont traitées simultanément.

A la différence de l'article 16, l'article 14 ne fait pas référence à la LVP. Lors des travaux parlementaires, aucun mot n'a été dit non plus de cette loi. La règle applicable au secteur public a subi une autre 'approche'. Elle ne vise par le membre du service de renseignement mais le fonctionnaire public; elle prévoit que ce dernier peut communiquer des renseignements 'dans le respect de la loi'. Mais quelle loi ou quelles lois ce fonctionnaire doit-il respecter?

Une première série de lois est

17 Doc. Parl., Sénat, 1997-98, 758/3, 8.

18 Doc. Parl., Sénat, 1997-98, 758/3, 11.

19 Doc. Parl., Sénat, 1997-89, 758/5. On peut écrire beaucoup de choses sur ce passage et sur la rédaction finale de l'article 16. Tout d'abord, le renvoi à l'article 3, § 3 (maintenant § 4) LVP n'est pas à sa place. Cet article stipule justement quelles exigences de la LVP ne sont pas applicables aux services de renseignement. Ensuite,

l'application littérale de l'article 16 élargit le champ d'application de la LVP aux services de renseignement. Il stipule en effet que les exigences de cette loi doivent être respectées, même si la Sûreté de l'Etat recueille des 'informations' qui ne sont pas des données à caractère personnel. Cela n'est jamais entré dans les intentions.

20 Doc. Parl., Chambre, 1995-96, 638/20, 4.

21 Article 10, alinéa 1er de la loi du 19 juillet 1991 organisant la profes-

constituée par les règles instaurant un secret professionnel ou un devoir de discrétion. Dans une telle lecture, l'article 14 n'aurait cependant pas beaucoup de sens. Toutes les autorités et fonctionnaires judiciaires ainsi que les agents des services publics sont en effet soumis à l'un ou l'autre secret²².

La note politique du gouvernement qui était à la base du projet de loi sur les services de renseignement prévoyait apparemment un système dans lequel le secret professionnel pouvait être mis de côté si des personnes travaillant dans des services publics voulaient communiquer des données aux services de renseignement²³. Toutefois, un passage de l'Exposé des motifs se tient clairement au secret professionnel: "Le recueil d'informations (...) ne peut porter atteinte à l'article 458 du Code pénal, qui protège le secret professionnel des personnes qui sont contactées à cette occasion"²⁴. Tout indique toutefois que l'on a oublié de supprimer ce passage du texte tel qu'il a été soumis au Conseil d'Etat. On lisait en effet dans le texte de l'article 14 (alors encore article 12) que les services de renseignement peuvent recueillir des données à caractère personnel sans recourir à la contrainte et "sans préjudice de l'article 458 du Code pénal"²⁵. La référence à l'article 458 C.P. a disparu sans autre commentaire du texte

soumis au Parlement. L'adaptation nécessaire de l'exposé des motifs a apparemment été oubliée. Mais il y a encore d'autres arguments qui indiquent clairement que le secret professionnel ne s'applique pas si l'on veut communiquer des données à des membres de services de renseignement.

L'article 14 a été inséré dans le projet pour résoudre le problème que chaque service public avait ses propres règles en ce qui concerne la communication de données à la Sûreté de l'Etat. "De plus, des lois interdisent expressément la révélation de certaines informations"²⁶. C'est pourquoi "la loi adopte une formule qui permet aux membres des services de renseignement et de sécurité d'obtenir les informations nécessaires tout en laissant un pouvoir d'appréciation, à cet égard, au service sollicité. Elle introduit une autorisation légale de révéler des informations mais non une obligation [nous soulignons]. Il appartient à chaque service de déterminer, en fonction des circonstances de chaque demande, le type d'informations communicables et la voie par laquelle elles peuvent l'être." Et plus loin: "(...) ce paragraphe ouvre un droit de donner l'information sollicitée par les services de renseignement et de sécurité"²⁷.

De plus, il a été explicitement cité comme exemple que des données

qui font l'objet d'une instruction judiciaire peuvent être échangées²⁸. Ainsi, un magistrat du parquet ou même un juge d'instruction peut communiquer à la Sûreté de l'Etat des informations sur une instruction en cours²⁹.

Il ne fait donc aucun doute que les magistrats et les fonctionnaires de police qui communiquent des données ne violent pas le secret professionnel ou le secret de l'instruction. Mais le législateur ne voulait manifestement pas limiter 'l'autorisation' à ces deux acteurs publics. L'article 14 crée en principe une exception légale pour toute forme de secret professionnel, de sorte que l'obligation de silence de fonctionnaires, le secret des lettres pour les personnes travaillant à La Poste³⁰ ou le secret professionnel des membres de la Cellule de traitement des informations financières³¹ ne s'applique pas dans leurs relations avec un membre d'un service de renseignement. En principe du moins, parce qu'il existe une série de règles postérieures à l'entrée en vigueur de la loi sur les services de renseignements qui prévoient un régime très strict de secret et qui négligent (probablement involontairement) la position particulière des services de renseignement. Nous ne renvoyons qu'au secret professionnel tel qu'instauré par l'article 74 de la loi du 2 août 2002 relative à la surveillance du

sion de détective privé (M.B., 2 octobre 1991; err. 11 février 1993).

22 A ce moment, une exception vaudrait uniquement pour les fonctionnaires de police. L'ancien article 39 (maintenant article 44/1) de la loi du 5 août 1992 sur la fonction de police permettait en effet déjà une communication de données à des membres de services de renseignement.

23 On peut le déduire de l'avis rendu sur le projet de loi par le Comité permanent de contrôle des services de renseignements (voir Rapport d'activités 1995, Comité permanent de contrôle des services de renseignements, p. 96, www.comiteri.be).

24 Doc. Parl., Chambre, 1995-96, 638/1, 13.

25 Doc. Parl., Chambre, 1995-96, 638/1, 23.

26 Doc. Parl., Chambre, 1995-96, 638/1, 6.

27 Doc. Parl., Chambre, 1995-96, 638/1, 13. Voir aussi Doc. Parl., Chambre, 1995-96, 638/14, 19-20 et Doc. Parl., Sénat, 1997-98, 758/10, 20.

28 Doc. Parl., Sénat, 1997-98, 758/9, 2-3. Une grande partie

de l'exemple cité par le gouvernement concerne toutefois le flux d'informations du service de renseignements vers le juge d'instruction.

29 Voir cependant plus loin en ce qui concerne le nouveau régime de l'article 56 C.I.Cr.

30 Article 28 de la loi du 26 décembre 1956 sur le service des postes (M.B. 30 décembre 1956).

31 Article 17 de la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme (M.B. 9 février 1993). Lors d'une récente modification de la loi du 11 janvier 1993, le législateur a erronément considéré que le secret professionnel des membres de la Cellule de traitement des informations financières s'appliquait à l'égard des membres des services de renseignement (Doc. Parl., Chambre, 2003-2004, 383/1, 49-50). Nous commentons ce régime plus loin étant donné qu'il implique une obligation de communication d'informations.

secteur financier et aux services financiers³². Les membres de la Commission bancaire, financière et des assurances "sont tenus au secret professionnel et ne peuvent divulguer à quelque personne ou autorité que ce soit les informations confidentielles dont ils ont eu connaissance en raison de leurs fonctions". Il y a toutefois une exception "dans les cas où la communication de telles informations est prévue ou autorisée par ou en vertu de la présente loi et des lois régissant les missions confiées à la CBFA". Le régime prévu par la loi sur les services de renseignement n'apporte apparemment pas de solution.

Quoi qu'il en soit, à l'époque de la rédaction de la loi sur les services de renseignement, les acteurs publics ne devaient pas tenir compte des règles qui les soumettaient à un secret professionnel. Mais quelle loi devaient-ils alors prendre en considération? La loi relative au traitement de données à caractère personnel?

Il ressort en tout cas des travaux parlementaires qu'on a accordé beaucoup d'attention au fait que la loi soit prise en considération, comme en témoigne la justification d'un amendement où les mots "dans le respect de la loi" ont été placés au tout début de l'article 14: "Le texte proposé met trop l'accent sur le fait que les fonctionnaires, les magistrats et les agents des services publics, agissant d'initiative ou à la requête d'un service de renseignements et de sécurité, communiquent des informations aux services concernés. Le fait que cette communication est soumise à la loi [nous soulignons] et aux modalités déterminées par leurs autorités compétentes est secon-

daire. Il nous paraît nécessaire de faire apparaître plus clairement que la communication d'informations par les fonctionnaires, les magistrats et les agents des services publics est conditionnée par le respect des dispositions légales [nous soulignons], des modalités déterminées par les autorités compétentes et des accords conclus entre ces autorités et les services de renseignements et de sécurité"³³. Mais cela ne nous fait pourtant pas avancer d'un pas vers la solution.

Si cette fameuse loi est (notamment) la LVP, il est pour le moins étrange qu'on ne la mentionne pas en tant que telle. Ni dans le texte de loi même, ni dans les travaux parlementaires on n'en dit mot, alors que cette loi a été citée à tort et à travers en relation avec le secteur privé. Il y a encore deux arguments qui indiquent que l'article 14 doit être considéré comme une exception à l'exigence que la finalité du traitement initial doit être conciliable avec le traitement des services de renseignement³⁴.

L'article 14 est conçu différemment de l'article 16 qui laisse aux services de renseignement la possibilité de solliciter une personne privée, sans accorder d'autorisation légale à ce particulier de laisser de côté des règles imposant une obligation de secret. L'article 14 s'adresse au détenteur des informations. Et ne peut-on lire dans les travaux parlementaires que "(...) ce paragraphe ouvre un droit de donner l'information sollicitée par les services de renseignement et de sécurité"³⁵. Enfin, l'intention du législateur était de supprimer les obstacles légaux à la communication d'informations. En s'en tenant à l'exigence de la finalité, on n'y arrive cependant pas.

Nous pouvons donc dire moyennant quelques réserves que la LVP n'est pas applicable à la communication d'informations par des autorités publiques³⁶. Nous continuons à nous demander quelle autre loi doit être respectée de manière aussi nécessaire.

AUTORISATION DE COMMUNIQUER DES INFORMATIONS

Le secteur privé peut donc communiquer des informations et des données à caractère personnel non traitées à la Sûreté de l'Etat/SGR à moins que l'intéressé soit tenu à l'une ou l'autre forme de discrétion ou secret professionnel. Les données à caractère personnel auxquelles s'applique la LVP peuvent être communiquées si c'est conciliable avec la finalité initiale et si aucun secret professionnel ou devoir de discrétion n'est en jeu.

Le secteur public a plus de possibilités. Il est certain que le secret professionnel ne peut constituer un frein à la communication d'informations: des données couvertes par un secret professionnel peuvent être communiquées. Mais, à notre avis des autorités publiques peuvent également communiquer à la Sûreté de l'Etat/SGR des données à caractère personnel automatisées ou figurant dans des fichiers, même si la finalité de leur traitement de données ne le permet pas.

Dans tous ces cas, il s'agit dans le chef de l'acteur public ou privé d'une *autorisation* et non d'une *obligation*. Les autorités publiques ne peuvent toutefois pas refuser purement et simplement de communiquer des informations. Si elles estiment que les renseigne-

32 M.B., 4 septembre 2002.

33 Doc. Parl., Sénat, 1997-89, 75815, 4.

34 L'article 13 de la directive européenne 95/46/CE du 24 octobre 1995 permet une telle exception.

35 Doc. Parl., Chambre, 1995-96, 63811, 13.

36 A la différence de l'hôtelier, Belgacom pourrait donc communiquer aux services de renseignement des données à caractère personnel conservées en vue de la facturation.

ments demandés par les services de renseignement ne peuvent être communiqués, elles en communiquent la raison par écrit dans le mois suivant la demande. Il ne faut pas attendre trop de choses de cette motivation. Le ministre de la Justice a laissé entendre lors des discussions qu'il ne fallait pas que la motivation soit trop précise. Il peut suffire que le magistrat dise qu'une information est en cours, dont il ne peut pas révéler la teneur³⁷.

L'autorisation de communiquer des données ne disparaît pas si aucun accord n'est conclu avec l'autorité concernée. L'article 14 parle d'accords 'éventuellement' conclus. Sur la base de cette règle, une série d'accords (confidentiels) a déjà été conclue avec différentes autorités. Un de ces accords figure dans la COL 13/99 du Collège des procureurs généraux traitant de la coopération entre les autorités judiciaires et les services de renseignement³⁸ ³⁹. Un autre régime plus global date du 16 février 2000. Il s'agit d'une directive du Comité ministériel du renseignement et de la sécurité en matière de communication de renseignements et de coopération entre les services de renseignement et de sécurité et les autorités et services administratifs. Cette directive recommande aux services de renseignement et aux services administratifs de se transmettre mutuellement dans

les meilleurs délais, d'initiative ou sur demande, tous documents et renseignements nécessaires à l'accomplissement de leurs missions légales respectives, dans le respect du principe de finalité⁴⁰.

Si la LVP est applicable à la communication de données, il faut également tenir compte de la notion de 'destinataire' de l'article 1er, § 7, et des conséquences que l'article 9 y couple. L'article 1er définit le 'destinataire' comme "la personne physique, la personne morale, l'association de fait ou l'administration publique qui reçoit communication de données, qu'il s'agisse ou non d'un tiers; les instances administratives ou judiciaires qui sont susceptibles de recevoir communication de données dans le cadre d'une enquête particulière ne sont toutefois pas considérées comme des destinataires"⁴¹.

L'article 9, § 1er, oblige le responsable du traitement à fournir au plus tard au moment où les données sont obtenues les informations relatives aux 'destinataires ou (aux) catégories de destinataires des données' à l'intéressé. Le secteur privé devra donc, dans la définition de la finalité, faire immédiatement référence aux catégories de services qui peuvent recevoir les données à caractère personnel⁴².

L'exigence de l'article 9 ne joue

pas à l'égard de l'autorité publique étant donné que nous considérons que l'article 14 de la loi sur les services de renseignement constitue une exception à la LVP. La loi fait en effet en sorte que l'intéressé sait que le service de renseignement peut être le destinataire de ses données.

Soulignons enfin l'article 36bis de la LVP inséré par l'article 10 de la loi du 26 février 2003⁴³. Si la communication de données à caractère personnel par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, a lieu par voie électronique, il faut obtenir l'autorisation de principe du comité sectoriel pour l'autorité fédérale près la Commission pour la protection de la vie privée⁴⁴.

OBLIGATION DE COMMUNICATION DES INFORMATIONS

Outre l'interdiction et l'autorisation, reste l'obligation éventuelle de communiquer des données. Il y a en effet plusieurs dispositions qui obligent les autorités (et dans deux cas les particuliers) à communiquer d'initiative des données ou à répondre aux demandes de l'un des services de renseignement. Deux dispositions légales vont encore plus loin: elles permettent aux membres de services de renseignement de demander eux-mêmes des

37 Doc. Parl., Sénat, 1997-89, 758/10, 125.

38 Voir le Rapport d'activités 2001 du Comité permanent de contrôle des services de renseignements, p. 83, à consulter sur www.comiteri.be.

39 Il existe également un protocole avec le parquet fédéral et on planche sur un protocole avec la police fédérale (Interpellations n° 337 et 338 en Commission de la Justice de la Chambre le 24 mai 2004).

40 Voir le Rapport d'activités 2003 du Comité permanent de contrôle des services de renseignements, p. 123 et 188 et Schuermans, F., "Bronnenbescherming en inlichtingendiensten", in *Informatiehuishouding binnen de politiediensten*, Tempels, L. (éd.), Bruxelles, Politeia, 2003, 69.

41 La Sûreté de l'Etat et le SGRS correspondent à cette notion s'ils reçoivent des données à caractère personnel. A notre avis,

ils ne sont pas visés par l'exception formulée par l'article 1er, § 7. Dans le cadre d'une procédure d'enquête particulière, la doctrine fait en effet référence à des enquêtes spécifiques, uniques ou à des enquêtes "par ex. dans le cadre d'une inspection fiscale ou sociale particulière, d'une instruction judiciaire, etc." (De Bot, D., o.c., 57-58). Dans ces cas, les autorités citées disposent d'un mandat spécifique. Ce n'est en principe pas le cas pour la Sûreté de l'Etat/SGRS. On peut à notre avis tenir un raisonnement analogue uniquement lorsqu'elle effectue une enquête de sécurité (zie 4.4.) ou dans le cas d'un mandat dans le cadre de la loi sur les détectives - zie 4.7.). (ndt n°??)

42 Voir note 17.

43 M.B. 26 juin 2003.

44 Ce comité n'est toutefois pas encore opérationnel.

données figurant dans les fichiers. Ces situations seront les premières commentées.

Données du registre de la population et des étrangers, du registre d'attente des étrangers et du Registre national

Les modalités de communication des informations contenues dans les registres de la population et des étrangers, devraient être fixées par arrêté royal délibéré en Conseil des Ministres⁴⁵. Pour le SGR, cela s'est réalisée par l'A.R. du 8 juillet 1999⁴⁶; pour le Sûreté de l'Etat par l'A.R. du 6 octobre 2000⁴⁷. Les autorités communales sont tenues à répondre immédiatement et de façon précise à toute requête d'un agent d'un de ces services lorsqu'elle est conforme aux exigences formelles. La communication concerne toutes les données reprises dans les registres. La Sûreté de l'Etat (et donc pas le SGR) peut également obtenir les mêmes données par l'intermédiaire du Registre nationale⁴⁸. Ce système constitue une espèce de contrôle.

En ce qui concerne les informations de personnes inscrites au registre de la population et des étrangers et qui sont repris dans le Registre national, le chef du SGR et les agents désignés par lui par écrit ont accès aux données mentionnées à l'article 3, 1° à 9° et à l'article 3, deuxième alinéa de la loi du 8 août 1983 organisant un Registre national des personnes physiques⁴⁹. In en va de même pour l'administrateur général, son adjoint et les agents désignés par écrit de la Sûreté de

l'Etat. En outre, les membres de la Sûreté ont accès aux données mentionnées à l'article 3, 1° à 11° et à l'article 3, deuxième alinéa, du Registre national concernant les étrangers aussi sont repris dans le registre d'attente.⁵⁰

Les règles ci-dessus sont valables pour toutes les missions légales de la Sûreté de l'Etat et du SGR. Dans le cadre de leur compétence pour effectuer des enquêtes de sécurité, la loi même donne de manière générale accès aux différents registres (voir plus loin). Dans le cadre de ces enquêtes il n'y a, selon nous, aucune restriction.

Données du Casier judiciaire central

Dans le cadre des missions fixées par la loi, les agents de niveau I des services de renseignement nommément désignés par écrit ont accès aux données à caractère personnel enregistrées dans le Casier judiciaire central. Ils ne peuvent toutefois pas disposer de quatre données⁵¹:

- condamnations ayant fait l'objet d'une mesure d'amnistie;
- décisions annulées par application des articles 416 à 442 ou des articles 443 à 447bis du Code d'instruction criminelle;
- décisions de rétractation rendues par application des articles 10 à 14 de la loi spéciale du 6 janvier 1989 sur la Cour d'arbitrage;
- condamnations et décisions prononcées sur la base d'une disposition légale ayant fait l'objet d'une abrogation, à la condition que l'incrimination pénale du fait soit supprimée.

A notre avis, les membres des services de renseignement peuvent néanmoins demander ces quatre données sur la base de l'article 14 de la loi sur les services de renseignement. Aucune obligation de communiquer les données ne repose toutefois sur l'administration à ce moment.

Documents d'inscription des voyageurs

Dans le cadre de leurs missions, les services de renseignement peuvent se faire présenter les documents d'inscription des voyageurs par les propriétaires, tenanciers ou préposés des établissements hôteliers⁵².

Renseignements dans le cadre d'une enquête de sécurité

Dans le cadre d'une enquête de sécurité, nombre de données dont disposent les services publics sont accessibles aux agents spécialement désignés de la Sûreté de l'Etat et du SGRS sur présentation de leur carte de légitimation⁵³. Il s'agit:

- * des données du casier judiciaire central⁵⁴;
- * des données des registres de la population et des étrangers⁵⁵;
- * des données du Registre national;
- * des données du registre d'attente des étrangers;
- * des données policières accessibles aux fonctionnaires de police lors de l'exécution de contrôles d'identité;
- * de toutes les informations utiles dont disposent les services de police généraux;
- * de toutes les informations utiles relatives à l'identité ou à la solva-

45 Arrêté royal du 10 août 2001 (M.B. 7 septembre 2001).

46 L'article 15 de la loi sur les services de renseignement.

47 M.B. 7 août 1999.

48 M.B. 11 novembre 2000.

49 M.B. 29 mars 2002.

50 M.B. 7 août 1999.

51 M.B. 22 février 1997, comme modifié par l'A.R. du 6 octobre 2000, M.B. 10 novembre 2000

52 Article 17 de la loi sur les services de renseignement.

53 Article 19 de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (M.B. 7 mai 1999).

54 Les quatre données qui ne sont normalement pas accessibles aux services de renseignement nous semblent toutefois accessibles dans le cadre d'une enquête de sécurité.

55 Cette disposition renvoyait également aux casiers judiciaires communaux. Ceux-ci doivent toutefois disparaître suite à la loi du 8 août 1997 relative au casier judiciaire central.

56 Cette énumération a été établie par l'article 30 A.R. 24 mars 2000

bilité de l'intéressé auprès⁵⁶:

- du Ministère des Finances:

- a) le Service central des dépenses fixes;
- b) l'Administration des contributions directes;
- c) l'Administration de la TVA, de l'enregistrement et des domaines;
- d) l'Administration du cadastre;
- e) l'Administration des douanes et accises;

- des autres services publics chargés de la gestion des traitements;

- du registre de commerce;
- du registre de l'artisanat;
- de l'Office des étrangers;

- des services suivants de la Banque nationale de Belgique:

- a) la Centrale des crédits aux particuliers;
- b) la Centrale des crédits aux entreprises;
- c) la Centrale du traitement des papiers commerciaux;
- d) la Centrale des bilans;

- de la Banque-Carrefour de la sécurité sociale.

Dans tous ces cas, le service public n'a donc aucun pouvoir d'appréciation: il devra communiquer les données demandées⁵⁷.

Missions de protection

A la différence du SGR, le service de renseignement civil s'est vu confier une mission opérationnelle: il doit dans certains cas assurer la protection de personnes.

Dans ce cadre, il ne peut y avoir de limitation à l'échange d'informations. L'article 23 de la loi sur les services de renseignement stipule que les autorités judiciaires, les fonctionnaires et les agents

des services publics sont tenus de communiquer au ministre de l'Intérieur toutes les informations utiles en leur possession qui ont trait à la protection de la vie et de l'intégrité physique des personnes à protéger, en se conformant aux modalités déterminées par leurs autorités responsables. A son tour, le ministre de l'Intérieur communique à la Sûreté de l'Etat tous les renseignements nécessaires à l'exécution des missions de protection qui lui sont confiées.

Cellule de traitement des informations financières

Lorsque la Cellule de traitement des informations financières a des indices sérieux que de l'argent a été blanchi ou que le terrorisme a été financé, elle doit communiquer ses informations au procureur du Roi ou au procureur fédéral. Si cette transmission contient des informations pour lesquelles la Sûreté de l'Etat ou le SGR a communiqué des renseignements à la cellule, elle l'en informe également⁵⁸.

Apparemment, l'obligation⁵⁹ de la Cellule de traitement des informations financières se limite à la communication du fait qu'un dossier a été transmis au parquet. Les dossiers ne peuvent être obligatoirement transmis sur la base de cette disposition. Mais, ainsi que nous l'avons déjà indiqué, cette cellule peut, en tant que service public, toujours décider de communiquer ces données sur demande ou spontanément.

Renseignements détenus par un détective

Nous avons vu plus haut que le

détective est tenu à une forme propre de secret professionnel. Il existe cependant aussi une obligation de déclaration à l'égard de certaines autorités. Cette obligation de déclaration consiste à ce que le détective privé doive fournir des renseignements si certaines autorités bien précises le lui demandent.

Ainsi, dans le cadre de la protection de la sûreté nationale, le ministre de la Justice peut requérir du détective privé les renseignements concernant une mission en cours ou exécutée. Le détective est tenu d'y répondre sans délai, pour autant que les personnes qui sont chargées de recueillir les renseignements sont en possession d'un mandat spécifique du ministre⁶⁰.

Bien que les travaux parlementaires ne parlaient que des services de police comme exécutants de ce mandat spécifique⁶¹, la loi permet au ministre de la Justice d'en charger la Sûreté de l'Etat. Etant donné qu'il s'agit d'un mandat spécifique, on peut argumenter que la Sûreté de l'Etat qui vient demander des données à caractère personnel figurant dans un fichier ne peut pas être considérée comme 'destinataire' au sens de la LVP.

Données ou renseignements spécifiques provenant d'une instruction judiciaire

Le nouvel article 56, § 1er, sixième alinéa du Code d'instruction criminelle⁶² oblige le juge d'instruction à communiquer au procureur fédéral ou au procureur du Roi les informations et les renseignements qu'il

portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (M.B. 31 mars 2000).

57 Le deuxième alinéa, 2° de l'article 19 ne parle que de la possibilité de 'demander' des informations. On remarque toutefois clairement à la lecture de l'ensemble de l'article et des travaux parlementaires que le législateur voulait également instaurer une obligation de communication des données ici.

58 Article 17 de la Loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de

capitaux et du financement du terrorisme (M.B. 9 février 1993). Cette obligation de déclaration s'applique également dans le cas de l'article 12, § 3, de la loi.

59 Les travaux parlementaires parlent d'une 'possibilité' (Doc. Parl., Chambre, 2003-2004, 383/1, 49).

60 Voir en détail à ce sujet: Cappelle, J. et Van Laethem, W., *Le statut du détective privé*, Bruxelles, Politeia, 2004, feuillets mobiles.

61 Doc. Parl., Sénat, 1990-91, 1259/2, 62.

62 Inséré par la loi du 21 juin 2004 (M.B., 13 juillet 2004).

a recueillis au cours de l'instruction et qui révèlent un péril grave et immédiat pour la sécurité publique et la santé publique. Voilà pour la loi. Mais l'Exposé des motifs va un peu plus loin. Le procureur doit transmettre les informations au ministre de la Justice qui, à son tour, doit les communiquer aux 'autorités compétentes en la matière'⁶³. Sur avis du Conseil d'Etat, l'exposé des motifs indique que "ce devoir d'information doit s'exercer dans le respect du secret de l'instruction de sorte que les informations transmises par le ministre de la Justice aux autorités compétentes en la matière se limiteront à ce qui est strictement nécessaire à la sauvegarde de la sécurité publique et⁶⁴ de la santé publique⁶⁵".

Il a été fait plusieurs fois référence à la situation de la Sûreté de l'Etat et du SGR dans les travaux parlementaires. L'affaire Trabelsi, dans laquelle le juge d'instruction avait interdit au service de renseignement civil, avait interdit de commu-

iquer des informations au SGRS, a constitué l'inspiration de cette modification législative⁶⁶.

Mais cela crée une situation étrange, parce que le législateur avait manifestement perdu de vue que le secret professionnel ne s'applique pas aux relations entre juge d'instruction et service de renseignement. Sur la base de l'article 14 de la loi sur les services de renseignement, le juge d'instruction peut transmettre directement toutes les informations utiles à l'exécution des missions d'un service de renseignement; sur la base de l'article 56 C.I.Cr. il doit transmettre indirectement les informations strictement nécessaires au maintien de la sécurité publique et de la santé publique.

d'interprétation, surtout lorsqu'il s'agit de répondre à la question de savoir si les autorités peuvent transmettre des données à caractère personnel traitées, indépendamment de la finalité du traitement formulée. Et ce n'est pas admissible dans une matière si importante du point de vue de la protection du droit fondamental au respect de la vie privée. La problématique de la communication de données nécessite une réponse plus claire du législateur. Il est peut-être indiqué de faire figurer la facette du travail de renseignement dans un texte légal qui réglerait de manière globale les 'méthodes particulières de recherche' des services de renseignement.

CONCLUSION

Les règles du jeu de la communication de données de particuliers et d'autorités aux deux services de renseignement manquent de clarté. Il faut procéder à trop de travail

Wauter Van Laethem,
juriste au Comité permanent
de contrôle des services
de renseignements⁶⁷

63 Doc. Parl., Chambre, 2003-2004, 863/1, 6.

64 Les deux conditions doivent apparemment être présente simultanément (Doc. Parl., Sénat, 2003-2004, 690/2, 9). (ndt pas trouvé dans 690/2 mais dans Chambre, 2003-2004, 863/1)

65 Idem.

66 Doc. Parl., Sénat, 2003-2004, 690/2, 3-4.

67 Les points de vue adoptés dans le présent article reflètent son opinion personnelle et n'engagent aucunement le Comité permanent R.

Bedrijfsregister - Index des annonceurs *Private Veiligheid/Sécurité Privée* 23

Facility Management			tel. - tél.	fax
Faceo Belgium N.V.	Havenlaan 86C bus 201	1000 Brussel	02-422.26.11	02-422.26.45
Opleidingen				
Faceo Security Academy (FACSA)	Havenlaan 86C bus 201	1000 Brussel	02-422.26.09	02-422.26.59
Bewaking - Meldkamer / Gardiennage - Centraux d'alarme				
Faceo Security & Prevention N.V.	Havenlaan 86C bus 201	1000 Brussel	02-422.26.83	02-422.26.59
Belgacom Alert Services	rue Caril 2	1140 Evere	0800-99000	
Group 4 Total Security SA/NV	Vierwinden 13	1930 Zaventem	02-712.59.11	02-711.07.73
Oktopus NV	Bronstraat 15	1000 Brussel	02-542.05.42	02-542.05.43
Beveiliging				
Group 4 Total Security SA/NV	Vierwinden 13	1930 Zaventem	02-712.59.11	02-711.07.73