Le secret professionnel et les technologies de l'information et de la communication

Poullet, Yves

Published in:
Le secret professionnel

Publication date:
2002

Document Version
le PDF de l'éditeur

TITRE 10 - LE SECRET PROFESSIONNEL ET LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Ombres et lumières

par

Yves POULLET
Doyen de la Faculté de droit de Namur
Directeur du C.R.I.D. des FUNDP
Professeur à la Faculté de droit de Liège

> *" La transparence paraît se confondre avec la limpidité, la pureté même. Elle ressemble au soleil et à la lumière. Elle ne peut souffrir des domaines interdits, le mensonge, le mystère, le secret, la discrétion, tous les artifices qui dissimulent la vérité. Au nom de la transparence, le droit à l'information tend à devenir un droit absolu. Les images qui restent dans l'ombre, les paroles qui se disent sous le sceau de la confidence, deviennent suspects ".*
>
> (J.-D. BREDIN, cité par T. MASSIS, La transparence et le secret, *Etudes*, Juin 2001, p. 751)

Chapitre - INTRODUCTION

Pierre Lambert, dans l'ouvrage qui constitue la référence majeure sur le sujet qui nous occupe, décrit les origines lointaines de l'institution du secret professionnel et l'ancre dans le dialogue oral singulier entre celui qui souffre et son confident nécessaire, avocat, médecin, confesseur.

Le fondement historique de ce rapport singulier justifie l'interrogation à la base de notre propos : le secret professionnel survivra-t-il à l'heure des technologies modernes de l'information et de la communication. Certes, dira-t-on, celles-ci mieux que le papier sur lequel se consignait le résultat du dialogue singulier, peuvent enfermer, cryptographie aidant, les secrets de la " confession ".

Premier temps de notre réflexion, il s'agira au détour de nombre de textes récents, d'analyser combien l'obligation de sécurité mise à charge de celui qui dispose de ces technologies nouvelles, renforce indéniablement ce secret ! Si le secret peut être bien gardé grâce à la technologie, il reste que le dépositaire de ce secret se doit d'utiliser ces protections offertes. En

toute hypothèse, des lois pénales récentes réprimant la criminalité informatique viendront à la rescousse des détenteurs de secrets utilisant ces nouvelles technologies.

Le second temps de la réflexion est introduit par la multiplication des flux qu'autorisent, suscitent et développent les technologies en cause. Le secret, partagé au sein de ces réseaux ou y déposé, survit-il à cet éclatement du caractère " face to face " de la relation singulière entre le confident nécessaire et son client ou patient ? La loi de protection de la vie privée suggère de nouvelles règles pour réglementer ces flux, faut-il conclure au caractère obsolète des règles induites des principes du secret professionnel ou regretter que l'approche vie privée ne consacre en définitive une "appropriation" par la personne concernée du secret qu'elle avait confié un instant du moins à une personne de confiance.

Cette dernière remarque conduit au troisième temps de la réflexion : le secret, ainsi approprié, par celui qu'il était sensé protéger n'est-il pas plus vulnérable dans la mesure où ce transfert complet à la personne concernée soumet cette dernière à des pressions externes quant à la communication de son contenu.

Le quatrième temps de la réflexion s'inquiète des dispositions de procédure pénale introduites récemment par la loi sur la criminalité informatique. Saisie et perquisition des systèmes d'information des dépositaires de secrets créent des risques nouveaux d'atteinte à ces secrets. Les devoirs de collaboration mis à charge de certains acteurs, au profit des autorités policières, viseront certains dépositaires. Les secrets déposés se trouvent ainsi percés, mis à nu.

Chapitre 2 - UN SECRET MIEUX GARDE OU A MIEUX GARDER

1. La protection des systèmes d'information est assurée par bien des moyens techniques couplés ou non à des moyens organisationnels (gestion des clés et mots de passe, etc.)[1]. La science " cryptographique " allonge chaque jour la longueur des clés et garantit une confidentialité quasi-absolue des messages ; les " firewalls " isolent les systèmes internes d'information de tout accès non désiré et préviennent des tentatives de hacking et autres. Sans doute, peut-on voir dans cette efflorescence des techniques de protection, une meilleure garantie pour le secret.

[1] Sur ces techniques de sécurité, parmi d'autres auteurs, lire J. HUBIN, " La sécurité informatique ", in La sécurité informatique entre technique et droit, J. HUBIN, Y. POULLET (éd.), Cahier du CRID n° 14, Bruxelles, Kluwer, 1998.

SECTION - UNE OBLIGATION DE SECURITE

2. Encore faut-il que ces productions techniques et organisationnelles soient mises en place. A cet égard, on souligne un premier rôle du droit, celui d'obliger les détenteurs de secrets à protéger techniquement, tant par les technologies " hardware " que " software ", que par des mesures organisationnelles, les confidences dont ils ont gardé la trace électronique. Cette obligation dite de sécurité trouve son fondement dans l'article 16 de la loi du 8 décembre 1998[2] qui modifie et complète l'ancien article 16 de la loi du 8 décembre 1992 sur la protection de la vie privée.

3. Le principe énoncé par l'article, et déjà contenu dans le texte originaire, dispose que " le responsable du traitement... devra prendre toutes les mesures techniques ou organisationnelles requises, devra assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels ".

Il va de soi que ce principe trouve, en matière d'informations protégées par le secret professionnel, une application remarquable. Il induit, en particulier, dans les bases de données partagées par plusieurs détenteurs du secret professionnel et accessibles à distance, le devoir d'utiliser des logiciels de vérification des accès, de sécurisation des transmissions et de cloisonnement des fichiers.

Sans doute, est-ce aux divers ordres professionnels de préciser, autant que faire se peut, et en tenant compte de la diversité des situations, les normes de sécurité auxquelles devra répondre le système d'information et de communication dans les secteurs d'activités des détenteurs de secret professionnel.

A cet égard, le secteur médical a déjà pris quelques initiatives[3]. En outre, la réglementation leur impose diverses mesures, la plus remarquable

[2] Loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (*M.B.*, 3 février 1999, p. 3049 et s.). Ce texte est entré en vigueur le 1er septembre 2001.

[3] Voir l'avis national du Conseil national du 16 avril 1994 (Bulletin n° 65) qui interprète l'article 44 du Code de déontologie médicale à propos des recherches scientifiques et les recommandations de l'ordre des médecins relatives à la protection de la confidentialité lors de la transmission de données médicales à caractère personnel par le réseau internet qui prescrit toute une série d'obligations

étant certainement la nomination dans les hôpitaux d'un conseiller en sécurité[4].

4. Les modifications introduites à l'article 16 par la loi de 1998 amplifient cette obligation de sécurité dans deux directions. La première a trait aux " sous-traitants ". Il n'est pas rare que des détenteurs de secret professionnel, soit à propos d'un dossier particulier, soit pour l'ensemble des données qu'ils détiennent, confient à un tiers, tantôt la gestion des données (par ex. un back-up, pour des raisons d'archivage), tantôt une mission d'analyser certaines informations (ex. analyse de certaines radioscopies ou de résultats). Le choix de tels sous-traitants, les relations entretenues avec eux et les limites quant à l'utilisation par ces tiers des données ainsi communiquées font l'objet désormais de dispositions légales particulières.

Ensuite, le nouveau § 2 de l'article 16 oblige le responsable du traitement à certains devoirs.

" § 2. Le responsable du traitement ou, le cas échéant, son représentant en Belgique doit :

1° ....

2° veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limitées à ce dont les personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service ;

3° informer les personnes agissant sous son autorité des dispositions de la présente loi et de ses arrêtés d'exécution, ainsi que de toute prescription pertinente relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ;

4° s'assurer de la conformité des programmes servant au traitement automatisé des données à caractère personnel avec les termes de la déclaration visée à l'article 17 ainsi que de la régularité de leur application ".

---

relatives tant à l'utilisation de méthodes cryptographiques, de clés secrètes et de longueur des clés qu'aux prestataires de services de certification.

[4] Ainsi, l'annexe A : " Normes générales applicables à tous les établissements visés par l'article de l'arrêté royal du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre " (de la....) stipule : " Le maître du fichier (lire le responsable du traitement) désigne un conseiller en sécurité chargé de la sécurité de l'information. Le conseiller en sécurité conseille le responsable de la gestion journalière au sujet de tous les aspects de la sécurité de l'information. La mission du conseiller en sécurité peut être précisée par Nous (...) ". Le statut de ce conseiller en sécurité pourrait être rapproché de celui de " détaché à la protection des données ". Sur ce concept, lire nos réflexions in J. HUBIN, Y. POULLET, Protection des données à caractère personnel et obligation de sécurité, *op. cit.*, p. 215 et s.

Dans la même ligne, le § 3 prévoit :

" § 3. Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance ".

5. Toutes ces dispositions nouvelles devront trouver un écho dans les pratiques professionnelles. Elles entraînent le devoir de préciser, dans les règlements internes, les contrats de travail et les devoirs des collaborateurs de veiller au respect de la confidentialité. Leur non-respect entraînera, vis-à-vis de celui dont la confidentialité des données a été violée, une responsabilité du responsable du traitement d'autant plus facile à mettre en œuvre que l'article 15bis de la loi du 8 décembre 1992 prévoit un système de responsabilité présumée sauf au responsable de démontrer que le fait qui a provoqué le dommage ne lui est pas imputable[5].

SECTION 2 - LE DROIT PENAL AU SECOURS DU DETENTEUR DU SECRET PROFESSIONNEL UTILISANT LES RESSOURCES DE LA TECHNOLOGIE

6. La vulnérabilité des systèmes d'information et de communication, objets de protection, ne sera jamais absolue. L'importance des dommages susceptibles d'être créés par l'intrusion dans un système d'informations est sans commune mesure avec ceux provoqués par les indiscrétions traditionnelles. Dans les domaines qui nous occupent, la lecture, voire l'exploitation par un tiers indélicat d'un dossier papier négligemment abandonné par un avocat sur une table de café, cause certes des dommages à celui dont le dossier est ainsi révélé mais comment comparer cela à la copie instantanément réalisée de centaines de dossiers traités par un avocat et stockés sur son ordinateur ou suite à l'accès à la banque de données d'un hôpital au repérage automatique de la liste des malades atteints du SIDA y soignés, sous une forme prête à la rediffusion sur le net.

---

[5] Sur le système de responsabilité mis en place par l'article 15bis de la loi, Th. LEONARD, Y. POULLET, La protection des données à caractère personnel en pleine (r)évolution, *J.T.*, 1999, p. 394, n° 65. Rappelons que l'obligation de sécurité est en grande partie une obligation de moyens. La responsabilité de l'article 15bis ne pourra donc être invoquée que si le juge relève, expert aidant, que le responsable du traitement a manqué à ses devoirs de responsable diligent.

7. La loi récente sur la criminalité informatique[6] entend, par la création d'infractions nouvelles, lutter contre de tels risques : le droit, en instaurant ainsi de nouvelles incriminations et en les sanctionnant, vient au secours de celui qui utilise la technologie nouvelle[7]. Sans entrer dans le commentaire des dispositions légales à leur propos, on note que : " celui qui sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de 3 mois à un an et d'une amende de 26 francs belges à 25.000 francs belges ou d'une de ces peines... ; qu'est puni également " celui qui outrepasse son pouvoir d'accès à un système informatique ". Si, en outre, à cette occasion, il prend connaissance des données stockées, traitées ou transmises par un système informatique ou prend de telles données de quelque manière que ce soit, pire les met à disposition, les diffuse ou les commercialise, la peine sera plus sévère encore.

8. A ces infractions, s'ajoutent celles de lois plus anciennes[8] relatives au secret des communications et à la protection de la vie privée : " Sous réserve de l'autorisation de toutes les autres personnes directement ou indirectement concernées par l'information, l'identification ou les données visées ci-après, il est interdit, à quiconque, qu'il agisse personnellement ou par l'entremise d'un tiers :

1° de prendre frauduleusement connaissance de l'existence de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature transmis par voie de télécommunications, en provenance d'autres personnes et destinées à celles-ci ;

[6] Loi du 28 novembre 2000 relative à la criminalité informatique. Sur cette loi, les commentaires de C. MEUNIER, La loi du 28 novembre 2000 relative à la criminalité informatique, in *Actualité du droit des technologies de l'information et de la communication*, Formation Permanente CUP, février 2000, vol. 45, p. 41 et s.

[7] ... même si celui-ci n'a pris aucune mesure de précaution destinée à la prévention des risques qu'il a lui-même contribué à créer. A cet égard, les réflexions de F. de VILLENFAGNE et S. DUSOLLIER, La Belgique sort enfin ses armes contre la cybercriminalité, Droit d'auteur et médias, 2001, p. 68.

[8] Loi du 11 février 1991 insérant un article 88 bis dans le Code d'instruction criminelle, *M.B,*. 16 mars 1991 à propos du repérage des communications (modifiée par la loi du 19 décembre 1997, *M.B.*, 30 décembre 1997) . Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement des communications et des télécommunications privées, *M.B.*, 24 janvier 1995 modifiée par la loi du 10 juin 1998. Sur ces deux lois, lire D. VANDERMEEERSCH, Les modifications en matière de repérage et d'écoutes de (télé)communications introduites par la loi du 10 juin 1998, *Rev.dr.pén.*,1999, p.1061 et s. et F. GOSSENS, Wanneer mag een telefonisch gesprek opgenomen en beluisterd worden ? Over art.314 bis § 1, 1° Sw., *A.J.T.*, 1999-2000, p.235 et s.

2° de transformer ou de supprimer frauduleusement par n'importe quel procédé technique l'information visée au 1° ou d'identifier les autres personnes ;

3° de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne ;

4° de procéder ou de faire un usage quelconque de l'information de l'identification et des données obtenues intentionnellement ou non, et visées aux 1°, 2°, 3°, de les modifier ou de les annuler "[9].

Sans doute, de telles incriminations permettront aux détenteurs de secret professionnel de protéger la confidentialité des informations dont ils sont les dépositaires.

Chapitre 3 - UN SECRET DE PLUS EN PLUS PARTAGE VOIRE DEPOSE

SECTION - DE LA MULTIPLICATION DES FLUX : DES SECRETS PARTAGES " AUX SECRETS " DEPOSES "...

9. La technologie met les acteurs professionnels " en réseau ". Chaque acteur n'est plus isolé mais se relie à des banques de données documentaires, parfois informatives, sur l'état du client souvent. L'équipe médicale ou le cabinet d'avocats se partagent le dossier du client et chacun, réseau aidant, y apportera sa contribution. Le désarroi devant un cas délicat obligera le praticien à le soumettre, virtuellement du moins, à un confrère parfois situé en terre lointaine.

Ainsi, la technologie met le cabinet de l'avocat ou du médecin, l'étude du notaire, l'officine du pharmacien, etc., au centre d'un flux d'informations entre une multitude d'acteurs avec lesquels la communication sera digitale. Au sein des réseaux, le secret se partage avec l'administration, avec les confrères, avec des intermédiaires techniques.

10. Les ordres professionnels eux-mêmes multiplient les initiatives pour favoriser ces échanges. Les intranets professionnels foisonnent parfois sans cohérence, se sécurisent et réclament des participants une certaine discipline inspirée de la nécessité d'y respecter la déontologie et le secret professionnel.

Pour faciliter ce partage, ces échanges, les administrations elles-mêmes exigent, dans le secteur de la santé en particulier, la mise en place de " cartes d'identité " médicales dont les fonctions sont à la fois

[9] Il s'agit de l'article 109ter D de la loi du 21 mars 1991 relative aux entreprises publiques autonomes, article inséré par la loi du 19 décembre 1997, article 77.

administratives et médicales. Le dossier médical informatisé[10] sous forme de carte à puce et la carte de sécurité sociale constituent deux exemples de cette volonté administrative d'hâter les échanges au sein des réseaux bien structurés, offrant ainsi à l'Administration un outil de contrôle de l'efficacité et de la " rentabilité " du secteur et de chacun de ces acteurs. Vis-à-vis de l'Administration qui les contrôle, les dépositaires de secrets auront-ils encore des secrets ? Sans doute, le contrôle des dépenses des soins de santé et la nécessité de définir une stratégie de l'action gouvernementale[11] justifient-ils cette " transparence " accrue des activités du secteur, mais cette transparence ne peut être totale au risque de remettre en cause la liberté thérapeutique qui caractérise l'art de guérir.

11. Personne aujourd'hui ne défend plus la thèse du caractère absolu du secret professionnel. Comme l'écrit Pierre Lambert[12], le secret professionnel "ne pourrait constituer un obstacle absolu aux intérêts de la collectivité" mais, ajoute-t-il, " il vaut la peine de rechercher les règles d 'un équilibre entre les diverses valeurs en présence, toutes légitimes, mais souvent contradictoires ". L'article 458 du Code pénal oblige à la divulgation lorsque "la loi oblige à faire connaître ces secrets ". Au delà de la discussion sur le sens à donner au mot " loi " (sens matériel ou formel)[13], on notera que la simple décision de modification de la configuration d'un réseau peut avoir des impacts importants sur la transmission de données protégées par le secret professionnel et que certaines de ces modifications ne font l'objet d'aucune décision réglementaire. Le cas Pharmanet[14] est

[10] A propos de ce dossier médical général, lire l'arrêté royal du 3 mai 1999 relatif au dossier médical général (*M.B.*, 17 juillet 1999) et l'avis de l'Ordre national des médecins sur ce dossier médical " global informatisé " en date du 12 décembre 1998.

[11] Dans le domaine médical, lire, à cet égard, l'avis très nuancé du Groupe européen d'éthique du 30 juillet 1999, avis n° 13 relatif aux aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information.

[12] P. LAMBERT, *op.cit.*, p.14.

[13] Sur ce débat, notamment, H. NIJS, Is aangifte van AIDS wettelijk verplicht ?, *R.W.*, 1987-1988, p.1326; F. DUMON, Le secret médical, Cons. Man., 1987, p. 20 et s. . Cf. à ce propos l'arrêt récent de la Cour d'arbitrage du 3 mai 2000 *(J.M.L.B.*, 19 mai 2000) qui reproche à une loi son manque de précision dans le cadre d'une levée du secret professionnel à des fins d'investigation fiscale.

[14] Le projet " Pharmanet " trouve sa base dans l'article 165 de la loi coordonnée du 14 juillet 1994 relative à l'assurance obligatoire, soins de santé et indemnité qui vient d'être modifié par l'article 17 de la loi du 10 août 2001 portant des mesures en matière de soins de santé (*M.B.*, 1 septembre 2001, p. 29.802). L'alinéa 9 est remplacé par la disposition suivante : " La communication de ces données vise à permettre le remboursement des médicaments prescrits ainsi que d'une part, à

intéressant. Il s'agit d'un projet dit purement technique de transmission par voie télématique, à partir des officines pharmaceutiques, des données des prescriptions médicales pour lesquelles un remboursement est prévu. Deux pistes de lecture permettaient jusqu'ici de séparer l'accessibilité, d'une part, aux données de prescription au sens strict accessibles en particulier à des groupes de médecins chargés de contrôler la qualité des soins et le non-abus de prescriptions et, d'autre part, à celles de facturations destinées aux organismes de remboursement. La suppression de la distinction de ces deux pistes, objet du projet Pharmanet, a nécessairement un impact sur la qualité des destinataires des données et crée des risques importants d'accès aux données de soin par des personnes extérieures au cercle des praticiens de l'art de guérir. Sans doute, une évaluation de la légalité et de l'impact de telles décisions techniques et réglementaires au regard des règles du secret professionnel serait-elle indispensable sous peine de voir l'équilibre entre les valeurs du secret professionnel et d'autres intérêts publics remis en cause.

12. La circulation de l'information, objet du secret professionnel au sein des réseaux, multiplie les acteurs qui peuvent y accéder. La gestion des systèmes d'information ou des réseaux professionnels habilite des informaticiens chargés du back up ou de la maintenance à devoir intervenir. Dans le domaine de la santé, les administrations des hôpitaux et les administrations publiques en charge des soins de santé devront également traiter ces données. Il est remarquable, à propos de ce dernier

organiser la surveillance des fournitures prescrites et facturées, et d'autre part, à fournir à l'autorité compétente des informations relatives à la politique à suivre, notamment afin de permettre l'évaluation de la pratique médicale en matière de médicaments. Par évaluation de la pratique médicale, il convient d'entendre notamment : l'établissement des profils des médecins prescripteurs, le cas échéant en relation avec leurs patients, l'étude de la consommation de médicaments sous la forme de données de prévalence, l'ampleur de la comédiation, l'analyse de l'interaction entre les médecins généralistes et les médecins spécialistes lorsque des prescriptions sont délivrées par différents médecins, la détection d'indications de la confiance dans la thérapie et la vérification des effets des campagnes d'information et/ou des directives médicales qui ont été rédigées en consensus ".
On notera que lors des discussions au Sénat (Séance du 18 juillet 2001, Sess. 2000-2001, Doc. 2-860/3), la question du contrôle de la profession médicale grâce à Pharmanet et des dangers potentiels pour l' " autonomie " du corps médical a été soulevée. La mise sur pied du réseau Pharmanet est consacrée par l'arrêté royal du 15 juin 2001 déterminant les données relatives aux fournitures à tarifer que les offices de tarification doivent transmettre aux organismes assureurs (*M.B.*, 27 juillet 2001). Trois avis de la Commission ont été émis à son propos, le 25 mai 1998, le 10 juillet 2000 et le 10 mai 2001.

domaine, que pour répondre à cette nécessité de l'extension de la communication des informations, la loi de protection de la vie privée n'ait plus confié aux seuls praticiens de l'art de guérir[15] la responsabilité des traitements opérés en matière de santé mais élargit à l'ensemble des "professionnels de santé", notion très floue[16] et très large, cette responsabilité en mettant à charge de ceux-ci une obligation de secret[17]. Au moment où la loi multiplie ainsi les personnes assujetties au secret[18], sans doute peut-on craindre que cette extension vers des catégories professionnelles nouvelles, non imprégnées de cette culture du secret professionnel, ne mette en péril ou en tout cas n'affadisse la rigueur de ce secret.

13. Cette même volonté de favoriser le partage amène à la création de vastes répertoires où sont identifiées *a priori* les relations entre les " clients " et leurs " confesseurs ". Ainsi, les notaires ont créé un répertoire des testaments qui permet à chaque membre de la profession de connaître l'existence préalable de ceux-ci. Dans le secteur médical, se multiplient les initiatives de banques de données locales[19] ou régionales[20] permettant aux praticiens d'identifier plus facilement le lieu (le confrère) où se trouve le dossier d'un client. La constitution de ces banques de données soulève un problème d'un autre ordre : le secret ici n'est pas partagé. Il est " déposé "

[15] A cet égard, le rappel par le Conseil National de l'ordre des médecins du principe : " la notion du secret partagé ne s'applique qu'en cas d'échange de données médicales entre médecins dans le cadre du maintien de continuité des soins et de la consultation médico-sociale. L'accord préalable du patient est requis " (Avis du 29 octobre 1999).

[16] A noter que l'intitulé de l'arrêté royal n° 78 du 10 novembre 1967 a été rebaptisé comme " relatif à l'exercice des professions des soins de santé " par l'article 27 de la loi du 10 août 2001.

[17] L'article 7, § 4 de la loi du 8 décembre 1992 a été modifié en ce sens. L'alinéa 1 se lit comme suit : " Le traitement de données à caractère personnel relatives à la santé peut, sauf dans le cas d'un consentement écrit de la personne concernée ..., uniquement être effectué sous la responsabilité d'un professionnel des soins de santé ".

[18] L'article 7, § 4 ,alinéa 2, laisse au Roi le soin, le cas échéant, de préciser les catégories de personnes considérées comme telles. A noter que l'alinéa 3 étend encore le secret aux préposés et mandataires de ces professionnels de santé.

[19] Cf. l'obligation qu'ont les hôpitaux conformément à l'arrêté royal du 3 mai 1999 de tenir un répertoire des " dossiers hospitaliers ".

[20] Ainsi, l'expérience IRIS de la Région bruxelloise qui vise la mise sur pied d'un répertoire d'identification des patients et de la " localisation " de leurs dossiers. Dans le cadre de l'arrêté royal du 3 mai 1999 relatif au DMG (Dossier Médical Général), il est prévu aussi un répertoire permettant d'identifier le médecin généraliste en charge de chaque DMG.

a priori sans que l'identité de celui qui viendra le lire ne soit connue à l'avance. La légitimité de telles banques de données me semble devoir être soumise à des conditions très strictes quant à l'autorisation de celui qui " accède " aux données déposées, qui doivent bien évidemment rester minimales voire dans certains cas être codées[21].

SECTION 2 - ... AU DOUBLE FONDEMENT DE CES FLUX LOI " VIE PRIVEE " ET/OU SECRET PROFESSIONNEL

14. Les limites aux communications des données peuvent être tirées de la législation " vie privée " certes. Elles se déduisent avec plus de force encore des principes mêmes du secret professionnel qui, s'ils consacrent le secret partagé, ne l'admettent qu'à certaines conditions. En particulier en matière médicale, la communication à un tiers, tenu lui-même par le secret professionnel, n'est admise que si elle poursuit l'intérêt du malade, que le destinataire concourt lui-même, de manière directe ou indirecte aux soins, que la communication se limite aux données indispensables et nécessaires de cet autre praticien, enfin, et surtout, recueille le consentement même implicite du patient dûment informé[22].

15. La comparaison voire l'opposition de ce double fondement : " secret professionnel " et/ou " vie privée ", des limites à la communication des données médicales autorise une réflexion complémentaire : la seule application des dispositions légales de protection de la vie privée n'aboutit pas à une protection équivalente à celle qu'octroient les principes du secret professionnel.

Pour être plus clair, la tentation de certains de se fier à la seule protection de la vie privée pour régir les communications entre dépositaires du secret professionnel représente le risque d'un affaiblissement des protections actuelles[23] assurées par le droit du secret professionnel.

[21] Sur tout ceci, lire M.-N. VERHAEGEN, Quand la communication du secret médical à des tiers est en cause, *supra*, p.119.

[22] Sur ces conditions, lire P. LAMBERT, " Le secret professionnel ", Némésis, Bruxelles, 1985, p. 104 et s. ; p. 158 et s. ; T. MOREAU, " Le partage du secret professionnel : balises pour des contours juridiques incertains ", in " Le secret professionnel : la reconstruction du sens ", *J. dr. jeun.*, 1999, n° 189, 12-13.

[23] ... sauf à considérer que la disposition générale de la loi du 8 décembre 1992 affirmant que tout traitement doit être licite implique que, nonobstant le respect des dispositions spécifiques de la loi précisant les causes de légitimité des traitements, le responsable du traitement doit en outre respecter les prescrits du secret professionnel. Sur ce point, *infra*, n° 18.

Pour reprendre le cas des données médicales repris ci-dessus, il est clair d'une part, que le consentement du patient, selon la loi dite vie privée (art. 7 § 2 a), est une cause suffisante et légitime de la communication à des tiers y compris en dehors du cercle des personnes astreintes au secret professionnel[24] et, d'autre part, que même sans consentement du patient, la communication est légitime si elle est, dit l'article 7, § 2, " nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration des soins ou de traitement soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée " et que " des données sont traitées sous la surveillance d'un professionnel des soins de santé "[25].

Chapitre 4 - LE PIEGE DE L'APPROCHE VIE PRIVEE : LE SECRET " APPROPRIE "

16. On s'interroge, à juste titre, la loi du 8 décembre 1992 remet-elle en cause la doctrine du secret partagé au nom à la fois d'une meilleure circulation de l'information facilement assurée par la technologie et qui peut apparaître, dans l'intérêt du patient ou conforme à l'intérêt public ou général et à la fois d'une appropriation plus complète par le patient des informations couvertes par le secret ?

Sur ce second point, on constatera que si le secret professionnel est la protection d'informations nées d'un dialogue singulier qui n'appartiennent dès lors ni au dépositaire du secret, ni à la personne concernée par de telles informations, la loi de protection de la vie privée de par son fondement même, à savoir le droit de l'individu sur son image informationnelle, a tendance à consacrer les droits sur cette formation personnelle en dehors de ce dialogue singulier qui les a fait naître.

17. Trop de personnes ont assimilé les dispositions relatives au secret professionnel à celles protégeant les données nominatives de celui que le secret concerne. Notre propos cherche à démontrer que le lien entre vie privée et secret professionnel n'est pas aussi évident qu'il y paraît, même si les deux types de dispositions concourent au même objectif. Certes, à la fois les prescrits "protection des données" et ceux relatifs au secret

[24] ... même si celles-ci ne sont pas traitées par ce tiers sous la responsabilité d'un professionnel des soins de santé.

[25] A noter également l'exception à des fins de recherche scientifique. La communication est alors soumise aux conditions prévues par l'arrêté royal. (Sur cet arrêté royal, lire C. de TERWANGNE et S. LOUVEAUX, Protection de la vie privée face au traitement des données à caractère personnel : le nouvel arrêté royal, *J.T.*, 2001, p. 457 et s.

professionnel se fondent sur la nécessité de protéger la vie privée définie au sens le plus large[26]. L'article 8 de la convention du Conseil de l'Europe qui consacre le droit à la vie privée constitue la base à la fois des uns et des autres[27]. Mais, au delà de ce fondement commun, les approches suivies sont bien distinctes : les lois de protection des données cherchent à permettre à la personne une " ré-appropriation " de son image informationnelle; la notion de secret protège une relation entre un individu et les membres de certaines professions. Ce secret exclut, à la limite certes, l'appropriation des données couvertes par le secret par chacune des parties à la relation.

Développons l'idée : les lois de protection des données nominatives incluent, à juste titre sans doute, un droit à la transparence[28]. Si secret il y a, ce n'est en tout cas pas vis-à-vis de la personne concernée qui, hormis quelques exceptions, doit avoir un accès complet à son dossier. Ainsi, le veut la transparence.

De la transparence des informations à la propriété de celles-ci, le saut est facile. Comment le patient ne serait-il pas propriétaire des données de sa santé [29]? Le client de l'avocat, de son dossier ? Il y a accès et le voilà donc maître de ses données, qu'il confiera demain à un autre médecin, à un autre avocat ou à un tiers quelconque qui exhibera de son intérêt à en disposer à son tour, qu'il s'agisse d'un assureur ou d'un employeur.

[26] c'est-à-dire à la fois comme le droit d'être laissé en paix, le droit à la non-discrimination et le droit à l'autodétermination informationnelle.

[27] Déjà en 1974, VELU (Le droit au respect de la vie privée, Presses Univ. Namur, n° 10, p. 112) écrivait : " Enfin, il semble que le droit au respect de la vie privée implique l'interdiction de divulguer ou de recueillir des informations couvertes par le secret professionnel ". L'auteur ajoutait tout aussi justement :" Cela ne signifie pas que la nécessité de respecter le secret professionnel trouve exclusivement sa justification dans le droit au respect de la vie privée... à la base du secret professionnel, l'intérêt social est pris en considération autant que le besoin d'intimité du particulier ".

[28] R.O. DALCQ, Evolution du droit des patients en matière d'information et de consentement des patients, in *Liber amicorum J. van den Heuvel*, Antwerpen, Kluwer, 1999, p. 413 et s.

[29] Cf. à ce sujet, en faveur d'une approche " libertés " de préférence à celle " propriété ", les réflexions de l'auteur, in A propos de la propriété du dossier médical... : Propriété ou Liberté, in *Eigendom-Propriété*, Actes des colloques organisés conjointement par les facultés de droit de l'UFSIA et des FUNDP, La Charte, 1995, p. 301 et s.; dans le même sens, F. VAN NESTE, Het medische beroepsgeheim, in *Juridische aspekten van de geneeskunde*, 1989, p.197, n°3. K. SCHUITYSER, Eigendomsrecht en medische dossiers, *R.W.*, 1989-90, p. 3023.

Au droit à la transparence s'ajoute en effet celui de l'appropriation qu'in fine, consacre la reconnaissance, par les lois "vie privée", du consentement, comme source première de légitimation d'un traitement. Puisque j'ai le droit de connaître les informations me concernant, j'ai le droit de les céder. La loi dite de protection de la vie privée énonce le consentement (parfois qualifié d'explicite, parfois d'indubitable[30]) comme première cause de légitimité d'un traitement des données et autorise même, en matière de données relatives à la santé, la communication des données à des personnes non professionnels de la santé .

18. Traditionnellement, en particulier à propos du secret médical mais non exclusivement, la jurisprudence et les auteurs[31] considèrent que si le consentement peut être une cause de justification pour l'infraction commise par le dépositaire du secret en révélant l'information, objet du secret, ce consentement ne peut à lui seul suffire pour en justifier la transmission[32]. Il appartient au praticien de l'art de guérir de s'interroger sur les finalités de la demande d'un patient d'obtenir copie de son dossier, en particulier lorsque la communication de l'information pourrait être commandée par l'intérêt d'un tiers non nécessairement conforme à l'intérêt du patient, ainsi l'assureur qui souhaiterait connaître les données génétiques d'un candidat à l'assurance. Comme l'écrit Van Neste[33], le secret professionnel est lié aux droits de la personnalité et non aux droits patrimoniaux. Récemment, l'avant-projet de loi sur les droits des patients, introduit par le Ministre des Affaires sociales et de la santé[34], rappelle à juste titre ce devoir de précaution : " le praticien professionnel concerné peut rejeter en tout ou en

[30] En matière de données sensibles et de données relatives à la santé, le consentement doit être donné par écrit (articles 6 §2 et 7 § 1 de la loi du 8 décembre 1992)

[31] De manière générale, la synthèse proposée par P. LAMBERT, *op.cit.*, p.134 et s. ; en matière de secret médical, celle de H. NIJS, *op.cit.*, p. 368 et s., n°955 et s. et de Y.-H. LELEU, G. GENICOT, Le droit médical, De Boeck, 2001, p. 151 : " Comme nous l'avons déjà signalé, d'autres dispositions légales subordonnent la levée du secret au consentement du patient. Ce faisant, le législateur renforce le droit du patient à l'autonomie, en lui permettant de renoncer au droit au silence ".

[32] A ce propos, l'article 64 du Code de déontologie médicale : " La déclaration d'un malade relevant son médecin du secret professionnel ne suffit pas à libérer le médecin de son obligation ".

[33] F. VAN NESTE, *op.cit.*, 1989, p.197, n° 3.

[34] Cet avant-projet de loi a fait l'objet de divers avis, ainsi celui du Conseil national de l'Ordre national des médecins (23 janvier 1989, Bull. Conseil national, n°83, mars 1989, p.19 et avis du 9 janvier 2001) et de la Commission de protection de la vie privée (avis du 11 septembre 2001) qui estiment légitime ce droit de refus mais s'inquiètent cependant du large pouvoir d'appréciation laissé au prestataire de soins.

partie la demande de la personne... visant à obtenir consultation ou copie... (de son dossier)[35] ".

Notre souci est de rappeler dès lors que le consentement de la personne concernée, s'il peut être une cause nécessaire de légitimité du traitement de données couvertes par le secret professionnel, ne peut cependant suffire[36] et que les règles traditionnelles en matière de secret professionnel doivent continuer à s'appliquer.

Chapitre 5 - LE SECRET " PERCE "

19. On connaît le droit des autorités policières à percer le secret professionnel. " Le législateur, écrit Nijs à propos du secret médical, n'a jamais eu l'intention d'accorder au cabinet médical une sorte de droit d'asile permettant de soustraire inconditionnellement aux recherches judiciaires aussi bien les documents suspects que les pièces à conviction. Pourtant, l'obligation de garder le secret est impensable sans un droit de garder le secret, qui, à son tour, doit être respecté également par la juridiction ".

Ce relatif équilibre s'avère délicat à réaliser de manière générale. La loi récente sur la criminalité informatique adoptée le 28 novembre 2000[37] remet-elle en cause cet équilibre ?

[35] Nous ne pouvons, dans le cadre de ce bref exposé, entrer dans toutes les controverses à propos du droit d'accès du patient à son dossier qui doit être le plus large possible. Par contre, le devoir de précaution doit exister, nous semble-t-il, en matière de copie du dossier. Des sanctions pénales en cas d'abus par un tiers, c'est-à-dire de pressions exercées par ce dernier pour que la personne concernée utilise son droit d'accès devraient être prévues.

[36] A cet égard, on rappellera que les causes de légitimation des traitements explicitement prévues par les articles 5, 6 ,7 et 8 de la loi du 8 décembre 1992 ne dispensent pas le responsable d'un traitement et le juge d'examiner conformément à l'article 4 de la même loi , si les données sont " traitées loyalement et licitement " et collectées pour des finalités déterminées, explicites et légitimes.... ". En d'autres termes, le respect des règles du secret professionnel est une condition de licéité du traitement des données à caractère personnel qui doit être respectée au delà des conditions nécessaires de légitimité par ailleurs prévues. Sur cette distinction entre l'article 4 de la loi qui fixe des conditions générales de licéité des traitements et l'article 5 qui énonce des conditions nécessaires mais non suffisantes de légitimité de ceux-ci, lire T. LEONARD et Y. POULLET, *op. cit.*, n° 25.

[37] La loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 18 mars 1993. Sur cette loi, lire C. MEUNIER, La loi du 28 novembre 2000 relative à la criminalité informatique, in *Actualités du droit des technologies de l'information et de la communication*, CUP, février 2000, vol. 45, p. 40 et s.

S'étant saisie d'initiative du texte du projet, la Commission de protection de la vie privée[38] avait mis en évidence ce problème particulier, dans la mesure où la personne appelée à collaborer devait pouvoir invoquer ce secret pour s'opposer à toute mesure et, lors d'une perquisition, devait pouvoir réclamer quelques garanties (présence d'un membre du Conseil de l'Ordre de la profession) pour limiter strictement sa collaboration au système d'information : "Par ailleurs, la Commission souhaite attirer l'attention du législateur sur le fait que les textes en projet ne règlent pas la question de savoir dans quelle mesure certains responsables de systèmes informatiques pourront invoquer la règle du secret professionnel (avocats, journalistes, médecins, ...). Rien n'est prévu pour que les personnes astreintes au secret professionnel puissent l'invoquer. Les précautions particulières qu'implique la sauvegarde du secret professionnel face à une perquisition nécessitant l'accès à un système informatique devraient également être réglées. La Commission est d'avis que des mécanismes d'intervention des instances professionnelles devraient être légalement prévus. Ainsi, on pourrait imaginer qu'un membre du Conseil de l'Ordre des médecins ou des avocats soit présent lors de l'intervention des autorités judiciaires[39]".

20. En ce qui concerne précisément le droit de perquisitionner le système d'information d'un professionnel de la santé[40], on rappellera que la jurisprudence de la Cour européenne des droits de l'homme exige, sur base de l'article 8 de la Convention, que les locaux abritant des documents couverts par le secret professionnel jouissent d'une protection accrue, que toute perquisition en la matière soit proportionnée et ciblée, de manière à

[38] Avis de la Commission de protection de la vie privée n° 33/99 du 13 décembre 1999 relatif aux projets de loi relatifs à la criminalité informatique.

[39] A cet égard, le débat entre la tendance dure qui exige la présence de membres de l'ordre professionnel et la tendance plus souple qui souhaite simplement l'information *a posteriori* de ceux-ci, développée par E. JAKHIAN et P. LAMBERT, Les perquisitions dans les cabinets d'avocats, note sous Cour eur. D.H., 16 décembre 1992, *J.T,.* 1994 , p. 65.

[40] Cf. l' avis du Conseil national de l'ordre des médecins du 9 janvier 2001 déjà cité : " A cet égard, le Conseil national attire spécialement l'attention du législateur sur la saisie de dossiers de patients par les juges d'instruction. Il est évident que rien ne peut s'opposer à la saisie lorsque le suspect est le médecin mais elle est selon le Conseil national, inconcevable lorsque le suspect du délit est le patient lui même. Les données confiées par un patient dans le cadre de son traitement ne peuvent être utilisées contre lui. Ceci réduirait à néant des relations de confiance péniblement construites avec des patients demandant et nécessitant de l'aide, souvent en raison de troubles graves de comportement. Une initiative législative devrait combler cette lacune dans la protection des droits du patient ".

éviter l'accès à des documents couverts par le secret professionnel étrangers à l'enquête. La présence ou au moins l'information d'un représentant autorisé de la profession (un membre du Conseil de l'Ordre) sont en outre requis. Ce devoir de précision, quant aux documents à saisir, se heurte à une difficulté lorsque les informations chez le dépositaire du secret professionnel se trouvent sur un support informatique ou sont accessibles via un réseau. Une disquette et a fortiori un disque dur contiendra des informations relatives à des milliers de personnes visées et leur saisie désormais autorisée par la loi sur la criminalité informatique[41] risque d'entraîner une divulgation d'informations bien au-delà des nécessités de l'instruction, divulgation particulièrement dommageable aux personnes dont les secrets avaient été confiés au support visé.

La même loi sur la criminalité informatique autorise la perquisition " virtuelle ", c'est-à-dire le droit des autorités policières dans le cadre d'une perquisition à étendre la recherche d'informations " vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu où la recherche est effectuée "[42]. A nouveau, comment ne pas craindre que, connexion via le réseau aidant, les autorités ne percent les " secrets " non d'un seul dépositaire mais de tous ceux connectés à celui perquisitionné. Pire, on peut imaginer qu'à partir de l'ordinateur d'un client, l'autorité policière ne remonte vers celui du confident nécessaire.

21. Enfin, la loi déjà citée prescrit un devoir, à charge de celui qui a une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, de collaborer à la recherche de la vérité, ainsi par exemple en fournissant les clés de décryptage ou les mots de passe en

[41] La loi du 28 novembre 2000 sur la criminalité informatique ( ) introduit un nouvel article 39bis dans le code d'instruction criminelle. Celui-ci stipule : " La saisie des données pertinentes pour l'instruction, stockées, traitées ou transmises par le biais d'un système informatique, peut s'effectuer intégralement conformément à la procédure traditionnelle dans la mesure où elle s'accompagne de la saisie du support matériel sur lequel elles se trouvent (par exemple, l'ordinateur, des disques optiques, disquettes, ...) "
Sur cette disposition, lire Y. POULLET, " A propos du projet de loi n° 214 : la lutte contre la criminalité dans le cyberespace à l'épreuve du principe de régularité des preuves ", Liber Amicorum J. du JARDIN (Y. POULLET, H. VUYE (éd.), Kluwer, 2001, p. 3 et s.; cf. également S. DUSOLLIER et F. de VILLENFAGNE, La Belgique sort enfin ses armes, Auteurs et Média, 2001, p. 73.

[42] Il s'agit du nouvel article 88ter du Code de procédure criminelle introduit par la loi sur la criminalité informatique.

assurant le fonctionnement du système[43]. On peut dès lors imaginer que le gestionnaire du système d'information d'un hôpital ou d'un cabinet d'avocat ne doive fournir la liste des clés utilisées par les médecins ou les avocats pour crypter leurs messages ou simplement leurs données.

Pire, les autorités professionnelles qui gèrent les intranets professionnels, qui souvent délivrent les certificats permettant à leurs membres l'utilisation de ces intranets et enfin gardent trace des communications échangées au sein de cet intranet, risquent de voir leur collaboration requise pour permettre l'accès à ces messages, sans que les autorités policières ne doivent même s'adresser aux dépositaires de secret professionnel, émetteurs ou destinataires de ces messages.

En ce qui concerne le devoir de collaboration, le Conseil d'Etat avait clairement plaidé pour une exception " sous peine de vider l'article 458 du Code pénal de tout sens ".

Sans que le texte ne mentionne expressément une exception au profit des dépositaires de secret professionnel, on notera cet étrange passage de l'exposé des motifs : " En ce qui concerne les personnes tenues au secret, le but n'est pas de déroger au droit commun en matière de respect du secret professionnel : les personnes tenues par le secret professionnel et agissant dans le cadre du secret professionnel suivent le même régime que si elles étaient appelées à témoigner en justice ; ceci implique donc un droit et pas une obligation de coopération lorsqu'elles doivent rechercher elles-mêmes des données spécifiques[44] ".

Ainsi, les personnes tenues au secret professionnel seraient-elles en droit de se taire et de ne pas collaborer. Une telle conclusion apparaît comme illogique dans la mesure où ce droit de se taire est copié, selon les dires du Ministre, de celui existant au profit de ces personnes lorsqu'elles sont appelées à témoigner. Et l'appel au témoignage du dépositaire d'un secret en réponse à des assertions formulées est bien différent de l'appel à la collaboration dans la recherche d'une infraction par la mise en œuvre de moyens propres à ce dépositaire.

22. En conclusion, si certes, toutes ces dispositions nouvelles se justifient par l'immatérialité, la volatilité et l'opacité des données que permettent les traitements modernes de l'information, leur existence et leur application dans la pratique quotidienne des parquets accroissent néanmoins les

[43] Il s'agit de l'article 88 4° du Code de procédure criminelle introduit par la loi sur la criminalité informatique.

[44] A propos du droit du dépositaire du secret à se taire lors de son interpellation comme témoins, lire C. HENNEAU, J. VERHAEGEN, Recherche policière et secret médical, *J.T.*, 1988, p.165 et s.

craintes de voir le secret professionnel mis à nu, percé dans une mesure jamais atteinte.

CONCLUSION

23. Le secret professionnel vit à l'heure des nouvelles technologies des heures difficiles. Les informations qu'il protège bénéficieront certes des protections nouvelles que la technologie développe et continuera à développer. Le rôle du droit et des organes déontologiques en charge du respect de ce secret est d'exiger que les secteurs en charge de secrets professionnels les utilisent pleinement dans le cadre de leurs systèmes d'information et de communication.

Au fil des réseaux, le secret se partage, se dilue. C'est le rôle du législateur et des ordres professionnels de bien peser en la matière les intérêts louables mais souvent contradictoires qui peuvent justifier ces communications ou au contraire les limiter : d'une part, intérêt des personnes concernées à des services meilleurs, intérêt de l'administration à mieux contrôler et définir sa politique, intérêt des praticiens à une meilleure information, etc. et, d'autre part, intérêt des personnes concernées à la confidentialité de leurs données et des professionnels à exercer librement leur art. Cette pesée d'intérêts doit être faite. Elle peut conduire à des solutions qui, sans proscrire la communication, la réservera à certains acteurs ou la limitera à des données codées, voire anonymes.

Ensuite, si les craintes engendrées par les technologies nouvelles ont suscité des législations protectrices de la vie privée des citoyens qui concourent indéniablement à la défense de la confidentialité des informations et donc offrent des synergies appréciables avec les règles du secret professionnel, on souligne que l'accent mis par ces législations nouvelles sur l'appropriation des informations par la personne concernée peut contribuer, si on n'y a garde, à un affaiblissement du secret professionnel.

Enfin, si les réseaux multiplient les acteurs et les traces de leurs interventions, ils permettent un exercice plus facile des compétences de l'autorité policière. Là, également, le droit traditionnel du dépositaire de se taire doit être respecté intégralement et ne peut être trahi par les multiples traces électroniques laissées par ce dernier au hasard des réseaux.