LES CONDITIONS DE LA CONFIDENTIALITÉ

dans la prise en charge des personnes vivant avec le VIH aujourd'hui.

JUILLET 2016

COREVIH Ile de France Sud

Rapport du groupe de travail du COREVIH Ile de France Sud

Préface

Ce rapport très complet sur les conditions de la confidentialité dans notre pratique de prise en charge s'inscrit dans la série de documents publiés par le Corevih Ile de France Sud depuis 2008. Ces documents, souvent le fruit de séminaires approfondis ou de travaux en groupe spécialisé, cherchent à peser sur la qualité du service rendu. Ils font l'objet de brochures largement diffusées contribuant à construire une stratégie, constamment réinvestie et améliorée, et un corpus éthique solide. Il peut s'agir de questions d'intérêt général, rappelant les auto-saisines du Conseil National du Sida des années fin de siècle. Mais l'effort au sein du travail Corevih est toujours apporté à des conseils et des solutions pratiques, prenant largement en compte l'évolution des connaissances et des idées.

Comme le rappelle l'introduction, la confidentialité est un problème ancien déjà étudié par Hippocrate. C'est un élément essentiel de la confiance nécessaire à la prise en charge de tout patient quelle que soit la pathologie. En anglais, confidence signifie autant la confiance que la confidence au sens français. Mais les bases connues et souvent décrites de la confidentialité doivent nécessairement être repensées au regard des changements considérables survenus depuis 30 ans (depuis le début de l'épidémie VIH) tant dans le soin et les parcours de santé que dans la recherche, et l'environnement technologique. C'est toute la société qui se transforme et les conditions théoriques et pratiques de la prise en charge sont constamment adaptées alors que la confiance et le respect de la personne, donc la confidentialité, peuvent être menacés.

Le rapport rappelle opportunément l'importance du secret, les menaces de la société moderne et les possibles ajustements, indispensables en réalité, dans l'ère des nouvelles technologies qui facilitent pourtant l'efficacité et la qualité du travail.

Alain SOBEL
Président du Corevih Ile de France sud

Les conditions de la confidentialité dans la prise en charge des personnes vivant avec le Vih aujourd'hui

Rapport du groupe de travail du Corevih Ile-de-France Sud :

Madame Claudine BOLLIOT
Madame Danielle LE ROUX
Madame Janine PIERRET
Madame Marie-Pierre PIETRI
et
Madame Hélène LELONG
Madame Rose NGUEKENG
Madame Dominique SALMON

Juillet 2016

Le groupe remercie tout particulièrement :

- *Monsieur Louis DO, pharmacien, membre du Corevih IdF Sud,*
- *Monsieur Jean-Marc MULET, responsable sécurité du système d'information, AP-HP.*

SOMMAIRE

I. Introduction

I - A - Confidentialité et secret : définitions, périmètre.

" Admis dans l'intimité des personnes, je tairai les secrets qui me seront confiés. Reçu à l'intérieur des maisons, je respecterai les secrets des foyers et ma conduite ne servira pas à corrompre les mœurs". (serment d'Hippocrate, vers - 400).

" Il n'y a pas de soins sans confidences, de confidences sans confiance, de confiance sans secret". (B. Hoerni, *Ethique et déontologie médicale*, Masson, 2000).

Quelques siècles séparent ces deux citations qui cadrent bien les notions de confidentialité, confidence et secret.

La confidentialité comporte plusieurs volets : **le secret médical, le secret professionnel**, la discrétion professionnelle, le devoir de réserve ; ces derniers sont surtout destinés à protéger l'administration ou l'entreprise. La discrétion professionnelle est un devoir moral, elle n'est pas soumise au code pénal, contrairement au secret professionnel

Si la notion de secret médical est ancienne, elle n'est apparue dans le code pénal français qu'en 1810. Des modifications ont été introduites en 1992 puis surtout en 2002 avec la loi dite loi Kouchner.

Le secret médical est un devoir, une obligation même, pour les soignants et un droit pour les patients. Afin de recevoir les meilleurs soins, le patient doit pouvoir tout dire sans craindre un instant que sa confiance, ses confidences, puissent être trahies.

Il existe des dérogations au secret médical : ainsi, les maladies contagieuses à déclaration obligatoire ; les incapables majeurs ; les internements psychiatriques (autrefois appelés 'hospitalisations à la demande d'un tiers', 'hospitalisations d'office') ; la prévention et la maîtrise des risques graves pour la santé humaine ; les immigrés en situation irrégulière en centre de rétention (obligation d'indiquer les pathologies contre-indiquant un retour au pays) ; les suspicions de maltraitance sur enfants de moins de 15 ans ou les personnes incapables de se protéger, etc...

Le terme secret professionnel étend l'obligation à tous les soignants et même à tous les intervenants autour d'un patient. Les assistants de service social sont soumis au secret professionnel (article L.411-3 du code de l'action sociale et des familles). Il en va de même pour toute personne participant aux missions de l'Aide sociale à l'Enfance (ASE).

Un médecin appelé à témoigner en justice, doit invoquer l'obligation de secret. Le secret est absolu et ni le juge ni le patient ne peuvent s'y opposer. De même, un médecin traitant doit refuser de répondre à une compagnie d'assurance qui lui demanderait des renseignements médicaux. Il n'y a pas de secret partagé entre un médecin traitant et un médecin de compagnie d'assurance.

Afin d'assurer la continuité des soins ou déterminer la meilleure prise en charge possible, le **secret** médical peut être **partagé** entre plusieurs professionnels de santé et peut être étendu à tous les professionnels intervenant autour d'un patient (article L1110-4 du code de la santé publique). " Lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe". Le patient, " dûment averti" peut toutefois s'opposer à ce partage.

La protection absolue des informations s'applique tant aux dossiers sur papier qu'aux supports informatiques et aux transmissions par voie électronique.

I - B - Confidentialité et secret dans d'autres pays.

La plupart des pays sont dotés d'une législation sur le secret médical ou professionnel. Dans les grandes lignes, ces législations se ressemblent, avec toutefois quelques variantes intéressantes.

Au **Danemark**, la loi sur les droits des patients (1998) permet aux compagnies d'assurance d'avoir accès à des informations sur la santé d'un patient et même de sa famille.

En **Suède**, pays qui dispose d'une loi applicable au secteur public et d'une autre pour le secteur privé, des dérogations au secret sont possibles : par exemple à la demande de l'Agence des Transports pour évaluer si telle personne est apte à conduire, y

compris un tracteur ou un taxi ; à la demande d'une université qui envisagerait d'exclure tel étudiant ; en cas de suspicion de meurtre, viol, agression aggravée, conduite en état d'ivresse.

Au **Royaume Uni**, " la confidentialité est un devoir important, mais elle n'est pas absolue" (General Medical Council, 2013). Le secret peut être levé mais seulement avec le consentement exprès du patient. Une compagnie d'assurance peut s'adresser à un médecin traitant pour obtenir des informations sur un patient, mais seulement après avoir obtenu l'autorisation du patient pour ce faire et le patient a le droit de consulter tout document le concernant dans ce cas.

En **Espagne**, en plus des dérogations classiques (risque pour la santé publique, mise en danger d'un tiers) les compagnies d'assurance peuvent demander à un candidat à l'assurance de se soumettre à un examen médical.

Le cas de l'**Allemagne** est particulièrement intéressant, compte tenu des débats qui ont suivi l'affaire du co-pilote de la Germanwings. Le code professionnel (Berufsordnung) qui réglemente les obligations éthiques et déontologiques des médecins allemands, n'autorise qu'une seule exception au secret médical, "*la défense d'une valeur juridique d'ordre supérieur*", à savoir une menace pour la vie humaine. D'après Caroline Copley (Reuters, 31/3/2015) si la confidentialité est tellement protégée en Allemagne c'est en réaction aux surveillances massives menées par la Gestapo de l'Allemagne nazie et la Stasi de l'Allemagne de l'Est. Pour Carissa Veliz (*Practical Ethics,* University of Oxford, 1/4/2015) " Si le médecin de Lubitz n'a pas alerté la Germanwings, ce doit être parce qu'il/elle n'estimait pas qu'il constituait une menace. (...) Il y a plus dangereux qu'un pilote avec une maladie mentale, c'est un pilote qui a une maladie mentale mais ne cherche pas à se faire soigner parce qu'il n'a pas confiance en son médecin".

Pour les Etats-Unis, comme pour le Canada, il existe à la fois des lois fédérales et des lois spécifiques pour les états ou provinces. En gros, le code d'éthique médicale, établi par l'Association des Médecins Américains, prévoit quelques exceptions au secret médical telles que le risque de suicide ou d'agression, les maladies contagieuses, les blessures par armes.

II. Secret et confidentialité : Le patient et son environnement

II - A - Pour les patients : dire ou ne pas dire

Maintenir ou non le secret sur le VIH a toujours été au centre des préoccupations des personnes concernées. C'est à la fois un moyen essentiel et une condition pour vivre, véritable pivot autour duquel s'organisent les ressources nécessaires à la poursuite de la vie. Cette ressource est aussi un enjeu pour les personnes qui vont avoir à faire des choix, à se contrôler et à exercer leur vigilance. Le secret a été la thématique centrale dans les premiers travaux de recherche sur les personnes atteintes en France comme aux Etats-Unis et dans les pays anglo-saxons.

Les " stratégies de contrôle de l'information » adoptées par les personnes pour vivre avec une maladie et faire face au stigmate ont été étudiées depuis 40 ans par les sciences sociales. Le sociologue E. Goffman[1] a souligné que le stigmate n'est pas un attribut mais que c'est en termes de **relations** qu'il convient de parler. Par conséquent, le stigmate intervient essentiellement dans les situations d'interaction et de rapport à l'autre. La personne suppose-t-elle que sa différence est déjà connue ou visible, ou bien pense-t-elle qu'elle n'est ni connue ni immédiatement perceptible par les autres ?

Dans le premier cas, on considère que la personne est discréditée, dans le second, elle est discréditable. Ainsi dans le cas de la personne discréditée, elle doit gérer les tensions que provoque sa différence, alors que l'individu discréditable doit savoir contrôler l'information de façon à garder la maîtrise de la situation. Dans ce dernier cas, les personnes ont alors recours à différentes techniques pour contrôler l'information relative à leur situation : la dissimulation ; l'imputation des signes à une autre origine ; le maintien d'une certaine distance sociale ; le dévoilement volontaire ou la divulgation.

"Je ne me cache pas pour prendre mes comprimés. Parfois mes petits-enfants demandent : grand-mère tu prends quoi ? Je ne leur parle

1 E. Goffman, *Stigmates. Les usages sociaux du handicap*, Paris, Les Editions de Minuit, 1975 (édition originale, 1963).

pas du VIH, je dis juste que je suis malade" Salomé, témoignage[2]

Si le secret a surtout été analysé comme une réaction au stigmate dans des maladies très différentes (épilepsie, maladie de Parkinson, autisme...) le sida, maladie inconnue et mortelle, a donné lieu à un discours social en termes d'épidémie, de contagion et de peur de l'Autre qui a réactivé et complexifié cette thématique. Et, comme nous le voyons encore aujourd'hui, l'existence d'un traitement et la diffusion d'informations ont des effets limités et ne suffisent pas à lutter contre les conséquences du stigmate. En d'autres termes, être atteint d'une maladie même non visible et traitable, c'est toujours être confronté aux réactions des autres.

Cette information que les personnes détiennent sur elles met en cause leur durée de vie et leur avenir, c'est pourquoi la diffuser ou la garder pour soi s'inscrit dans des rapports aux autres qui sont différents selon les divers lieux de la vie sociale. Rapports de filiation, rapports électifs amicaux et amoureux, rapports professionnels qui demandent un véritable travail pour savoir à qui, quand et comment faire une telle annonce. Ces destinataires, capables de partager ce qui est considéré comme un secret, sont choisis et sélectionnés à partir de l'acquisition d'un savoir sur eux qui s'est fait au fil des années et par un frayage au quotidien. Mais dans tous les cas, que le secret soit levé ou maintenu, il occupe une place centrale dans la réorganisation de la vie des personnes infectées par le VIH et dans l'image qu'elles veulent donner d'elles. La nature des liens affectifs dans cette nébuleuse que constituent les proches pose des problèmes d'appréciation et d'évaluation de l'Autre. Confiance, amour, sollicitude, attente, souci et savoir de l'Autre sont autant d'éléments qui vont permettre d'inscrire le secret dans la relation et lui donner son statut.

Ce secret a changé de signification au cours des années car apprendre sa contamination en 1986, dix ans plus tard et aujourd'hui ce n'est pas être confronté à la même révélation. Ce secret dont étaient dépositaires les personnes dans les années 1980 était à la fois celui de l'annonce de leur mort et celui d'être pris dans une épidémie que les médias ont contribué à faire connaître en la présentant comme la peste ou un châtiment divin.

2 COREVIH Ile-de-France Sud, *Femmes vivant avec le VIH aujourd'hui,* Actes du Colloque 11 décembre 2014, p. 29.

À partir de 1996, les personnes apprennent qu'elles sont infectées par un virus, cause d'une maladie dont les métaphores, même quand elles sont encore présentes, ont perdu de leur force. Elles évoquent alors le respect de l'intimité, de la vie privée et familiale pour maintenir le secret. Ce repli ou ce rabat sur l'individu se retrouve dans beaucoup de maladies graves. Ce changement est aussi à mettre en relation avec l'importance prise par les traitements qui contribuent à l'individualisation de chaque cas.

Il importe de remarquer que la honte ne permet pas à soi seule de comprendre le maintien du secret et quand elle apparaît, elle n'est pas seulement celle du corps souillé mais aussi celle du corps contaminant et donc dangereux qui transmet la mort en particulier chez les femmes. La honte est aussi celle d'un passé ou d'une histoire que ces personnes ne souhaitent pas divulguer (passage en prison, usage de drogue). Mais toute expérience de la maladie confronte aux métaphores préexistantes, produites et imposées par la société et la diffusion de connaissances scientifiques ou même l'existence d'un traitement ne sont pas toujours suffisantes pour les contrebalancer.

Bien que le contenu du secret ait changé de signification au cours des décennies, les raisons de sa diffusion ou de son maintien sont à la fois relativement stables et diverses. Ainsi dans le cas de l'épilepsie, révéler la maladie peut servir les mêmes buts que la dissimuler. En effet, le dire peut avoir un but préventif afin de se décharger du poids du secret et ne pas courir le risque d'être découvert en cas de crise ; thérapeutique pour que l'entourage sache comment réagir si un problème survient. Mais dans tous les cas, " le dire" parce que " ça n'a pas d'importance" revient au même que " ne pas le dire" parce que " ça ne sert à rien". Cette difficulté à dire sa contamination correspond également à ce que des sociologues anglais, G. Scambler et A. Hopkins[3], ont nommé le stigmate ressenti ou intériorisé. Ce serait en quelque sorte la part d'irréductible à laquelle chacun est confronté quand il est atteint dans son intégrité corporelle et dans l'image qu'il a de lui comme dans celle qu'il veut donner aux autres. Cette faillite du corps ébranle la confiance en soi et conduit à s'interroger sur celle des autres.

3 G. Scambler et A. Hopkins, " Being epileptic : Coming to terms with stigma", *Sociology of Health and Illness*, 1986, 8 : 26-43.

Mais si le sens du secret s'est modifié avec la durée et les avancées médicales qu'en est-il dans l'histoire de la personne ? Que s'est-il passé entre le moment où la personne a appris sa contamination et reçu un message et sa transmission à un destinataire ou à un dépositaire ? Car l'annonce de l'infection à VIH s'accompagne d'un effet de sidération, d'abattement voire de dépression. Période plus ou moins longue qui peut varier entre plusieurs semaines et quelques années en fonction de l'époque où elle a lieu et de l'histoire de la personne. Période au cours de laquelle s'élabore une stratégie de vie à partir de l'agencement de divers éléments parmi lesquels le secret occupe une position centrale : comment vais-je vivre ? combien de temps ? à qui le dire, quand et comment ?

Sa diffusion se fait généralement de façon progressive, mais le compagnon, le(a) conjoint(e) en est rapidement le destinataire. Ensuite, commence le travail de sélection qui s'inscrit le plus souvent dans une stratégie raisonnée de diffusion de l'information : quelques personnes de l'entourage en seront informées, les parents ainsi que les enfants sont généralement tenus en dehors le plus longtemps possible. Par-delà la diversité des situations individuelles, quand un choix est fait la personne n'en change guère sauf sous le poids d'événements contingents et extérieurs. En effet, tout semble se passer comme s'il n'y avait pas de remise en question et de modification majeure du choix effectué dès le début. Des personnes vivent depuis dix ans avec un secret qu'elles n'ont partagé qu'avec un petit nombre de personnes, le plus souvent un compagnon ou un(e) conjoint(e) et un proche. D'autres ont levé le secret à la suite d'une hospitalisation, d'une maladie d'un proche, d'une émission de télévision sur le sida, mais quand ce secret si chèrement maintenu est divulgué par un tiers, ce sera une véritable violence pour la personne qui se sent alors dépossédée de sa propre vie dont elle a l'impression de perdre le contrôle. Car il s'agit bien d'un secret et non d'une confidence étant donné sa charge émotionnelle : on dit à l'Autre que l'on a une maladie mortelle. C'est pourquoi la personne à qui ce secret est confié en est le "*dépositaire*" pour reprendre la distinction proposée par l'anthropologue A. Zempleni : " On 'révèle' un secret à tout le monde ou à n'importe qui, ou alors – sous la forme de la confession et de l'aveu – directement à son destinataire. On ne le 'communique' qu'à des confidents choisis par décision individuelle ou bien -selon l'étymologie- qu'à ceux qui partagent une fonction ou une charge dans la Cité en vertu d'une décision historique

antérieure. Dans l'un et l'autre cas, on ne le communique qu'à des dépositaires, généralement proches mais par définition distincts des destinataires"[4].

Cette différence entre les personnes à qui le choix a été fait de dire la contamination par le VIH et celles qui l'ont appris par un tiers se révèle importante dans les stratégies de vie.

Le secret s'inscrit dans des stratégies complexes et sélectives qui correspondent à l'interprétation donnée aux relations avec les proches ainsi qu'à la façon dont chacun va se reconstruire et reconquérir son soi. **Dans l'ensemble, les personnes vont plutôt décider d'une diffusion limitée de leur contamination et sélectionner au cas par cas les dépositaires.** Véritable travail de choix et d'identification des Autres, proches ou lointains, avec qui elles vont partager leur secret. Ce message qui met en cause la vie même de celui qui le livre n'est pas facile à recevoir et enferme l'Autre dans un secret qui peut être lourd à porter. La façon dont les personnes envisagent leur situation et l'appréciation qu'elles portent sur la capacité de l'Autre à être le dépositaire de ce secret sont au cœur de cette sélection.

Dans l'enquête ANRS-Vespa de 2003[5], plus d'une personne sur trois interrogée (35%) a révélé systématiquement l'infection VIH, alors que 28% l'ont maintenu secrète. De nombreuses personnes ne sont pas concernées par la révélation car elles n'ont plus de père, plus de mère et ne travaillent pas et ont donc des stratégies réussies de dissimulation à un entourage restreint.

Au sein des relations de filiation, les ascendants ont pris une importance particulière compte tenu de l'âge et des modes de vie des personnes infectées par le VIH, alors que les enfants sont dans l'ensemble jeunes étant donné l'âge de ces dernières. C'est pourquoi, aux deux âges extrêmes de la vie, les raisons du silence sont le désir de protéger l'Autre et de ne pas troubler l'ordre naturel des générations.

---

4 A. Zempléni, " La chaîne du secret", *Nouvelle Revue de Psychanalyse*, 1976, 14, p. 315. Souligné par l'auteur.

5 P. Peretti-Watel, B. Spire, Groupe ANRS-VESPA, *Sida, une maladie chronique passée au crible*, Presses de l'EHESP, 2008, chapitre 14, 177-190.

Cette protection recouvre différents aspects : une telle annonce est inutile car l'enfant est trop jeune pour comprendre ou les parents trop âgés et malades ; l'Autre peut ne pas comprendre, mal réagir et être déstabilisé. Cette protection de l'Autre est aussi un moyen de se protéger de ses réactions car une telle annonce peut déclencher une angoisse et susciter un questionnement incessant que ne veut, ni ne peut vivre la personne concernée.

" On ne dit pas à son enfant qu'on est séropositive car il va penser que maman est une prostituée" Albertine Pabingui de l'association Da Ti Séni[6]

Le refus de la compassion s'accompagne souvent de la peur que le regard de l'autre change. Le maintien du secret aux deux âges extrêmes de la vie peut être vu comme le devoir de se taire selon une expression empruntée à la sociologue I. Théry. En revanche, quand les parents ont été informés c'est généralement assez tôt et la mère l'a souvent été la première. Cette annonce est présentée comme normale et s'inscrit dans une véritable relation d'amour et de confiance dont la personne peut attendre compréhension et soutien.

" Je suis veuve, j'ai dix enfants, je suis grand-mère et arrière-grand-mère. Quand je me suis sentie plus forte, je l'ai annoncé à mon fils aîné de 42 ans, avec qui je parle beaucoup. Il m'a dit de ne pas en parler aux autres" Salomé, témoignage

Le secret s'inscrit différemment dans les relations avec les Autres proches que sont l'entourage amical et certains membres de la fratrie. Il ne sera partagé que dans des conditions particulières d'intimité et de confiance en fonction des caractéristiques de cette relation. Dans l'enquête VESPA 2003, 70% et 62% des personnes interrogées choisissent d'en parler spontanément à des amis et à des frères et sœurs. À ce niveau, le savoir sur le proche, l'évaluation de sa capacité de sollicitude et de compréhension seront des éléments importants dans la décision qui suppose que l'Autre soit considéré comme un tiers véritable.

" Si la femme migrante ose dire qu'elle est contaminée à une tante ou une cousine, elle peut se retrouver du jour au lendemain à la rue.

6 COREVIH Ile-de-France Sud, *Femmes vivant avec le VIH aujourd'hui*, Actes du Colloque 11 décembre 2014, p. 26.

Nous avons reçu beaucoup de femmes rejetées par leur famille" Albertine Pabingui de l'association Da Ti Séni

Il n'est pas rare qu'à l'intérieur de la fratrie une sélection soit opérée en fonction des relations de proximité avec les différents mem bres : un frère aîné ou la petite dernière peuvent ne pas être informés. Les proches mis dans le secret pourront être très divers allant d'un ami vivant loin, à une sœur elle-même malade ou encore une vague relation. Pour les femmes migrantes d'origine africaine hébergées par un proche, le simple fait d'avoir un dépliant associatif dans leurs affaires peut révéler ce qu'elles ne veulent pas dire. Parfois même l'obtention d'un titre de séjour (difficile à obtenir en dehors du VIH) peut éveiller les soupçons de l'entourage. Mais même quand les personnes disent n'en parler à personne, il y a toujours au moins une personne dans le secret. C'est alors le besoin de dire qui caractérise les relations électives.

Dans les relations amoureuses et sexuelles, le secret intervient de façon plus contrastée entre la personne avec qui les relations sont régulières, conjoint(e), compagnon ou compagne, qu'elle vive ou non sous le même toit, et les rencontres occasionnelles. Pour la première, c'est presque toujours un devoir de dire qui s'impose dès les premiers jours à l'exception d'une petite minorité (5% dans l'enquête VESPA), alors que pour les secondes le droit de taire l'emporte avec l'adoption de précautions au moment des rapports sexuels. Quand la relation occasionnelle devient une relation stable, l'annonce est alors un moment d'intenses tensions, de peur de l'incompréhension de l'autre et du risque de rejet.

" J'accompagne une femme que j'ai dépistée séropositive, elle l'a révélé à son compagnon, mais il ne l'a pas crue... Elle est venue avec lui pour que je lui fasse un test rapide et lui redire que sa femme est séropositive" Nicole Tsague de AIDES[7]

Quant aux associations, elles occupent une place singulière puisque c'est le seul lieu de la vie sociale où le VIH est connu et évident même si les conditions de la contamination peuvent être maintenues secrètes. Elles peuvent parfois être le seul lieu où les personnes peuvent évoquer leur situation et en retour elles ont une confiance totale en elles. Pour les femmes migrantes d'origine

7 COREVIH Ile-de-France Sud, *Femmes vivant avec le VIH aujourd'hui*, Actes du Colloque 11 décembre 2014, p. 28.

africaine, il n'est pas rare que l'association Ikambere garde dans ses locaux les médicaments et les ordonnances. Mais à quoi s'engagent les participants à un groupe de parole, que recouvre l'anonymat dans les groupes de parole, ne risque-t-il pas d'y avoir des fuites ?

" Les associations sont les seuls lieux où l'on peut en parler ouvertement sans peur des conséquences, mais dehors ce n'est toujours pas possible". Salomé, témoignage

Le lieu de travail est celui où les raisons du secret sont les plus stables et les moins conflictuelles pour les personnes. La peur du licenciement ou de la *"mise au placard"* est ici centrale et conduit à éviter d'en parler. Néanmoins, dans certaines situations de travail, un collègue peut avoir été informé soit par peur des absences, soit du fait des particularités mêmes des conditions de travail. Dans l'enquête VESPA 2003, 5% des personnes interrogées (toutes regroupées dans une des catégories sur les 6 distinguées) n'ont pas réussi à cacher leur séropositivité sur le lieu de travail. Le médecin du travail, bien que tenu par le secret médical, n'est pas toujours informé de la situation sérologique.

En ce qui concerne le milieu médical et hospitalier, les personnes témoignent d'une confiance totale dans le personnel soignant et aucune n'évoque la moindre peur de rupture du secret.

Quant aux diverses institutions comme les banques, les assureurs, les agences immobilières, il semble que les personnes concernées taisent leur statut sérologique par peur de se voir opposer un refus.

Les textes existants sur la protection des personnes sont méconnus et insuffisamment diffusés ou souvent sujets à caution par les personnes les mieux informées (voir à ce sujet les travaux du Conseil national du sida de 1991*, Avis à propos de la convention " Assurances et sida"* et de 1999*, Pour une assurabilité élargie des personnes et une confidentialité renforcée des données de santé).*

Les raisons du maintien du secret sont relativement stables et constituent en quelque sorte un pool qui sera ou non mobilisé en fonction de la relation à l'Autre. On peut néanmoins souligner que le silence sur l'infection à VIH demeure fréquent. Silence total ou diffusion complète sont des situations extrêmes et minoritaires.

Mais dans tous les cas le secret n'est jamais complètement levé, il reste toujours un indicible et un non-dit, en particulier sur les conditions de la contamination.

Ce choix qui est fait de maintenir le secret est le plus souvent assumé et revendiqué bien que certaines personnes, le plus souvent des femmes, se soient enfermées dans le secret et le subissent. Mais pour toutes les personnes, ce silence s'inscrit dans une stratégie qui leur permet de vivre comme tout le monde et non comme quelqu'un dont l'avenir est limité. Car pour la majorité d'entre elles, le dire ne sert à rien actuellement si ce n'est à inquiéter inutilement l'entourage et il sera temps de modifier cette situation quand la maladie se déclarera. C'est aussi vouloir conserver la diversité des liens avec les Autres : continuer à être la femme, l'amant, l'enfant, l'ami et non se voir devenir objet d'attention, de compassion et même de pitié. Le secret est bien une condition nécessaire pour réaménager la vie et " vivre le plus normalement possible » en conservant la diversité des inscriptions identitaires. Le maintien du secret pour les personnes infectées par le VIH est une ressource essentielle pour construire l'espoir et continuer à vivre, un principe central et structurant de leur biographie.

Maintenir ou lever le secret est bien une ressource qui renvoie à des stratégies de vie différentes avec le VIH. Cette ressource demeure essentielle et ne connaît que des modifications marginales avec le temps et les nouveaux traitements. Pour celles qui souhaitent maintenir le secret, la vie doit continuer comme avant même si des inflexions et des changements interviennent. En faire état peut s'inscrire dans le choix d'une vie différente : engagement dans la lutte contre le sida, acceptation de la maladie et du statut de personne malade. Le maintien ou la divulgation du secret sur l'infection à VIH s'inscrit bien dans des stratégies de vie et des réaménagements biographiques et en sont même les conditions essentielles : continuer à vivre normalement le plus longtemps possible, se reconstruire autour de la maladie sida soit comme militant et personne engagée, soit comme personne malade. La sexualité vient cependant rappeler les limites qu'impose le VIH. La reprise ou le maintien d'une activité sexuelle qui est souvent un défi pour les personnes atteintes se heurte aussi au secret quand il s'agit de nouer de nouvelles relations, l'adoption d'une sexualité protégée pouvant révéler le statut sérologique de la personne.

Le groupe a estimé qu'il était difficile de faire des recommandations sur cette question et a repris cette phrase de Salomé lors de la journée du 11 décembre 2014 sur " Femmes vivant avec le VIH" : *" Quand on parle de dire ou ne pas dire, c'est au cas par cas".*

II - B - Consultations et suivi à l'hôpital

Aujourd'hui encore, la plupart des personnes vivant avec le VIH sont suivies à l'hôpital. Le service hospitalier, l'équipe soignante, représentent pour ces patients un contact privilégié et bien souvent c'est une relation au long cours qui s'instaure. Outre tous les aspects techniques du traitement, c'est là que seront évoquées les questions intimes telles que les pratiques sexuelles, l'usage de produits illicites, la procréation, l'information du/des partenaire(s)... C'est dire si confiance et confidentialité sont essentielles.

La confidentialité à l'hôpital doit s'appliquer de la même façon à toutes les maladies et à tous les patients sans exception. L'infection au VIH ne devrait théoriquement pas constituer une exception à cette règle.

En pratique, les patients porteurs du VIH sont beaucoup plus sensibles au manque de confidentialité car cette maladie reste beaucoup moins bien acceptée par la société que d'autres pathologies même graves comme le cancer. Ils sont donc très souvent demandeurs d'une confidentialité renforcée, avec des demandes très spécifiques à cette maladie dont voici quelques exemples :

- par crainte de rencontrer un collègue ou un proche, certains patients sont très réticents à être suivis dans des services où les salles d'attente regroupent uniquement des patients porteurs de VIH ; dans ce contexte, la prise en charge des files actives VIH dans les polycliniques ou des centres de diagnostics multidisciplinaires est beaucoup plus adaptée au respect de la confidentialité et permet d'éviter toute discrimination ;

- lorsqu'il existe des salles d'attente multidisciplinaires, certains ne s'assoient pas sur les chaises attenantes au box de consultation du spécialiste VIH mais devant celles d'un

autre spécialiste. Il faut alors toute la diplomatie du médecin référent VIH pour inviter le patient à entrer dans son box d'un signe de tête sans prononcer son nom tout haut dans une salle pleine ;

- certains patients refusent d'être suivis pour leur VIH par tel médecin, même excellent, du fait d'une spécialité trop évocatrice du VIH (immunologie, maladies infectieuses) ;

- certains patients demandent que l'on enlève le nom de la spécialité sur le tampon du service (" maladies infectieuses" par exemple) et qu'on le remplace par " médecine interne" pour éviter toute suspicion de VIH de la part du médecin du travail ou d'un autre spécialiste. Dans ce contexte, le terme " maladies infectieuses, tropicales et médecine des voyages" est plus adapté que maladies infectieuses seules ou immuno-infectiologie ;

- certains ne comprennent pas pourquoi tout compte rendu à un collègue d'une autre spécialité comporte la mention VIH et demandent que la mention à cette maladie, si elle est bien contrôlée, soit enlevée.

Les équipes qui suivent depuis longtemps des patients porteurs du VIH se sont adaptées pour respecter au mieux ces demandes des patients tout au long de leur parcours de soins et qu'il s'agisse de la prise de rendez-vous, de l'accueil, des prélèvements, personne ne prononce ou ne fait référence au nom du virus. Mais cela persiste dans les équipes moins habituées et des dysfonctionnements continuent à être observés dont voici quelques exemples :

- appel à tue-tête des patients par leur nom en salle d'attente par des médecins dont la spécialité est tout à fait identifiée. Le médecin devrait s'avancer vers son patient et lui parler de façon à ce que les voisins n'entendent pas ;

- persistance de salles d'attente dédiées au VIH ;

- existence dans certains centres d'un niveau de confidentialité différent selon que l'on est une personne 'lambda' ou VIP ;

- résultats biologiques qui trainent dans des bureaux sans être rangés dans des pochettes opaques.

Mais pour conclure, on rappelle que l'application d'une confidentialité globale, s'appliquant aussi bien au VIH qu'aux autres pathologies graves, permettrait souvent d'éviter ces défauts de confidentialité.

Recommandations :

Suggérer aux ARS de rappeler régulièrement aux services hospitaliers les règles impératives de confidentialité :

- **discrétion absolue en salles d'attente comme dans les couloirs des salles d'hospitalisation en évitant d'appeler les patients par leur nom ;**

- **suppression des salles d'attente fléchées VIH ;**

- **organisation matérielle : récupération rapide des télécopies et des textes sur imprimantes partagées ; rangement à l'abri des regards de tous les dossiers médicaux ; utilisation de tampons neutres ; vigilance extrême à l'égard des mails, messages téléphoniques et SMS adressés aux patients ;**

- **respect absolu des procédures de sécurité informatique et changement régulier des codes d'accès pour tous les logiciels de résultats médicaux.**

Au-delà du problème de respect de la confidentialité, le respect du "*secret médical*" appartenant au patient et à lui seul met parfois le médecin face à des problèmes éthiques qui ne trouvent pas de solution idéale.

Prenons par exemple le cas *(vécu)* d'une découverte de séropositivité chez une jeune femme consultant avec son mari dans le cadre d'un bilan pré-grossesse.

Outre le problème de l'annonce pour laquelle il faut pouvoir isoler la patiente alors qu'elle a l'habitude de consulter avec son mari, se pose la question du risque encouru par celui-ci : peut-être est-il séropositif également et nécessite une prise en charge ; s'il ne l'est pas il est "en danger" étant donné qu'ils essaient d'avoir un enfant.

Faut-il persuader la patiente de le lui dire quand on sait qu'elle risque d'être mise à l'écart ou abandonnée tant la séropositivité est source d'exclusion dans certaines populations ?

Le médecin se retrouve face à une décision qui sera, il le sait d'expérience, soit néfaste pour sa patiente, soit dangereuse pour le conjoint. Il n'y a pas de bonne réponse à cette situation et il est très peu probable qu'une "législation" sur le sujet puisse apporter des réponses qui seraient éthiques.

Il nous a paru important de mentionner cet aspect qui reste particulièrement important dans cette affection.

II - C - La délivrance des traitements sensibles en pharmacie d'officine

La préparation des médicaments à l'avance et sous sachet opaque est une pratique assez peu généralisée qui se rencontre surtout dans les régions à forte prévalence (Ile-de-France, PACA).

Il existe plusieurs façons de préparer une commande à l'avance :

- la forme classique : la dépose préalable de l'ordonnance, y compris en boîte aux lettres ;
- le pharmacien suit de très près les ordonnances 'sensibles', commande les médicaments une semaine avant la date prévue et prévient le patient ;
- il existe une application pour Smartphones, " ma pharmacie mobile", gratuite et 'sécurisée' : le patient photocopie son ordonnance et la transmet au pharmacien via l'application ;
- certaines pharmacies ont leur propre site internet, le patient dispose d'un log-in et d'**un mot de passe, et transmet son ordonnance. Les données sont cryptées.**

II - D - Les personnes mineures - Les personnes détenues

Notre groupe de travail n'avait évidemment pas les moyens de faire des enquêtes de terrain. Par ailleurs, il existe déjà des rapports sur ces questions. Le groupe renvoie donc notamment aux travaux suivants :

- *Avis suivi de recommandations sur la garantie du droit au secret des personnes mineures dans le cadre de leur prise en charge médicale* : Conseil national du sida et des hépatites virales, 2015 ;
- Rapports d'activité du Contrôleur général des lieux de privation de liberté.

II - E - L'Assurance maladie

Ameli, le site internet de l'assurance maladie, garantit la confidentialité des dossiers. Et le fait est que tout accès d'un assuré à son compte personnel passe par une procédure assez complexe (mot de passe, questions de contrôle). Nous n'avons pas trouvé de traces de rupture de confidentialité dans ce domaine.

Les arrêts de travail ne semblent pas poser de problème, y compris pour les régimes spéciaux. Les " éléments d'ordre médical" portent généralement sur tel ou tel symptôme sans préciser le diagnostic.

Le dossier médical personnel (appelé également dossier médical 'partagé') DMP.

L'ASIP santé (agence des systèmes d'information partagés de santé) en assure la réalisation et le déploiement. En décembre 2015 le système d'information du dossier médical personnel a été déclaré conforme au référentiel général de sécurité (RGS). Ce référentiel, instauré par décret en 2010, s'applique aux échanges électroniques entre les usagers et les administrations. Il définit les règles permettant aux administrations de garantir un **niveau élevé de sécurité** de leurs systèmes d'information.

Le DMP n'est pas obligatoire. Il est disponible pour tout bénéficiaire de l'assurance maladie ; l'assuré en demande la création soit à l'établissement de santé, soit lors d'une consultation médicale. Il peut contenir : des comptes rendus hospitaliers et radiologiques, des résultats d'analyses biologiques, d'éventuels antécédents et allergies, les actes importants réalisés, les médicaments prescrits et délivrés.

L'assuré peut consulter son DMP via un accès internet et des **codes confidentiels**. Son accès aux professions de santé doit être autorisé par le patient. Le patient peut à tout moment le fermer ou supprimer ou masquer certaines données. A la mi-avril 2016, 577 871 DMP ont été créés.

La médecine du travail n'a pas accès aux DMP. Il existe un dossier médical en santé au travail (DMST) qui a fait l'objet de recommandations de la Haute Autorité de Santé en 2009. Il est tenu par le médecin du travail et est soumis au secret professionnel.

Les médecins conseils de l'assurance maladie ne communiquent pas les données médicales relatives aux mi-temps thérapeutiques ou à l'invalidité (totale ou partielle) aux médecins du travail. Ces derniers connaissent la situation administrative du patient mais lui seul peut en donner les détails médicaux.

Le dossier pharmaceutique (DP).

En théorie le dossier pharmaceutique est ouvert à la demande du patient ou sur proposition du pharmacien. Il peut être ouvert par inadvertance, par une simple manipulation. En principe, le consentement du patient doit être recueilli ; dans le cas contraire, la CNIL peut réagir, elle peut faire des contrôles inopinés mais cela est très rare. Certains patients refusent le dossier pharmaceutique. Ce dossier peut ne pas contenir certaines données, notamment celles sur les multithérapies, ce qui peut poser des problèmes en termes d'interactions ou de contre-indications.

Evoquer ces questions suppose que le dialogue entre patient et pharmacien bénéficie d'une totale discrétion. Or toutes les pharmacies ne sont pas équipées d'un espace de confidentialité (problème du prix du mètre carré).

Quant aux informations contenues sur la carte vitale et leur durée de vie, nous avons interrogé plusieurs pharmaciens et les réponses divergent. Cela semble dû au fait que toutes les officines ne sont pas équipées du même logiciel (il en existe plusieurs sur le marché). Il pourrait aussi y avoir confusion entre les données présentes sur la carte elle-même et les données stockées ailleurs. En théorie, les données sont effacées de l'ordinateur du pharmacien dès que la carte vitale est retirée du lecteur. La carte vitale ne contient aucune donnée sur les médicaments, les données sont toutes stockées chez un " hébergeur de données personnelles de santé" agréé par le ministère de la santé.

Les informations du patient sont stockées sur 2 bases cryptées :

- 1/ l'identité
- 2/ l'historique des dispensations de médicaments

Un système de chiffrement assure le lien entre les 2 bases. La loi du 29/12/2011 établit que ni l'Ordre des Pharmaciens, ni personne,

n'a accès aux données nominatives du dossier pharmaceutique (DP). Seul le médecin de l'hébergeur de données de santé est autorisé par la CNIL à avoir accès au DP.

Recommandation :

Suggérer à l'Ordre des Pharmaciens de rappeler aux officines :

- **la nécessité de recueillir en toute confidentialité le consentement éclairé des patients pour la création d'un dossier pharmaceutique.**

II - F - La recherche

Prévue dans l'article 47 du projet de loi santé, l'ouverture des données de santé regroupées dans une énorme base pour permettre leur exploitation à grande échelle, a suscité des débats au sein du corps médical et des associations de patients. Des risques de non respect du secret médical et de rupture de la confidentialité ont été mis en avant. L'ensemble de l'article 47 a été remanié lors des débats au Parlement et certains alinéas ont été supprimés ou réécrits. Par exemple, l'article L. 1461-5, " Le système national des données de santé ne contient ni les noms et prénoms des personnes (...)", est devenu dans la loi n° 2016-41 du 26 janvier 2016 " Le système national des données de santé ne permet d'accéder ni aux noms ni aux prénoms des personnes (...)".

Depuis l'adoption de la loi, aucune voix ne s'est élevée sur des risques relatifs à la confidentialité et au secret médical.

III. De l'Informatique au Numérique : l'Intrusion de la technologie

Pour commencer quelques chiffres :

Facebook : plus d'un milliard d'abonnés, dont 30 millions en France

Instagram : 400 millions d'utilisateurs

Twitter : 316 millions d'abonnés

Wikipedia : 287 langues ; 27 millions d'articles en accès libre (et gratuit)

Selon Eric Sadin[8] " l'humanité produirait autant d'informations en deux jours qu'elle ne l'a fait en deux millions d'années".

Ensuite, quelques repères en termes d'unités de mesure :

- Début de l'informatique grand public : l'octet
- Premiers micro-ordinateurs : le kilo-octet
- Fin des années '90 : le mégaoctet
- Tournant du millénaire : le gigaoctet
- Aujourd'hui : le téraoctet
- Demain : le petaoctet, l'exaoctet (un milliard de gigaoctets), et après-demain : le zettaoctet et le yottaoctet...

Enfin, quelques 'faits divers' dont la presse s'est fait l'echo :

En 2011, suite au vol des sauvegardes informatiques de TRICARE (organisme américain qui gère l'assurance maladie des militaires), les données personnelles d'environ 5 millions d'assurés ont été piratées.

Quelques mois plus tard, au Howard University Hospital (Washington), un ordinateur portable équipé d'un simple mot de passe a été volé ; il contenait les données médicales non cryptées de 34 000 patients.

8 E. Sadin, *La vie algorithmique, critique de la raison numérique*, L'Echappée, 2015

En 2012, le département de santé de l'état de l'Utah a révélé que des hackers basés en Europe de l'Est, avaient réussi à accéder aux données personnelles d'environ 800 000 personnes.

La même année, un ordinateur a été volé chez le Cancer Care Group (Indiana) ; il contenait les données (noms, adresses, dates de naissance, numéros de couverture médicale, données cliniques) d'environ 55 000 patients.

En avril 2015, le site 'Territorial' du ministère de l'Intérieur français a été piraté par des hackers d'Extrême-Orient.

Toujours en avril 2015, un laboratoire d'analyses a été victime d'un logiciel de chantage ('ransomeware'), à savoir un virus qui verrouille l'accès d'un ordinateur et demande une rançon à la victime, faute de quoi elle ne peut reprendre le contrôle de son ordinateur. Le laboratoire n'a pas cédé au chantage et 15 000 dossiers de patients ont été diffusés sur le 'dark web' (ensemble de réseaux virtuels privés et décentralisés, constitués par des internautes qui se connectent entre eux, c'est le net sous la surface ; les achats s'y font en 'bitcoins', une monnaie virtuelle que l'on peut cependant échanger).

Le centre médical presbytérien de Hollywood a également été victime d'un logiciel de chantage, son activité a été totalement paralysée, la rançon a été payée (40 bitcoins, soit 15 000 Euros). D'après *Le Monde* (24/02 et 7/03 2015) les hôpitaux français ne seraient pas épargnés mais évitent de médiatiser ce type d'incidents.

En septembre 2015, à Londres, une clinique spécialisée dans la santé sexuelle et le traitement du VIH-Sida, le 56 Dean Street, a diffusé par mail une lettre d'information accompagnée par erreur des noms et adresses mail de quelque 780 patients.

En Belgique, des chercheurs de l'Université catholique de Louvain ont récemment découvert que Facebook, par ses 'cookies' (logiciels espions), non seulement suit les utilisateurs partout sur le net même quand ils sont déconnectés du réseau, mais aurait même implanté un 'cookie' sur le site " Your Online Choices", site qui permet à l'utilisateur de désactiver tous les 'cookies' dont il ne veut pas.

Ce mouchard pourrait tracer l'internaute essentiellement européen pendant deux ans, même s'il n'a jamais utilisé Facebook.

En novembre 2015 la société VTech, qui fabrique des jouets connectés, a été victime d'un piratage informatique de sa base de données. C'est ainsi que les données personnelles d'environ 5 millions de comptes de parents et 200 000 comptes d'enfants ont été volées : noms, adresses électroniques, mots de passe, adresses postales. Le service Kid Connect, qui permet une discussion en direct entre un enfant équipé d'une tablette Tech et ses parents, aurait également été attaqué et environ 190 giga-octets de photos, plusieurs mois d'historiques de conversations et quelques enregistrements audio auraient également été volés.

Qu'il s'agisse d'erreurs humaines, d'accidents, de piratages ou de captations, ces quelques exemples montrent que nos données personnelles sont très vulnérables. Il existe un marché noir où ces données sont vendues, parfois à des entités supposées honorables. Il existe même des 'data brokers', sorte de courtiers en données, qui collecteraient pour d'autres, Facebook notamment, les données personnelles de millions d'individus de par le monde.

Par sa rapidité et son volume, l'univers numérique nous pose de nouveaux défis. Nous sommes véritablement à la croisée des chemins, nous vivons un véritable maelström, **la transition numérique.**

III - A - Les systèmes d'information à l'hôpital

La Haute Autorité de Santé (HAS) définit ainsi la confidentialité dans un système d'information : " propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés. Plus couramment, maintien du secret des informations. (...). Les établissements de santé sont tenus de garder la confidentialité des informations qu'ils détiennent sur les personnes hospitalisées (informations médicales, d'état civil, administratives, financières). Néanmoins, l'application de ce principe ne doit pas être une entrave à la continuité et à la sécurité des soins. Ainsi les informations à caractère médical sont réputées avoir été confiées par la personne hospitalisée à l'ensemble de l'équipe qui la prend en charge."

La sécurité des informations à l'hôpital est devenue une règle essentielle.

L'Agence Technique Informatique (ATI) assure la sécurité et le maintien en conditions opérationnelles de l'infrastructure technique du réseau du système d'information de l'AP-HP et de l'ensemble des fonctions informatiques locales du siège. L'agence sécurise ses serveurs hébergeant des logiciels traitant la biologie des patients (ex STARE), les pathologies, actes et traitements (ex PMSI), les bases de données globales sur les patients (DIAMM, NADIS, DOMEVIH) mais aussi les messageries internet du personnel.

Certains serveurs peuvent dépendre des hôpitaux où ils sont localisés, mais ils sont tout autant sécurisés. La sécurité et la confidentialité sont essentielles et effectives grâce à l'utilisation de pseudonymes et mots de passe. De son côté, le patient est informé soit par affichage, soit par un consentement éclairé qu'il doit signer.

L'ATI est une barrière entre les établissements de santé et l'extérieur. En établissant des règles strictes de sécurité, notamment sur la prise de main à distance, la préparation des ordinateurs pour le télétravail, le cryptage des données, etc, l'ATI assure un niveau élevé de sécurité, même si les informaticiens sont formels : **la sécurité absolue n'existe pas.**

Le service informatique de l'AP-HP a élaboré une brochure à la fois détaillée et claire, intitulée " Sécurité de l'information : les règles essentielles" (voir page suivante).

Les systèmes d'information, les dossiers médicaux informatisés et les bases de données spécifiques au VIH.

Notons en préambule que toutes les bases de données sont soumises à autorisation de la Commission nationale Informatique et Libertés (CNIL).

- **Système d'information et dossier médical informatisé :**

ORBIS, en cours de déploiement à l'AP-HP, doit permettre


Sécurité de l'information :
Les règles essentielles
RISQUES D'HÉMORRAGIE DU SYSTÈME DE DONNÉES !!!
RISQUES D'ATTAQUES VIRALES !!!
RISQUES DE RUPTURE DU SECRET MÉDICAL !!!
Ensemble, prenons soin des informations de nos patients et de notre institution !

d'améliorer la sécurité des soins et le quotidien des professionnels. Il modifie les modes d'organisation des services grâce au partage des informations médicales.

C'est le dossier patient unique à l'AP-HP sur les 12 groupes hospitaliers de cette administration.

Le recueil et le traitement des informations ne sont pas soumis à l'obtention d'un consentement éclairé et écrit des patients ; l'information concernant ce recueil est uniquement publiée par voie d'affichage dans les hôpitaux.

ORBIS est accrédité et conforme aux préconisations du dossier médical partagé (sécurité, cryptage, déclaration à la CNIL). L'accès aux données est limité par le profil des utilisateurs : ainsi, les personnels d'accueil qui donnent les rendez-vous aux patients, n'ont pas accès à leurs données médicales mais seulement à leur état civil et coordonnées. **Cependant, des inquiétudes sont formulées par certains personnels - notamment parmi les soignants - qui considèrent que la confidentialité n'est pas totalement assurée dans ORBIS. Certains soignants préfèrent ainsi faire faire leurs propres examens en ville.**

- **Dossier médical informatisé spécifique au VIH : deux exemples, DIAMM et NADIS**

DIAMM est un dossier multi-spécialités sur mesure, modulable et intégré au sein du système d'information hospitalier. Il est utilisé pour gérer les données administratives, médicales, paramédicales, PMSI, comptables, DOMEVIH ; il participe à l'organisation du travail et permet la circulation de l'information.

Le consentement éclairé du patient est nécessaire par écrit. L'accès est soumis à l'attribution d'un compte personnel lié au profil de l'utilisateur. Chaque utilisateur est responsable de son compte.

NADIS est un dossier médical informatisé spécifique au VIH, aux hépatites et aux accidents d'exposition. Il est destiné à améliorer la qualité de la prise en charge des patients, faciliter la communication entre les différents intervenants et constituer une base de données pour la recherche.

Le logiciel NADIS a été créé pour les consultations des médecins : impression des ordonnances de traitements, prescriptions d'examens, rédaction des divers courriers aux médecins traitants et comptes rendus de consultation. Un consentement doit être co-signé par le patient et le médecin.

Chaque intervenant a un profil d'accès spécifique à sa fonction médicale, paramédicale ou administrative, possède un mot de passe et est soumis au secret médical ou professionnel.

Ce logiciel est évolutif en fonction des différentes avancées médicales, grâce à un comité scientifique. Il est connecté avec les laboratoires biologiques des hôpitaux ou de ville, ce qui permet le transfert des données biologiques directement dans NADIS grâce au NIP (numéro d'identité permanent). Les transferts de données sont codés.

Ce logiciel a été développé en 1998 par Fedialis Médica, une filiale du groupe Glaxo. Il est actuellement déployé et utilisé dans 126 centres hospitaliers répartis dans 23 Corevih.

Tous les hôpitaux (en particulier à l'AP-HP) ne l'utilisent pas. La société ABL vient d'en faire l'acquisition suite au retrait du soutien financier du laboratoire VIIV.

L'avenir de NADIS est conditionné par des négociations contractuelles qui devront notamment déterminer son mode de financement.

- **Base de données spécifique au VIH : le DOMEVIH**

Propriété du ministère chargé de la santé, le DOMEVIH a été mis à la disposition des Corevih afin de pouvoir évaluer l'épidémie du VIH en France en recueillant les données médico-épidémiologiques concernant les personnes vivant avec le VIH. Il ne s'agit pas d'un dossier médical informatisé mais d'un système d'information permettant de :

- constituer des bases d'analyses locales, régionales et/ou nationales ;
- renseigner le rapport d'activité demandé par les Agences régionales de santé ;

- réaliser des projets locaux ou régionaux de recherche clinique ou épidémiologique.

L'intégration des données du patient est soumise à son accord écrit : les médecins doivent remettre à chaque patient une lettre d'information sur la finalité et les conditions de mise en œuvre du traitement informatique, sur les destinataires des informations et les modalités d'exercice du droit d'accès, afin qu'il puisse exprimer sous forme écrite un consentement éclairé. Ce consentement doit être co-signé par le patient et le médecin. Le patient peut à tout moment retirer son consentement.

Le recueil, la saisie et la participation à l'analyse médico-épidémiologique des données sont effectués par les Techniciens d'Etudes Cliniques (TECs). Ils sont chargés d'apporter une expertise méthodologique dans l'amélioration de la prise en charge globale des patients vivant avec le VIH dans le cadre du suivi médical et de la recherche clinique au sein des établissements de santé situés sur le territoire du Corevih. Personnels des établissements de santé, les TECs sont soumis au secret professionnel.

Il existe un conseil scientifique pour le DOMEVIH auquel participent l'INSERM, des médecins et des représentants des personnes vivant avec le VIH (TRT-5).

Le ministère de la santé et l'INSERM sont destinataires de l'ensemble des informations recueillies, **à l'exception du nom, prénom, numéro d'identification hospitalier du patient.** Les données collectées alimentent la base de données hospitalières française sur l'infection à VIH (FHDH-ANRS-CO04). Les informations transmises sont cryptées et un numéro d'anonymat est établi automatiquement.

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Hôpital Bicêtre
78 rue du général Leclerc
94275 LE KREMLIN BICETRE CEDEX

DOMEVIH- NADIS
CONSENTEMENT ECRIT DU PATIENT

Le service qui vous accueille bénéficie de systèmes informatisés du dossier médical et participe à des actions et des recherches visant l'amélioration de la prise en charge des patients vivants avec le virus de l'immunodéficience humaine (VIH), le virus de l'hépatite C (VHC) ou le virus de l'hépatite B (VHB) et des personnes exposées accidentellement à un risque viral VIH,VHC,VHB.

Afin de vous assurer une qualité de prise en charge optimale, un suivi adapté et de disposer au mieux de l'ensemble des données médicales qui vous concernent, votre médecin utilise les outils informatiques DOMEVIH et NADIS.
En dehors du service, toute identification directe, tels que vos nom , prénom, adresse et lieu de naissance est impossible afin de garantir votre anonymat.
La gestion de votre dossier médical par DOMEVIH et NADIS se fait dans le strict respect du secret médical et de la plus grande confidentialité, suivant les principes de déontologie médicale et les dispositions de la loi « Informatique et Libertés ». DOMEVIH et NADIS ont reçu l'accord de la commission nationale de l'informatique et des libertés (CNIL).

Vous pouvez refuser que les données vous concernant soient informatisées en le signifiant ci-dessous. Dans tous les cas vous pouvez accéder aux informations contenues dans votre dossier par l'intermédiaire du médecin de votre choix .Vous pouvez également faire modifier ou supprimer ces informations (loi n°78-17, articles 26,27et 34 du 06 janvier 1978).

Je soussigné (e) (nom, prénom) : .....

☐ Autorise
☐ N'autorise pas
La saisie informatique des données de mon dossier médical dans DMI2 et NADIS .

☐ Autorise

☐ N'autorise pas
Le transfert de mon dossier Nadis de l'hôpital de Longjumeau vers l'hôpital Bicêtre

Fait au Kremlin Bicêtre le :

VOTRE SIGNATURE
précédée de « lu et approuvé »

SIGNATURE DU MEDECIN
précédée de « lu et approuvé »

Conclusion

Suite aux préconisations de la CNIL une charte a été élaborée et signée en décembre 2015 : *La Charte du bon usage du système d'information de l'AP-HP* qui vise à assurer une parfaite information des utilisateurs, à sensibiliser les personnels aux exigences de sécurité. Cette charte est désormais annexée au règlement intérieur de l'Assistance Publique-Hôpitaux de Paris (voir synthèse ci-dessous).

Synthèse des principales règles

- Il est de la responsabilité de chaque utilisateur d'adopter un comportement professionnel.
- La configuration initiale du poste de travail doit être respectée.
- La connexion au SI d'équipements non fournis par l'AP-HP est soumise à des règles strictes.
- Les ordinateurs doivent être protégés physiquement.
- Les sessions des ordinateurs doivent être verrouillées en cas d'absence.
- Les informations professionnelles nécessaires à la continuité des activités doivent être sauvegardées sur les répertoires réseaux mis à disposition .
- Les supports amovibles doivent être utilisés avec vigilance.
- Les documents sensibles doivent être rapidement récupérés aux imprimantes.
- Les moyens de télécommunication sont à usage professionnel avant tout.
- Les téléphones portables et smartphones doivent être protégés par un code.
- Les mots de passe doivent respecter les règles de bonnes pratiques de la CNIL.

- L'accès aux informations se fait au regard des nécessités professionnelles pour l'exercice de l'activité de chaque utilisateur.

- Internet et la messagerie électronique sont à usage professionnel avant tout.

- L'accès à Internet avec les équipements de l'AP-HP doit se faire au travers des infrastructures fournies par l'AP-HP.

- L'accès à des sites Internet, initialement bloqués par l'AP-HP, e$t interdit sauf cas dérogatoire.

- La publication depuis le Système d'Information de l'AP-HP doit se faire dans le respect de la loi et des codes de déontologie professionnelle.

- Les outils de communication audiovisuelle par Internet doivent être utilisés pour l'échange d'informations confidentielles avec vigilance.

Recommandations :

Assurer une très large diffusion de la brochure du service informatique de l'AP-HP " Sécurité de l'information : les règles essentielles"

Rappeler aux médecins la nécessité impérative de veiller à la bonne information des patients et s'assurer de leur compréhension avant de recueillir leurs consentements éclairés.

III - B - L'Hôpital numérique

Le programme 'hôpital numérique'

" Afin de rendre les systèmes d'information plus performants, en particulier en termes de qualité et de sécurité des soins, la direction générale de l'offre de soins (DGOS) a lancé, en novembre 2011, le programme hôpital numérique".

Il s'agit d'accompagner les établissements de santé dans leur transformation par les technologies de l'information et de la communication, avec l'appui de l'Agence des Systèmes d'Informations Partagées de santé (ASIP santé) et l'Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux (ANAP).

Lancé en 2011, avec une montée en charge progressive, le programme définit un socle commun de priorités[9], dont la confidentialité est l'un des trois pré-requis.

Le pré-requis de confidentialité impose :

- de disposer d'un système d'authentification individuel, de traçabilité et de gestion des contrôles d'accès permettant **la protection contre les intrusions et la fuite de données médicales ;**

- de disposer d'un moyen d'authentification unique au sein du parc applicatif de la production de soins pour rendre le dispositif utilisable et acceptable ;

- de s'engager à respecter la confidentialité des données médicales ;

- de protéger les données personnelles des utilisateurs. Chaque utilisateur des applications et des systèmes d'information doit disposer d'un compte nominatif lui permettant d'y accéder. Ce compte est strictement personnel et sous la propre responsabilité de l'utilisateur. Celui-ci s'engage à signaler toute violation de son compte personnel ;

- de veiller à ce que les systèmes d'authentification et de traçabilité soient conformes au cadre réglementaire et aux référentiels nationaux.

9 Trois pré-requis : identités - mouvement, fiabilité - disponibilité, confidentialité. Cinq domaines fonctionnels : les résultats d'imagerie, de biologie et d'anatomopathologie, le dossier patient informatisé et interopérable, la prescription électronique, la programmation de ressources et l'agenda du patient, le pilotage médico-économique

Les seuils d'éligibilité au système numérique pour les établissements sont les suivants :

- existence d'une politique de sécurité et d'une analyse des risques formalisée, existence d'une fonction " référent sécurité" ;

- existence d'une charte ou d'un document et d'un processus de diffusion et d'acceptabilité formalisé tenant compte de la réglementation sur la sécurité de l'information en vigueur et des droits et libertés reconnus aux utilisateurs ;

- existence d'une information des patients sur les conditions d'utilisation des données de santé à caractère personnel (livret d'accueil, affichage...).

Ce programme constitue la feuille de route 2012-2017 pour la modernisation des systèmes d'information hospitaliers. L'objectif visé est qu'en 2017 l'ensemble des établissements de santé atteignent un " palier de maturité minimum de leurs systèmes d'information".

L'Agence nationale d'Appui à la Performance des établissements de santé et médico-sociaux (ANAP), a mis en place un site dédié, " mon hôpital numérique" équipé d'une 'boîte à outils' d'aide à l'accès aux pré-requis : un outil d'auto-diagnostic et des fiches pratiques.

Une évaluation des possibilités d'adaptation, menée par la Haute Autorité de Santé, est prévue.

A mi-parcours (2014) environ 800 établissements avaient atteint les 3 pré-requis.

NB : en 2013, selon l'INSEE, la France comptait 3192 établissements de santé.

III - C - Les réseaux sociaux

Les réseaux sociaux constituent une " exposition volontaire et continue des comportements" (Eric Sadin) et la " notion de vie privée mue (...) vers une exposition délibérée de soi (...), "une vie publiée" (op. cit.).

Facebook, Apple, Twitter, Instagram, Netflix, Google, Amazon, tous ces géants ont su séduire des millions de personnes à travers le monde. Des millions de personnes qui ont fait une démarche volontaire pour s'abonner. Mais combien d'entre elles savent quelles en sont les implications en termes de captation d'informations, de calculs de profils, de vente de données... ?

Mark Zuckerberg, le patron de Facebook, ne croit pas à la vie privée ; pour lui, comme pour son homologue de Google, la protection de la vie privée pourrait bien être une " anomalie".

Une étude américaine a montré que 78% des cambrioleurs utilisent Facebook, Twitter et Instagram pour repérer les logements vides l'été. Sur son site, la CNIL recommande de ne pas évoquer lieux et dates de vacances sur Facebook ou Twitter.

Avec les cookies et les algorithmes, tout ce que l'on fait sur la toile laisse des traces et sert à calculer des profils, à une vitesse astronomique.

Dans une interview à Médiapart, en décembre 2013, le président du Conseil national du numérique, Benoît Thieulin a déclaré que " (...) la DGSE en sait moins sur chacun de nous, citoyens français, que Facebook ou Google (...)"

" La vérité, c'est que Google est bien pire que la NSA (...). Le secret de Google, c'est l'utilisation des données privées à des fins commerciales, c'est de l'espionnage privé. Une NSA privée". (Gary Reback, avocat, cité par Frédéric Martel[10]).

10 F. Martel, *Smart, enquête sur les internets*, Stock, 2014

III - D - Je suis connecté, donc je suis : le "quantified self"

Des villes connectées 'smart cities' gérées par les technologies de l'information et de la communication ; des réfrigérateurs qui feraient un inventaire permanent de leur contenu et passeraient commande des produits manquants ; des vêtements qui permettraient de déceler un problème de tension, un problème cardiaque, une chute et pourraient donner l'alerte via un serveur ou un numéro de téléphone... Tout cela a des allures de science-fiction – et pourtant : Frédéric Martel (op. cit.) a décrit des projets de 'smart cities' en devenir dans des pays aussi différents que le Kenya, la Jordanie, la Russie, l'Argentine...

La société française Boldoduc travaille déjà sur des vêtements connectés destinés au marché des seniors ; ces vêtements seraient capables de détecter différents incidents de santé pour les transmettre par wifi à un téléphone ou un ordinateur et pourraient être commercialisés d'ici 5 à 10 ans.

D'ores et déjà bracelets, montres, pèse-personnes, connectés à des applications ou des smartphones, enregistrent nos heures de sommeil, le nombre de pas quotidiens, la tension artérielle, les calories absorbées, les pulsations cardiaques, lesquels sont stockés en temps réel sur des serveurs.

C'est ce que l'on appelle le *quantified self* (quantification de soi, mesure de soi). Toutes ces données personnelles dont on ne sait pas très bien où elles sont stockées ni qui y a accès, sont partageables. Donc accessibles par des tiers.

Dans un rapport de 2014 *(Quantified self, m-santé : le corps est-il un nouvel objet connecté ?)*, la CNIL a fait des recommandations aux internautes " Quelques bonnes pratiques du quantified self" :

- utiliser un pseudonyme sur les plateformes ;
- ne pas automatiser le partage des données vers d'autres services (notamment réseaux sociaux) ;
- effacer ou récupérer les données lorsqu'on n'utilise plus un service ;

- vérifier la fiabilité des informations auprès d'un professionnel en cas d'utilisation d'une application ou d'un capteur dédié à un usage médical.

C'est dire qu'il n'y a aucune garantie de protection de nos données personnelles ni aucune transparence quant à leur éventuelle utilisation.

"Si demain la société qui contrôle l'appli vend ces données à mon insu à ma compagnie d'assurance, celle-ci ne va-t-elle pas en profiter pour augmenter le prix de ma police ? Voire se débarrasser d'un client à risque si les résultats ne lui plaisent pas ?" s'interroge, dans une interview à *Libération* en avril 2014, Benoît Thieulin, président du Conseil national du Numérique.

III - E - La génétique

Les **biobanques** collectent et conservent des échantillons biologiques. En France, une banque de données de ce type doit obligatoirement obtenir l'autorisation de la CNIL et les données doivent être anonymisées. " Pourtant, le système de double chiffrage utilisé n'exclut pas le risque que ces données soient de nouveau identifiables, et donc celui de leur utilisation abusive par les employeurs ou par les assurances".[11]

Les autotests ADN

Aux Etats-Unis, comme en Grande Bretagne, des chaînes de magasins (Walmart, Boots) proposent en vente libre des kits ADN à réaliser soi-même et à renvoyer pour analyse. Il s'agit soit de recherches généalogiques, soit de recherche de paternité, soit encore de recherche de facteurs de risque de certaines maladies. Le prix en est modique : £30 en Grande Bretagne pour une recherche de paternité, environ $99 aux Etats-Unis. La FDA (Food and Drug Administration) s'était opposée à la société 23andMe qui commercialise ces kits et s'est ainsi constitué une banque de plus de 1,5 millions de génomes. Le débat a porté sur la fiabilité des résultats, mais pas sur la confidentialité des données !
Ces tests génétiques dits de convenance personnelle sont interdits

11 Catherine Mary, *Le Monde*, 9 décembre 2015

en France. Mais on peut les commander sur Amazon... Et les kits vendus par Boots en Grande Bretagne sont envoyés aux Etats-Unis pour analyse.

III - F - Les risques, les dérives possibles " à l'insu de mon plein gré"

Alors que l'on parle de démocratie participative et de transparence, les utilisateurs ne sont pas consultés sur la question numérique et l'utilisation de leurs données personnelles. On peut même poser l'hypothèse que bon nombre d'entre eux n'en sont absolument pas conscients. Il n'y a pas de consentement éclairé, ni même de consentement tout court pour la collecte et l'utilisation commerciale des données recueillies. Qui lit jusqu'au bout sur telle ou telle page les 'mises en garde' sur les cookies, ou les 'conditions générales d'utilisation' ?
Ensuite, par le biais des 'cookies' et des algorithmes, se développent le fichage et le croisement des données. Goûts culturels, habitudes de consommation, mais aussi préférences sexuelles, état de santé - passé, actuel ou à venir -, tout est analysé, stocké, répertorié, revendu, dès lors qu'on touche au net.

Le "Cloud"

Le 'cloud computing' (en français informatique en nuage ou informatique dématérialisée) c'est la délocalisation de l'infrastructure informatique, l'accès à la puissance de calcul et de stockage de serveurs distants. La connexion entre les postes et les serveurs passe par les réseaux internet, avec des risques accrus de piratages et de violation de confidentialité.

Les règles de sécurité et même de gestion du cloud sont assez floues. Certains géants du web, dont les serveurs sont situés aux Etats Unis, sont soumis au Patriot Act qui permet au gouvernement américain d'accéder à tout fichier 'suspect'. Apple et Dropbox, pour ne citer que ces deux sociétés, chiffrent les données stockées dans leur nuage, mais pourraient posséder les clés de chiffrement et donc accéder aux données, même chiffrées. Qui peut dire comment ses données personnelles sont réparties entre les différents 'data centers' ? Et qui peut dire comment ces données sont utilisées ? Qui contrôle ?

Marc Dugain et Christophe Labbé[12] dans leur enquête alarmante sur le numérique, décrivent ainsi le 'cloud' : " Pour parachever le cauchemar (...) on est en train de nous déposséder de notre mémoire, en nous poussant à l'externaliser, à la confier aux machines. (...) L'iCloud d'Apple permet en se connectant d'accéder, en un seul clic, à sa mémoire numérique délocalisée dans un serveur. Les informations familiales, sentimentales, financières ou médicales, parfois les plus intimes donc, sont ainsi confiées à d'autres, sans aucune garantie réelle sur l'usage qui pourrait en être fait."

Dans une interview à Médiapart en 2013, Benoît Thieulin résumait ainsi la situation : " (...) Mais les faits sont là : potentiellement nous pouvons basculer dans une société de surveillance totale où elle devient la règle, et non plus l'exception".

III - G - Les garde-fous, les lanceurs d'alerte

Il en existe de différentes sortes, publiques et privées :

- Le **Forum d'Avignon** est un 'think tank' qui travaille notamment sur une 'déclaration universelle des droits de l'homme numérique'. Autre 'think tank', la **FING** (fondation internet nouvelle génération) aide les entreprises et les institutions à anticiper les mutations du numérique ; entre autres travaux, elle a recensé dans son " Cahier d'exploration " Self Data" 10 défis à relever pour les années à venir, dont 'maîtriser ses identités numériques et ses données personnelles'".

- Un site appelé **la Quadrature du net** s'inquiète de la mise à mal de la vie privée sur le net : " La protection de la vie privée est un droit fondamental garanti par la Déclaration universelle des droits de l'Homme (...). Or, de nombreux acteurs ont aujourd'hui intérêt à voir assouplie la protection de ce droit fondamental, afin d'augmenter la surveillance des citoyens ou de tirer profit des informations les concernant, par leur collecte, leur traitement, leur stockage et leur commerce. Ces pratiques, dangereuses pour nos libertés en ligne et hors ligne, sont particulièrement répandues sur Internet".

12 M. Dugain, C. Labbé, *L'Homme nu : La dictature invisible du numérique*, Robert Laffont et Plon, 2016

- **La Commission Nationale Informatique et Libertés.** La CNIL élabore depuis longtemps des fiches pratiques sur des sujets sensibles, comme par exemple " Données de santé : un impératif, la sécurité" à destination des médecins. Parmi les précautions élémentaires (accès protégés, protection des codes personnels, antiviraux, sauvegardes, etc), elle recommande de veiller à ce que le contrat d'assistance et de maintenance du matériel informatique comporte bien une clause de confidentialité "rappelant au fournisseur ses obligations". Cette préconisation est-elle connue des cabinets médicaux ?

  La CNIL a initié en 2013 un collectif, **Educnum**, pour " porter et soutenir des actions visant à promouvoir une véritable 'culture citoyenne du numérique'". En font partie plus de 50 structures issues du monde de l'éducation, de la recherche, de l'économie numérique, de la société civile, etc. Un de ses récents ateliers concernait la maîtrise de la vie privée en ligne. Une attention particulière est portée aux jeunes, avec des 'outils pédagogiques vie privée' en 10 conseils à afficher près des postes informatiques, des lieux de wifi public, des centres de jeunes. Qui connaît ce travail ? Qui a déjà vu l'affiche que nous montrons en page suivante ?

10 conseils de la CNIL pour rester Net sur le web

1 Réfléchis avant de publier !

Sur internet, tout le monde peut voir ce que tu mets en ligne : infos, photos, opinions.

2 Respecte les autres !

Tu es responsable de ce que tu publies en ligne alors modère tes propos sur les réseaux sociaux, forums... Ne fais pas aux autres ce que tu n'aimerais pas que l'on te fasse.

3 Ne dis pas tout !

Donne le minimum d'informations personnelles sur internet. Ne communique ni tes opinions politiques, ni ta religion, ni ton numéro de téléphone...

4 Sécurise tes comptes !

Paramètre toujours tes profils sur les réseaux sociaux afin de rester maître des informations que tu souhaites partager.

5 Crée-toi plusieurs adresses e-mail !

Tu peux utiliser une boîte e-mail pour tes amis et une autre boîte e-mail pour les jeux et les réseaux sociaux.

6 Attention aux photos et aux vidéos !

Ne publie pas de photos gênantes de tes amis ou de toi-même car leur diffusion est incontrôlable.

7 Utilise un pseudonyme !

Seuls tes amis et ta famille sauront qu'il s'agit de toi.

8 Attention aux mots de passe !

Ne les communique à personne et choisis-les un peu compliqués : ni ta date ni ton surnom !

9 Fais le ménage dans tes historiques !

Efface régulièrement tes historiques de navigation et pense à utiliser la navigation privée si tu utilises un ordinateur qui n'est pas le tien.

10 Vérifie tes traces !

Tape régulièrement ton nom dans un moteur de recherche pour découvrir quelles informations te concernant circulent sur internet.

CNIL
Commission Nationale de l'Informatique et des Libertés

Retrouvez d'autres conseils et astuces sur www.cnil.fr et sur www.educnum.fr ! #EducNum

Dans ses Enjeux 2015-2, " la protection des données, clé de voûte de l'innovation", elle note que les révélations de Snowden ont coûté 22 milliards de dollars en pertes aux sociétés américaines. La CNIL considère donc que la protection optimale des données personnelles constitue un impératif pour les citoyens mais aussi un avantage concurrentiel. Et dans ses Enjeux 2015-3, elle fait une série de propositions visant à redonner aux utilisateurs la maîtrise de leurs données : droit à l'oubli, accès libre et aisé de chacun à ses données personnelles, notification obligatoire des failles.

Un bras de fer avec Facebook

Au terme d'une enquête minutieuse, la CNIL a constaté notamment que :

- Facebook peut, grâce à des 'cookies', suivre la navigation des internautes à leur insu, sur des sites tiers, alors même qu'ils ne disposent aucunement de compte Facebook ;

- Facebook ne recueille pas le consentement exprès des internautes lors de la collecte et du traitement des données relatives à leurs opinions politiques, religieuses, à leur orientation sexuelle ;

- Facebook transfère les données de ses membres aux USA sur la base de Safe Harbor, ce qui n'est plus possible depuis la décision de la Cour de Justice de l'Union Européenne du 6/10/2015. Nous reviendrons sur cette affaire.

En conséquence, la CNIL a en février 2016, mis publiquement en demeure Facebook de se conformer, dans un délai de 3 mois, à la loi informatique et libertés. Faute de mise en conformité avec la loi, des sanctions pourront être prononcées.

Une mise en demeure de Microsoft.

En juillet 2016, " la CNIL met publiquement en demeure Microsoft Corporation de se conformer, dans un délai de trois mois, à la loi Informatique et Libertés".

En effet, suite à différents contrôles en ligne de Windows 10 en avril et juin 2016, la CNIL a constaté une collecte excessive de données et le suivi de la navigation des utilisateurs sans leur consentement. L'enquête a également montré la persistance de transferts internationaux sur la base du Safe Harbor, ce qui n'est plus possible depuis la décision de la Cour de Justice de l'Union Européenne d'octobre 2015. **Elle demande donc à Microsoft de cesser ces pratiques et de mieux assurer la sécurité et la confidentialité des données des utilisateurs. Faute de mise en conformité avec la loi, des sanctions pourraient être prononcées.**

Il s'agit maintenant de savoir si la CNIL a les moyens de faire appliquer ces décisions...

Le Projet de Loi numérique

Le chapitre II, en son article 26, énonce que " Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant (...)" et ajoute cet article à la loi informatique et libertés. L'article 29 " vise à élargir les missions de la CNIL. Elle jouera dorénavant un rôle plus en amont en soutenant le développement des technologies respectueuses de la vie privée, c'est-à-dire en développant la protection intégrée de la vie privée dès la conception (" Privacy by Design") et en accompagnant davantage les responsables de traitement. Le but est également de renforcer son rôle auprès des pouvoirs publics en clarifiant les cas de saisine obligatoire sur les projets de loi et de décret. Enfin, elle pourra conduire une réflexion sur les problèmes éthiques et les questions de société soulevées par l'évolution des technologies". L'article 33 réforme les procédures et délais de sanctions de la CNIL.

Cependant, les moyens dévolus à la CNIL pour assurer ses missions présentes et surtout celles à venir ne sont pas évoqués.

L'article 34 sanctuarise en quelque sorte le secret des correspondances.

Ce projet de loi a fait l'objet de 840 amendements et a été voté en première lecture à l'Assemblée nationale le 26 janvier 2016. Le Sénat prévoyait de l'examiner courant avril...

Et l'Europe dans tout ça ?

Le Parlement européen a voté dès 1995 une directive sur la protection des données à caractère personnel. Elle interdit notamment le traitement des données sur l'origine raciale ou ethnique, les convictions religieuses ou philosophiques, les données relatives à la santé et la vie sexuelle. En 2002, une directive *(2002/58)* a été votée sur la protection des données dans le secteur des communications électroniques ; elle évoque notamment la confidentialité des communications et le consentement des utilisateurs dans de nombreux cas... Et encore en 2014 une directive sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Sa mise en œuvre semble laborieuse ; la transposition d'une directive met environ 5 ans à être réalisée...

La European Union Agency for Network and Information Security, ENISA, existe depuis 2004. C'est un centre d'expertise dont le rôle est d'aider les Etats membres, les institutions européennes et les entreprises, à résoudre les problèmes de sécurité des réseaux et de l'information. Cette agence semble très discrète.

Selon Frédéric Martel, certaines associations d'apparence rassurantes seraient indirectement financées par les géants du net ou les équipementiers télécoms : European Digital Media Association, Industry Coalition for Data Protection, Digital Europe.

Le mois européen de la cybersécurité en octobre 2015 a eu peu d'echos...

Safe Harbor

Il s'agit d'un ensemble de principes de protection des données personnelles, publié par le Département du Commerce américain et auquel les entreprises établies aux Etats-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union Européenne.

" En 2000, la Commission européenne avait constaté que les Etats-Unis assurent un niveau de protection suffisant des données à caractère personnel européens transférés." (CNIL). Safe Harbor était donc validé.

Mais début octobre 2015, la Cour de Justice de l'Union européenne invalidait Safe Harbor.

L'affaire avait débuté lorsqu'un étudiant autrichien avait porté plainte contre Facebook après avoir récupéré non sans mal 1222 pages concernant ses données personnelles. Ensuite, il y eut les révélations de Snowden.

La CNIL et ses homologues européens (regroupés en G29) ont rappelé que " la question de la surveillance massive et indiscriminée est au cœur de l'arrêt de la CJUE". Le G29 a demandé aux institutions européennes et aux gouvernements concernés de trouver des solutions juridiques et techniques avant le 31 janvier 2016. La date limite est dépassée, les négociations auraient abouti et il faut maintenant que le Sénat américain se prononce.

Benoît Thieulin, alors président du Conseil national du numérique, a salué la décision de la CJUE, qu'il voit comme un enjeu de souveraineté majeur et aussi " une fenêtre d'opportunité historique pour l'Europe" : (...) " à nous de construire un internet européen avec sa culture, ses règles, ses principes, ses usages (...)".

Il apparaît clairement que nos données personnelles et notre vie privée, objets d'une grande convoitise, doivent être protégées et que nous devons nous les réapproprier ('empowerment'). Les outils juridiques dont nous disposons aujourd'hui face aux géants du net, sont insuffisants[13].

Si Frédéric Martel considère qu'internet " n'est ni bon ni mauvais, en soi. Il dépendra de ce que – passifs ou actifs face aux technologies – nous en ferons, ensemble", Eric Sadin, lui, voit là " un combat politique, éthique et civilisationnel majeur de notre temps." Dugain et Labbé, plus pessimistes, résument ainsi la situation, dans le dernier chapitre de leur enquête (*Le pire est désormais certain*) : "Prévisibilité, sécurité, allongement de la durée de vie contre la transparence absolue, la disparition de la vie privée, la perte de la liberté et de l'esprit critique."

13 Voir à ce sujet *La protection des données personnelles de santé dans le cadre de leur application numérique.* Eve Sobel, master 2 Droit du multimédia et de l'informatique, Paris II, juin 2015.

Recommandations :

Elaboration d'un document clair et ludique alertant sur les risques et dérives possibles et à remettre à tout acheteur d'un ordinateur, d'une tablette tactile ou d'un smartphone. Un peu, en version attractive, comme une notice de médicament.

Militer pour une prise de conscience du grand public et une démarche de consentement éclairé à l'utilisation des données personnelles, assortie d'un droit au refus.

Mieux faire connaître les avis du Conseil national du sida sur la confidentialité.

Assurer aux outils de la CNIL sur la maîtrise de la vie privée une très large diffusion, notamment auprès des jeunes.

Constituer un groupe de travail inter-Corevih, avec des experts en numérique, des médecins, des usagers, sociologues et anthropologues, administratifs de la santé etc...

COREVIH | Ile de France sud

Etablissement siège d'implantation du COREVIH :
Hôpital Henri Mondor
N° FINESS 940100027
51, avenue du Maréchal de Lattre de Tassigny
94010 CRETEIL cedex