Application de la directive relative à la protection des données à caractère personnel à un projet de carte santé

Sophie Louveaux sous la direction de Yves Poullet[*]

Table des matières:

Application de la directive à un projet de cartes santé

Introduction

Le choix de se pencher sur les implications de l'application de la directive relative à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation des données[1] (ci-après directive) à un projet de cartes santé s'explique d'une part, par le caractère potentiellement contraignant de cette norme vis à vis des différentes législations nationales des États membres[2], et, d'autre part, parce que ce texte permet de soulever quelques unes des difficultés rencontrées lors de l'application d'une législation "protection des données" à un projet de ce type.

Il va de soi que ce sont les législations nationales, modifiées en vertu de la directive qui trouveront à s'appliquer aux différents projets nationaux de cartes santé. Toutefois, puisqu'un examen exhaustif de l'application des diverses dispositions nationales en vigueur nous semble, faute de temps, dépasser le cadre de cette étude, nous avons cru bon d'étudier l'application de la directive en tant qu'analyse "test" permettant de souligner certaines des difficultés rencontrés lors de l'application d'un législation "protection des données" à un projet de carte santé[3].

1. La carte santé

La carte à puce s'introduit peu à peu dans le secteur des soins de santé, même si actuellement elle en reste encore fréquemment au stade expérimental. L'originalité de la carte santé réside dans la nature parfois "ultra sensible" des données qu'elle contient et qui soulève diverses questions juridiques notamment en matière de confidentialité et de protection des données à caractère personnel. L'analyse des scénarios des projets existants, révèle des projets qui varient en fonction de ces types d'application de la carte, des données inscrites sur la carte et des intervenants, chaque type de scénario correspondant à une philosophie propre. Après un bref aperçu des différents scénarios, nous tenterons d'analyser certaines des principales difficultés rencontrées lors de l'application de la directive.

1.1. Types d'application

Dans un système de cartes santé, il peut exister différents types de cartes. Ce que l'on appelle la carte santé peut consister soit en une carte "professionnel de la santé", carte détenue par un professionnel de la santé utilisateur du système carte santé, soit en une "carte patient" contenant des données informatiques relatives au patient porteur de la carte[4].

La carte patient peut remplir différentes fonctions: elle peut remplir une fonction purement administrative (identification du patient, accès à un autre dossier, support pour des procédures

administratives générales, confirmation des droits de couverture d'assurance maladie du patient...); soit exercer une fonction médicale. En tant que carte à vocation médicale, la carte peut être envisagée soit comme un véritable dossier médical portable, soit comme un aide-mémoire pour le patient reprenant seulement certaines données clés de son dossier médical, soit comme un dossier "pointer" renvoyant à des informations en réseau, soit comme un moyen d'accès logique à des informations contenues sur une base de données médicales. Par ailleurs la carte à vocation médicale peut être considérée comme une carte patient d'urgence, soit comme un dossier spécialisé ("carte clinique spécialisée") ou général ("carte patient médecine générale")[5].

1.2. Le contenu de la carte

Le contenu de la carte peut être analysé sous différents angles. Il est possible d'opérer une distinction entre le contenu externe et le contenu interne, et de séparer les données administratives et financières des données médicales.

Le contenu externe de la carte est constitué par les données qui apparaissent sur la carte elle-même et qui sont directement lisibles. Le contenu interne ne peut être lu que moyennant recours à un procédé technique (lecteur) avec éventuellement l'introduction d'un code d'accès ou d'une carte d'habilitation à la lecture de la carte.

Les données administratives sont notamment les données relatives à la carte en elle-même (émetteur de la carte, dates d'émission et d'expiration), les données relatives à l'identification du patient, la personne à prévenir en cas d'urgence ou le médecin traitant, l'assurance sociale et éventuellement l'assurance sociale complémentaire. Les données d'ordre financière sont, entre autres, celles relatives au coût des prestations et des médicaments, des remboursements effectuées. Les données médicales sont plus difficiles à qualifier. La directive ne définissant pas ce qu'elle entend par donnée médicale, nous nous baserons sur une définition développé dans le cadre du Conseil de l'Europe : "toutes les données à caractère personnel relatives à l'état physique ou mental passé, actuel ou futur d'une personne y compris toute autre information ayant un lien manifeste avec l'état de santé de cette personne"[6].

1.3. Les intervenants

Un système de carte santé implique l'intervention de plusieurs acteurs présentant des intérêts spécifiques divergents. Cette multiplicité d'intervenants ne va pas sans accroître la complexité des projets et engendrer un certain nombre de questions tenant à la responsabilité des différents interlocuteurs.

Parmi les acteurs impliqués on trouve d'abord les utilisateurs premiers de la carte: les professionnels de santé et les patients. Nous retiendrons essentiellement trois catégories de professionnels : le médecin (généraliste ou spécialiste), le professionnel qui, bien que non médecin peut être amené à utiliser la carte (le pharmacien(ne), le kinésithérapeute, le dentiste), et enfin l'équipe médicale dont le travail évolue autour du médecin et des paramédicaux (l'infirmier(e), l'ambulancier et le personnel administratif).

On trouve ensuite les acteurs qui ont une responsabilité dans la conception, la gestion et le contrôle du système de santé. L'organisme de gestion du système de carte santé[7] (ci-après "le promoteur") est l'organisation qui détermine les objectifs du système et fixe les critères de succès de l'implantation d'un système de carte santé. Il peut s'agir d'un fabricant industriel, des pouvoirs publics, d'un hôpital, des médecins, des mutuelles d'assurance, d'un laboratoire d'analyse médicales, d'un centre de recherche ou une combinaison de ceux-ci. En général, les centres de gestion s'occupent eux-mêmes ou en sous-traitance de l'allocation des cartes et des moyens d'y accéder en lecture et en écriture et du développement du système permettant aux personnes habilitées d'accéder au système.

Enfin, il peut exister des intervenants qui jouent un rôle périphérique au système, soit par la fourniture d'équipements et de services (fabricants de carte, d'équipements ou de systèmes associés, laboratoires privés d'analyse médicale, compagnies pharmaceutiques...), soit par l'intérêt spécifique qu'ils portent au dossier médical (employeurs, assurances, institutions de recherche médicale, écoles, autorités judiciaires...).

2. Application de la directive

2.1 Identification des concepts

2.1.1. Identification des données

Selon l'article 2 a) de la directive est considérée comme donnée à caractère personnel, "toute information concernant une personne physique identifié ou identifiable ("personne concernée"); est réputée identifiable une personne qui peut être identifiée directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale".

Sont considérées comme données personnelles uniquement les données qui sont relatives à une personne physique[8].

Quel que soit le type d'application de la carte santé (carte administrative, d'urgence, médicale spécialisée...) elle contient des données à caractère personnel puisque des données d'identification du porteur sont toujours présentes, soit sur l'extérieur de la carte, soit dans son contenu interne. La simple référence à un numéro d'identification peut être considérée comme une donnée à caractère personnel puisqu'elle permet l'identification ne fut-ce que indirecte de la personne concernée.

Des catégories particulières de données sont par ailleurs identifiées dans le texte de la directive. Il s'agit "des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle"[9]. Ces données, dites "sensibles", bénéficient d'un régime protecteur spécifique énoncé à l'article 8 de la directive.

Toute donnée médicale relative à la santé de personne concernée, qu'elle soit relative à l'état antérieur, actuel, ou futur de sa santé physique ou psychique est classée comme donnée sensible.

Les données d'identification et les données administratives contenues sur la carte ne tombent pas *a priori* dans ces catégories particulières de données. Toutefois il convient de nuancer cette position. Certaines données qui, à première vue, semblent "purement administratives" peuvent néanmoins être considérées comme des données sensibles[10]. Songeons, par exemple, à une donnée indiquant la résidence d'une personne établie dans un hôpital psychiatrique: il s'agit certes d'une donnée administrative mais qui fournit en même temps une information sur l'état de santé de la personne (psychique en l'occurrence). D'autre part, l'affiliation à une mutuelle ou à une caisse de sécurité sociale (Mutualités Chrétiennes, Caisse des Syndicats Libéraux...) peut révéler une conviction religieuse ou une appartenance politique ou syndicale et être considérée comme une donnée sensible. Enfin même une carte de nature purement administrative ayant pour principal objectif le remboursement des soins auprès des patients, peut contenir des données sensibles. En effet, la référence à la nomenclature des soins servant à évaluer les frais exposés révéleront la nature même des soins et dès lors l'état de santé du patient pour ceux qui sont en mesure de déchiffrer la nomenclature.

2.1.2. Identification des traitements

Le régime de protection mis en place par la directive s'articule autour de la notion de traitement[11]. L'application de la directive à l'égard d'un système de cartes santé implique dès lors une identification des traitements existants.

L'article 2 b de la directive définit le traitement de données à caractère personnel comme : "toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction".

Deux conditions doivent être remplies pour que l'on puisse parler de traitement au sens de la directive.

1deg.. Il faut tout d'abord qu'une opération ou un ensemble d'opérations soient effectuées sur des données à caractère personnel ;

2deg.. Il faut aussi que des procédés automatisés ou non soient employés.

La directive détermine de manière non limitative certaines des opérations tombant dans son champ d'application. De sorte que l'on peut dire qu'à partir du moment où les données sont collectées, toute utilisation[12], en ce compris la collecte elle-même, de celles-ci fait partie intégrante d'un traitement tel que visé par la directive.

Le critère de détermination de l'existence d'un traitement ne découle pas directement de cette définition. C'est pourtant la première difficulté rencontrée en pratique lorsque l'on décide d'appliquer la directive.

Mis à part les cas où il n'existe qu'une seule des opérations décrites dans la définition poursuivant à elle seule une finalité spécifique[13], il faut que les opérations effectuées au moyen de procédés automatisés ou non forment un ensemble. Le critère d'unité est, selon nous, à trouver dans la finalité poursuivie par celui qui met en oeuvre le traitement.

D'après les termes de la directive, l'article 6.1.a, b et c énonce deux principes distincts qui seront développés ultérieurement[14]. Le premier -principe de légitimité- postule que le but poursuivi par la collecte soit déterminé, explicite et légitime et que les données soient traitées de manière loyal et licite et ne soient pas traitées de manière incompatible avec la finalité pour laquelle elles ont été récoltées. Le second -principe de conformité- exige un lien nécessaire et suffisant entre les données utilisées et les finalités pour lesquelles elles sont traitées. Les opérations effectuées sur les données s'apprécient donc en fonction de la finalité pour laquelle elles ont été collectées. Elle y trouvent leur raison d'être et leur justification.

Le critère de la finalité comme fondement de la détermination de l'existence d'un traitement répond parfaitement à la logique de la protection mise en place. De la détermination de la finalité poursuivie découle un grand nombre de conséquences. C'est cette finalité qui permettra le cas échéant de contrôler la légitimité du traitement. Une fois cette finalité légitime déclarée, les données ne peuvent être utilisées pour d'autres buts incompatibles avec celle-ci[15]. C'est encore en fonction de la finalité du traitement qu'un contrôle de la qualité des données utilisées est rendu possible (respect du principe de conformité). La durée de conservation légitime des données s'apprécie également fonction de la finalité[16]. Bref, la finalité est à la base du système de protection mis en place. C'est pourquoi partir du principe que le traitement s'identifie au but qu'il poursuit semble être la voie la plus simple pour garantir une protection efficace. Une fois les différents traitements déterminés en fonction des finalités poursuivies, le responsable peut facilement envisager quelles mesures sont à prendre pour rendre ces traitements conformes à la loi.

La gestion et l'utilisation d'une carte santé implique l'existence d'un certain nombre d'opérations sur des données à caractère personnel, opérations souvent effectuées par des intervenants différents, à des moments et dans des lieux différents. Ainsi les données sont collectées auprès de la personne concernée ou auprès de son médecin traitant; elles sont enregistrées sur la carte soit par le médecin lui-même, soit par le fabricant des cartes ou le promoteur du projet; elles font l'objet d'un accès en lecture ou en écriture en vertu des habilitations existantes. Par ailleurs, les données peuvent être copiées sur une base de données servant de "back-up", utile lors de l'émission d'une nouvelle carte en cas de perte ou de bris de la carte initiale.

Puisque les opérations sont effectuées sur des données à caractère personnel et que des procédés automatisés sont employés l'on peut en déduire qu'il y a bel et bien "traitement" au sens de la directive. En France, la C.N.I.L. a statué dans ce sens " utilisée dans un environnement informatique approprié comme support technique d'informations nominatives, la carte à mémoire constitue indéniablement, au sens de l'article 5 de la loi du 6 janvier 1978[17], un traitement automatisé d'informations nominatives[18]".

La définition de traitement que nous avons retenue considère que toute opération ou ensemble d'opérations poursuivant une même finalité constitue un traitement à part entière. En cernant la notion de traitement par rapport à la finalité poursuivie un nouveau problème se pose: si l'exécution des opérations constitutives du traitement est effectuée par différents participants qui ne sont pas entre eux, dans une relation de responsable de traitement à sous-traitant - les uns faisant du traitement pour le compte des autres - est-il possible de trouver pour chacun d'eux une finalité propre générant un traitement particulier?

D'après nous la carte santé en tant que support d'informations, peut être envisagée comme une base de données en elle-même constituant un traitement à part entière. Base de données "carrefour" à partir de laquelle d'autres traitements vont venir se greffer, soit afin de l'alimenter, soit afin d'y puiser des informations. La carte santé doit être considérée comme un traitement en elle-même; Elle doit également être envisagée comme étant au centre des divers traitements effectués par les acteurs qui gravitent dans le système (par le médecin pour la gestion de sa clientèle et le suivi de ses patients, par l'administration d'un hôpital pour la gestion des malades,...). La carte se nourrit et nourrit divers fichiers extérieurs tels que les fichiers des hopitaux, des médecins et des laboratoires. Ainsi les différents intervenants lors de leur utilisation de la carte, poursuivant une finalité propre, effectueront leur propre traitement utilisant la carte comme source d'information.

A ce titre nous pouvons comparer la carte santé à la Banque-carrefour de la sécurité sociale instaurée en Belgique par la loi du 15 janvier 1990[19] et qui est chargée de conduire, d'organiser et d'autoriser les échanges de données sociales entre les banques de données sociales des institutions de sécurité sociale et entre celles-ci et le Registre national des personnes physiques. La Banque-carrefour est elle-même un traitement au centre des divers traitements effectués par les différentes institutions mentionnées. La comparaison est cependant limitée dans la mesure où la Banque-carrefour n'enregistre pas des données personnelles mais uniquement des références renvoyant aux institutions de sécurité sociale qui possèdent de telles données. Elle ne peut donc être considérée comme effectuant un traitement de données à caractère personnel au sens de la directive.

Puisque, selon nous, l'existence d'un traitement est déterminé en fonction de la finalité poursuivie, lorsque une carte poursuit à elle-même plusieurs finalités (carte d'urgence et carte administrative, par exemple) une seule finalité déclarée suffit-elle pour permettre un contrôle efficace de la conformité des données ? Les données ne pourront être traitées de manière incompatible avec la finalité déclarée. Dans le cas contraire il faut considérer qu'il existe plusieurs traitements. Si l'on estime qu'il y a compatibilité des finalités entre elles, il faudra alors déterminer parmi les différentes finalités poursuivies, celle qui englobe les autres et qui permet un contrôle efficace de la qualité des données. Ainsi, par exemple, l'objectif poursuivi par une carte d'urgence est, d'une part, l'identification du patient lorsque celui-ci ne peut s'exprimer, et d'autre part, de fournir les

informations de base nécessaires comme support d'une décision médicale permettant d'agir dans l'urgence. La pertinence des données inscrites sur la carte s'évalue en fonction de cette finalité déclarée. S'il peut être pertinent de connaître le groupe sanguin, les allergies et la pathologie spécifiques du patient. Par contre, il n'est pas forcément pertinent d'inclure sur la carte toutes les données relatives au suivi médical du patient. Cette dernière information pourrait toutefois être jugée comme une donnée pertinente sur une carte patient médecine générale.

2.1.3. Identification des responsables de traitement.

L'article 2d désigne le responsable du traitement comme étant "la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités du traitement sont déterminées par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire".

Le responsable du traitement est la personne responsable des choix qui président à la définition et à la mise en oeuvre des traitements et non les personnes qui procèdent aux opérations de traitement conformément aux instructions du responsable. C'est pour cette raison qu'il est précisé que le responsable définit "les finalités"[20]. Nous pouvons par contre nous interroger sur ce que la directive entend par "les moyens du traitement". S'agit-il des moyens techniques et matériels de mise en oeuvre du traitement ou des moyens organisationnels qui concourent à la réalisation de sa finalité ?

Page suivante

Notes

[*] Nous remercions Marie-Hélène BOULANGER pour sa relecture et ses précieux commentaires

[1]Directive européenne relative à la protection de données à caractère personnel et à la libre circulation des données adopté le 24 octobre 1995, *J.O.,* 23.11.95, ndeg. L 281/31

[2]En vertu de l'article 32 de la directive les États membres sont tenus de mettre en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la directive et ceci à l'issue d'une période de trois ans. Passé le délai de mise en application, si un État membre ne s'est pas conformé à la directive, ou ne s'y est pas conformé de manière adéquate, les individus pourront se prévaloir devant les tribunaux nationaux des dispositions claires, précises et inconditionnelles énoncées dans la directive (principe de l'effet direct des directives européennes, voir notamment C.J.C.E., 5 avril 1979, (Ministère public contre Ratti), 148/78, Rec. CJCE, 1979, p.1629).

[3] Nous tenons à préciser que l'analyse se fonde uniquement sur notre interprétation propre du texte de la directive, la Cour de Justice des Communautés européennes, dans le cadre de ses pouvoirs d'interprétation, pouvant toutefois adopter une position divergente.

[4] Nous n'envisagerons la carte du professionnel que dans la mesure où elle permet l'accès aux données contenus sur le carte d'un patient (cfr. infra l'accès qualifié dans Confidentialité et sécurité des traitements)

[5] Cfr. à ce propos la classification des cartes patients effectuée par Dominique Dieng dans le cadre de AIM D.G. XIII "Eurocards" concerted action/WG5 *(inédit)*

[6] Cfr. la définition de donnée médicale adoptée par le groupe de travail ndeg.12 dans le groupe de projet sur la protection des données (CJ-PD) du Conseil de l'Europe, Strasbourg, 1992. L'article 7 de la loi belge relative à la protection de la vie privée à l'égard de traitements de données à caractère personnel du 8.12.1992, *M.B.*, 18.03.93, 5801, adopte une définition semblable en excluant expressément les données "purement administratives ou comptables relatives aux traitements ou aux soins médicaux".

[7] "PCS Customer" selon le Glossary on Health Cards établi par le WG 2 du projet AIM D.G.XIII "Eurocards" concerted action, 03.02.95 et défini comme étant "the organisation that determines the objectives of the system and sets the criteria for the success of a patient card system implementation".

[8] Certaines législations nationales étendent la protection accordée également aux personnes morales; c'est le cas, par exemple, de la loi luxembourgeoise (article 1), danoise (article 1.1) et autrichienne (article 3.2).

[9] Article 8.1.

[10]Cfr. à ce propos LAFFINEUR Jacques, Réflexions sur la protection des données médicales dans le cadre de la Banque-carrefour de la sécurité sociale, *DCCR*, ndeg.26, 1995

[11] Article 1.1. de la directive

[12] Au sens large du terme, "utilisation" des données est d'ailleurs reprise comme telle dans la liste des opérations.

[13] Lorsqu'une société de mailing, par exemple, vend à une entreprise les fichiers qu'elle a élaborés, la communication constitue en elle-même une finalité spécifique

[14] Sur ces distinctions cfr. Th. LEONARD et Y. POULLET, "Les libertés comme fondement de la protection des données nominatives", in F. RIGAUX, *La vie privée une liberté parmi les autres ?,* Travaux de la Faculté de droit de Namur ndeg.17, Bruxelles, Larcier, 1992, p. 232 et svtes, spéc. ndeg.35 et svts.

[15] Article 6.1.b

[16] Cfr. Article 6.1.e. La durée de conservation des données à caractère personnel est limitée dans la plupart des législations de protection des données par la reconnaissance d'un droit à l'oubli à l'égard de la personne concernée par les données (voir par exemple l'article 5 e de la Convention ndeg.108 du Conseil de l'Europe qui dispose que les données ne peuvent être conservées que "pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées").

[17] Loi française du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO du 25 janvier 1978.

[18] Cité dans Sophie VULLIET-TAVERNIER, *Revue d'Informatique hospitalière,* Janv./Mars, 1988 et cfr. en ce sens la délibération ndeg.87-91 du 15 septembre 1987 portant avis sur la projet de décision du directeur du Centre Hospitalier de Saint Nazaire concernant l'expérimentation de cartes à mémoire hospitalières; la délibération ndeg.95.002 du 10 janvier 1995 portant avis sur l'expérimentation de cartes à mémoire medico-administratives afin d'améliorer la communication entre professionnels de la santé au service des malades (Santal 2)

[19] *M.B.*, 22 février 1990

[20] Exposé des motifs COM (92) 422 final - SYN 287, p. 10.

 ISSN 1201-7302
