FACULTES UNIVERSITAIRES NOTRE DAME DE LA PAIX DE NAMUR

FUNDP

Faculté de droit.

Master complémentaire en droit
des Technologies de l'Information et de la Communication.

BELGIQUE

SUJET : «LES IMPLICATIONS JURIDIQUES DE LA DISTRIBUTION AUTOMATISEE DES MEDICAMENTS SUR LES LIBERTES FONDAMENTALES DES TRAVAILLEURS ET DES PATIENTS».

Par: *MBUNGU TSENDE Liévin*

Mémoire présenté pour l'obtention du Diplôme de Master complémentaire en droit des Technologies de l'Information et de la Communication.

Encadreurs : Cécile de TERWANGNE, Professeur
Jean HERVEG, Assistant

Année académique 2011-2012

LISTE D'ABREVIATIONS

ADN	Acide Désoxyribonucléique
A.R.	Arrêté royal
Art.	Article
CCT	Convention collective de travail
CEDH	Convention européenne des droits de l'homme
CNIL	Commission Nationale de l'Informatique et des Libertés
Cour EDH	Cour européenne des droits de l'homme
CuSL	Cliniques universitaires Saint-Luc
Éd.	Édition
INAMI	Institut National d'Assurance Maladie - Invalidité
J.O.C.E.	Journal officiel des communautés européennes
J.O.U.E.	Journal officiel de l'Union européenne
M.B.	Moniteur Belge
TSBag	*Time stamp bag*

INTRODUCTION

La distribution automatisée des médicaments s'impose de plus en plus dans les hôpitaux comme solution idéale à la prescription électronique des médicaments aux patients, mais aussi à la gestion intelligente et efficace de certains produits dangereux comme les stupéfiants.

La ''prescription'' désigne « le document par lequel le prescripteur prescrit un ou plusieurs médicaments destinés à un patient déterminé »[1]. Elle a, par le passé, obéi à un environnement visible et matériel. Elle devait, en effet, passer par une ordonnance-papier signée et datée par le médecin ou le praticien de l'art dentaire[2]. De nos jours, cette forme de prescription a, en droit belge, fait l'objet d'une attention particulière de la part du législateur qui lui a fait profiter des opportunités qu'offrent les technologies de l'information et de la communication (TIC) en décidant que « pour son utilisation dans les hôpitaux, les prescriptions du médecin et du praticien de l'art dentaire peuvent être remplacées par un document électronique, dans la mesure où ce document électronique remplit les conditions… »[3].

La prescription que vise la disposition précédente n'est plus matérielle, mais électronique ou virtuelle, elle fait appel à des procédés électroniques. Pour accorder la pratique au niveau de l'évolution de la législation, les hôpitaux s'obligent d'adopter des dispositifs informatisés ou automatisés auxquels le prescripteur peut ordonner de délivrer telle quantité précise de tel médicament précis au profit de tel patient précis. Cette distribution automatisée des médicaments offre l'avantage de ne mettre à la disposition de l'administrateur des soins que le produit et la quantité spécifiés par le prescripteur pour un malade déterminé, mais aussi de permettre le traçage des opérations effectuées par les utilisateurs[4] en vue d'un contrôle et d'une gestion efficaces des médicaments dont les stupéfiants.

Il va donc sans dire que les accès à ces dispositifs informatisés doivent être contrôlés et réservés aux seules personnes autorisées. Pour y parvenir, il est souvent fait recours à des processus intelligents d'identification, de reconnaissance ou d'authentification utilisant un login, un mot de passe, un identifiant, un code, une carte à puce, un badge,… Dans ce sens, « La technologie la plus en vogue à l'heure actuelle est l'identification biométrique. Ce procédé vérifie les empreintes digitales, les iris et les rétines, les réseaux vasculaires ou encore les traits de visage….En effet, l'utilisation des produits de contrôle d'accès ne se résume pas uniquement à autoriser, restreindre ou contrôler les entrées et sorties de personnes physiques au sein d'un immeuble ou d'une zone sensible. Ils peuvent aussi servir à sécuriser l'accès à un système d'informations ou à un matériel professionnel »[5]. Une base de données gère généralement, de manière centralisée, les empreintes digitales des utilisateurs en donnant indifféremment accès à n'importe laquelle des machines pour y faire les opérations désirées qui répondent cependant au profil de l'utilisateur.

La distribution automatisée des médicaments devient ainsi une meilleure approche pour la gestion intelligente que requièrent les produits dangereux comme les stupéfiants. En effet, s'ils sont d'un soulagement et d'une importance on ne peut plus incontestables pour certains malades, ils posent d'importantes questions de sécurité sanitaire; ils font l'objet d'une plus grande suspicion et appellent une surveillance spéciale à cause des abus dont ils peuvent être à l'origine. Le stupéfiant est « une substance, médicamenteuse ou non, dont l'action sédative,

---

[1]. Art. 1.1°, A.R. du 10 août 2005 fixant les modalités de la prescription à usage humain, *M.B.*, 20 sept. 2005.

[2]. Voy. art. 21, A.R. n° 78 du 10 nov. 1967 relatif à l'exercice des professions des soins de santé. *M.B.*, 14-11-1967.

[3]. Art. 1, al. 1, A.R. réglementant la prescription médicale électronique. *M.B.*, 7 juin 2009.

[4]. Les utilisateurs sont des travailleurs: les médecins, les praticiens de l'art dentaire, les infirmiers, les administrateurs.

[5]. Voy. Easydentic, « La biométrie et les produits de contrôle d'accès ». Disponible à l'adresse http://easydentic.skynetblogs.be/tag/entreprises

analgésique, narcotique et/ou euphorisante provoque à la longue une accoutumance et une pharmadépendance. De ces substances, les principales sont: la morphine, l'opium, la codéine, la tilidine, l'alfentanil, la méthadone et la méthaqualone. Et, dans leur pratique professionnelle, médecins et infirmiers sont appelés à utiliser ces produits, notamment pour le traitement de la douleur, dans le cadre de substitutions,… »[6].

Tant dans sa phase de prescription médicale électronique que dans celle de l'accès à la machine de stockage des médicaments, cette distribution automatisée n'est cependant pas sans inquiétude s'agissant des libertés fondamentales des travailleurs et des patients. Elle est aussi une des traductions de la présence ubiquitaire de l'informatique dans le quotidien de l'homme car, finalement, « sur le lieu de travail, chez soi et dans la vie quotidienne avec le développement du commerce électronique l'informatique a envahi notre vie. Aujourd'hui l'informatique est partout. Ce qui augmente d'autant la possibilité d'utilisation abusive portant atteinte à notre vie privée et nos libertés individuelles »[7]. La distribution automatisée des médicaments soulève donc une profusion de questionnements juridiques nouveaux: comment mettre en pratique la réglementation sur la prescription médicale électronique au sein de l'hôpital sans enfreindre les droits et libertés des travailleurs et des patients? Si les accès aux automates installés imposent le recours aux dispositifs biométriques, comment doivent-ils fonctionner sans attenter aux règles démocratiques? Quelles sont, pour les travailleurs, les conditions auxquelles peut être subordonnée l'introduction de ces nouvelles technologies au sein de l'entreprise? Constituent-elles une menace pour leurs droits fondamentaux? Quels sont les droits auxquels peuvent prétendre les travailleurs-utilisateurs et les patients s'agissant d'une telle technologie,…?

Ces questions pertinentes intéressent la présente réflexion qu'il sied de mener à bon port en analysant certaines normes - le droit belge principalement - qui correspondent aux préoccupations qu'elles soulèvent, mais aussi en nous imprégnant de la réalité par l'analyse du fonctionnement du projet d'armoires à médicaments aux Cliniques universitaires Saint-Luc (CuSL) de Belgique en vue de fonder les affirmations théoriques sur les faits.

En s'attachant à trouver des réponses aux interrogations suscitées par ce nouveau système, il appert bien que la présente réflexion ne manque pas un intérêt certain dans la mesure où elle peut servir de moyen d'évaluation du système tel que conçu par les CuSL, mais aussi et surtout de support ou de guide aux institutions hospitalières désireuses de recourir à un système identique ou semblable et ce, afin de mieux comprendre la complexité juridique d'une solution technologique au centre de l'actualité sans jusqu'alors avoir été suffisamment débattu.

Pour mieux en aborder les différents aspects, la réflexion s'intéresse, en un premier temps, à comprendre ce qu'est ‘'la distribution automatisée des médicaments''. Cet exercice se fait au départ de l'armoire à médicaments (machine *Vannas*) telle qu'elle fonctionne aux CuSL, mais aussi telle que d'autres armoires entendent fonctionner en réseau au sein de ces mêmes Cliniques (*Chapitre premier*). Fort de cette compréhension, la réflexion s'intéresse ensuite à la mise en œuvre des objectifs poursuivis par un tel système (*Chapitre deuxième*). Le cadre juridique auquel doit obéir ce système pour ne pas enfreindre les libertés fondamentales tant des travailleurs que des patients (*Chapitre troisième*) constitue le cœur ou l'objet même de la présente réflexion. Une conclusion propose, enfin, certaines recommandations concrètes à prendre en compte pour le succès du système.

---

[6]. Adrien DELORME et al. « La gestion des stupéfiants ». Disponible à l'adresse http://lickirider.free.fr/ifsi/3eme_ann%E9e/expos%E9s/La_gestion%20des%20stup.ppt

[7]. Marie-Pierre FENOLL-TROUSSEAU et Gérard HAAS, *Internet et protection des données personnelles*, éd. Litec, Paris, 2000, p.1.

CHAPITRE I. COMPRENDRE LA DISTRIBUTION AUTOMATISEE DES MEDICAMENTS AU DEPART DU PROJET DES CuSL[8]

Section I. Contexte factuel et notion

§1. L'armoire à médicaments de type *Vannas* des CuSL

Il existe une armoire à médicaments aux CuSL. Elle n'est utilisée que par les anesthésistes et se trouve dans la salle d'opération ou quartier opératoire (QUO). Il s'agit, en réalité, d'un dispositif informatisé, en forme d'armoire, qui sert à la gestion des stupéfiants.

En effet, les stupéfiants sont des produits à sécuriser à cause de leur dangerosité. Les hôpitaux sont donc tenus de les soumettre à une gestion rigoureuse et stricte. Il est ainsi apparu nécessaire d'organiser leur gestion pour mieux contrôler les utilisations qui en sont faites et éviter ou réduire les abus.

Le fonctionnement du système veut que les stupéfiants soient stockés dans l'armoire à médicaments par les administrateurs que sont les pharmaciens de l'hôpital. L'anesthésiste qui désire y retirer des médicaments ou l'administrateur qui doit approvisionner l'appareil se présente devant la machine. Celle-ci dispose d'un écran qui sert d'interface pour commander toute opération. Il s'agit d'un écran tactile (pas de bouton ni souris) sur lequel toutes les opérations ont lieu en touchant du doigt l'endroit voulu. Si l'écran est noir ou semble éteint, il suffit de le toucher du doigt à n'importe quel endroit afin d'obtenir l'écran de départ. Pour se connecter ou entrer dans le système, on appuie sur entrer. La machine exige, par la suite, que l'anesthésiste ou l'administrateur s'identifie en entrant son code d'utilisateur. L'anesthésiste ou l'administrateur le fait soit en tapant son login (2 lettres + 4 chiffres), soit en scannant le code barre de son badge à partir du scanneur placé sur le côté latéral gauche de la machine. Cette opération réussie donne accès à un lecteur d'empreinte digitale qui apparait sur l'écran et la machine propose la vérification de l'empreinte digitale. L'anesthésiste ou l'administrateur place la pulpe de son pouce ou index ou majeur de sa main gauche ou droite. C'est alors, qu'après authentification par la machine, il voit apparaître l'écran qui lui permet de faire les opérations voulues en suivant les instructions: la sortie de stupéfiants, la restitution ou retour avec défacturation du patient, la restitution ou le retour sans défacturation du patient et, la défacturation du patient sans retour du stupéfiant. Il y a, en outre et, de manière exceptionnelle, une procédure spéciale au cas où le patient est inconnu pour l'anesthésiste, d'une part et, l'approvisionnement de l'armoire ou le retrait des stupéfiants indésirables pour l'administrateur, d'autre part.

§2. Le projet de mieux développer la gestion automatisée des médicaments aux CuSL

Les CuSL veulent davantage développer la gestion automatisée des médicaments dont, particulièrement, les stupéfiants. A ce titre, elles entendent installer 5 autres armoires à médicaments.

L'accès à ces armoires obéit aux mêmes principes que ceux vus ci-dessous et, les opérations y effectuées sont presque identiques à celles décrites au §1. Mais, le développement de ce système répond à des attentes beaucoup plus nobles: il ne s'agit plus seulement d'une gestion contrôlée des médicaments, mais il est aussi question d'une prescription médicale électronique et d'une distribution automatisée de ces médicaments.

---

[8]. L'auteur remercie M. Gery MOLLERS et Mme Chantal DEFLANDRE du service de la sécurité du système d'information des CuSL pour l'avoir encadré pendant son stage d'un mois au sein du service précité et avoir mis à sa disposition les informations relatives au système automatisé de distribution des médicaments.

En outre, leur fonctionnement est en réseau et utilise une base de données qui permet de gérer, de manière centralisée, les informations susceptibles non seulement de donner indifféremment accès aux utilisateurs[9] à n'importe quelle machine, mais aussi d'y mener les opérations désirées qui répondent cependant au profil de l'utilisateur et se conforment aux ordres qui sont transmis électroniquement aux machines par le médecin traitant du patient ou le professionnel de l'art dentaire au travers d'une prescription médicale électronique en faveur du patient. Cela veut dire que ces machines ne mettent à la disposition, par exemple de l'infirmier traitant, que le produit et la quantité spécifiés, pour un temps déterminé, par le prescripteur en faveur d'un malade donné. Elles permettent aussi l'accès non plus aux seuls anesthésistes et administrateurs, mais aussi aux médecins, aux infirmiers et aux praticiens de l'art dentaire. Et, comme pour le système décrit au §1, elles assurent le traçage des opérations y effectuées par les utilisateurs en vue d'un contrôle et d'une gestion efficaces des stupéfiants.

C'est en réalité ici qu'apparait véritablement la distribution automatisée des médicaments, c'est-à-dire, un système informatisé pour prescrire électroniquement les médicaments, les stocker et en automatiser le processus de distribution[10]. Ce système fonctionne, dans l'espèce sous examen, en deux phases intimement liées: l'une, en amont, s'occupe de la prescription médicale et poursuit l'objectif de prescrire électroniquement les médicaments aux patients; l'autre, en aval, s'occupe des accès à l'armoire à médicaments et vise la gestion ainsi que le contrôle efficaces de l'usage qui est fait des médicaments (stupéfiants). Comment atteindre ces objectifs? C'est l'objet de notre deuxième chapitre.

CHAPITRE II. LA MISE EN ŒUVRE DES OBJECTIFS POURSUIVIS PAR LA DISTRIBUTION AUTOMATISEE DES MEDICAMENTS

Section I. Distribution automatisée des médicaments et prescription médicale électronique

§1. Fondement juridique de la prescription médicale électronique

Un arrêté royal du 7 juin 2009 sert de base juridique à la prescription médicale électronique. Il a marqué la fin du règne absolu de la prescription médicale-papier.

En effet, l'article 1e, §1e, al.1e de cet arrêté royal stipule : « pour son utilisation dans les hôpitaux, les prescriptions du médecin compétent et du praticien de l'art dentaire compétent peuvent être remplacées par un document électronique… ».

Ce document électronique doit remplir certaines conditions dont les unes sont des mentions obligatoires (I) et les autres militent pour la sécurité des données (II).

I. Les mentions obligatoires

Le document électronique doit contenir les renseignements suivants[11]: le nom, prénom et l'adresse du prescripteur concerné; le numéro d'identification à l'Institut National d'Assurance Maladie - Invalidité (INAMI) en chiffres et en code-barres, s'il échet; le nom ou la dénomination commune du médicament; le prénom et le nom du patient, la posologie

---

[9]. Les utilisateurs sont des travailleurs: les médecins, les praticiens de l'art dentaire, les infirmiers, les administrateurs du système (pharmaciens), les anesthésistes.

[10]. Pour plus de détails à ce sujet, voy. Louis LEVY, « Stockage et distribution automatisée des médicaments dans l'hôpital Dodoens à Malines ». Disponible à l'adresse http://www.sixi.be/Stockage-et-distribution-automatises-des-medicaments-dans-l-hopital-Dodoens-a-Malines_a166.html

[11] Voy. art.1, §2, A.R. du 7 juin 2009 réglementant la prescription médicale électronique et art. 2, A.R. du 10 août 2005 fixant les modalités de la prescription à usage humain.

journalière du médicament et, s'il échet, la mention précisant que le médicament est destiné à un enfant ou à un nourrisson; la signature datée du prescripteur, et, le cas échéant, la date de délivrance déterminée par lui; la forme d'administration; le dosage unitaire du médicament; la mention du nombre d'unités dans le conditionnement et du nombre de conditionnements, ou la mention de la durée de la thérapie en semaines et/ou jours.

II. Les conditions visant la sécurité de données

Ces conditions sont reprises à l'article 1, §1 et à l'article 2 de l'arrêté royal précité.

En effet, l'article 1, §1 impose que le document électronique :

- mentionne l'identité du médecin ou du praticien de l'art dentaire responsable de la prescription, authentifiée selon la procédure visée à l'article 2, al. 2, 1° (art.1, §1, 1°);
- soit associé, de manière précise, à une date de référence et une heure de référence attribuées soit par la plate-forme eHealth, visée à l'article 2 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth, soit par une autre instance ayant prouvé au Comité de l'assurance de l'Institut national d'assurance maladie-invalidité qu'elle répond aux conditions établies pour les prestataires de service d'horodatage électronique par et en vertu de la loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance (art.1,§1, 2°);
- ne soit modifié de manière imperceptible après la mention de l'identité du médecin ou du praticien de l'art dentaire et après l'association à une date de référence et une heure de référence (art.1,§1,3°);
- soit lu par la voie électronique durant la période mentionnée dans ''l'article 33, § 5, de l'arrêté royal du 31 mai 1885 approuvant les nouvelles instructions pour les médecins, pour les pharmaciens et pour les droguistes''[12] (art.1, §1, 4°).

Par ailleurs, l'article 2 impose la conclusion d'un ''protocole informatique''[13] qui comprend la procédure permettant au médecin ou praticien de l'art dentaire concerné d'authentifier son identité lorsqu'il rédige la prescription ainsi que celle (procédure) dont l'application permet au document électronique de répondre aux conditions visées à l'article 1e, § 1er, 2° et 3°.

§2. La distribution automatisée des médicaments au regard des mentions obligatoires

Tel qu'il fonctionne aujourd'hui, si le système de la machine *vannas* permet d'identifier le nom du patient, son n° de dossier (= n° séjour ou administratif), le login du médecin; de choisir le stupéfiant désiré et la quantité; il ne mentionne pas, par contre, les autres informations exigées par l'arrêté royal précité[14]. Et pourtant, il s'agit d'informations qui apparaissent toujours dans une prescription médicale-papier. Il est important qu'elles soient également visibles et lisibles sur l'écran de commande du système automatisé dès l'identification du patient concerné.

---

[12]. Selon cette disposition, « les registres, les photocopies, les listages informatiques et les supports magnétiques sont conservés pendant dix ans dans l'officine, de manière telle que rien des données stockées ne soit perdu ». Il en découle que le délai de conservation des prescriptions médicales électroniques et des données qu'elles contiennent est fixé à 10 ans.

[13]. Il est signé entre, d'une part, la direction de l'hôpital, le médecin en chef, le pharmacien titulaire ou le pharmacien en chef et le responsable du système informatique et, d'autre part, chaque médecin et praticien de l'art dentaire prescripteur.

[14]. Il s'agit des nom, prénom et adresse du prescripteur concerné, numéro d'identification à l'Institut National d'Assurance Maladie - Invalidité (INAMI) en chiffres et en code-barres, nom ou dénomination commune du médicament, posologie journalière du médicament et mention précisant que le médicament est destiné à un enfant ou à un nourrisson, signature datée du prescripteur, et, le cas échéant, date de délivrance déterminée par lui; forme d'administration, dosage unitaire du médicament, mention du nombre d'unités dans le conditionnement et du nombre de conditionnements, ou mention de la durée de la thérapie en semaines et/ou jours.

Selon l'esprit de l'arrêté précité, le personnel soignant qui, au nom d'un patient précis, accède à l'armoire à médicaments, ne doit pas avoir un choix délibéré du produit désiré, encore moins du dosage unitaire parce que déterminés à l'avance par le prescripteur. Celui-ci précise aussi la date de délivrance du produit, la durée de la thérapie en semaines et/ou jours. Ces exigences cachent le souci de ne donner aucune possibilité de manœuvre quelconque au personnel soignant: il ne peut retirer ni plus ni moins de produits que prescrits; il ne peut accéder aux produits d'un patient déterminé que pour la durée prescrite de la thérapie en semaines et/ou jours.

Il se fait malheureusement que dans le fonctionnement actuel de la *vannas*, le personnel soignant n'est pas limité ni par rapport au choix du produit, ni par rapport à la quantité. Ce qui ne permet pas de respecter scrupuleusement les prescrits de l'arrêté royal précité. Les cinq autres machines que les CuSL entendent installer permettront de résoudre ce problème dans la mesure où la prescription médicale détermine à l'avance le produit et la quantité.

§3. Distribution automatisée au regard des conditions de sécurité des données

I. Par rapport aux conditions de l'article 1, §1

L'arrêté royal précité organise une sécurité orientée vers la non répudiation des données contenues dans la prescription médicale électronique. Pour atteindre cet objectif, l'INAMI propose, conformément à l'article 2 du même arrêté, un « Protocole dans le cadre de la prescription hospitalière électronique ». Ce protocole distingue trois moments importants de ladite sécurité: l'authentification du prescripteur (I.1), la procédure de hachage, enregistrement de la prescription électronique et du hash-code y afférent et logging (I.2) ainsi que l'horodatage et l'enregistrement des TSBags pourvus d'une estampille temporelle et d'une signature électronique (I.3).

I.1. L'authentification de l'identité du prescripteur

L'INAMI[15] laisse l'hôpital fixer les procédures utiles pour garantir l'identification et l'authentification correctes du prescripteur. Il propose néanmoins de choisir entre deux procédures :

1°. Authentification au moyen d'un nom d'utilisateur et d'un mot de passe

Le nom d'utilisateur et le mot de passe sont strictement personnels et non transmissibles. Le mot de passe peut être utilisé une seule fois ou plusieurs fois. Si celui-ci peut être utilisé plusieurs fois, le prescripteur est tenu de le modifier le plus rapidement possible après réception ou du moins au moment de la première utilisation; le prescripteur doit ensuite régulièrement le modifier.

Un mot de passe sécurisé est idéalement composé de 15 signes et comporte au moins 8 signes. Il peut soit être utilisé une fois sur base d'un "challenge" (mot de passe dynamique) chiffré pour chaque utilisation, soit être utilisé plusieurs fois (mot de passe statique). Un mot de passe qui peut être utilisé plusieurs fois, contient des caractères et des symboles alphanumériques placés dans un ordre difficile à déceler. Chaque prescripteur doit veiller à ce que le mot de passe choisi réponde à ces conditions. La responsabilité de chaque prescripteur est engagée lorsqu'un mot de passe est décelé et/ou utilisé de manière illicite.

Il appartient à chaque prescripteur de faire un usage judicieux de son nom d'utilisateur et mot de passe et d'assurer le secret en ce domaine. Chaque prescripteur assume la responsabilité de tout usage approprié ou non de son nom d'utilisateur et mot de passe, en ce compris l'usage

[15]. INAMI, « Protocole dans le cadre de la prescription hospitalière électronique », p.3.

par des tiers. Lorsqu'un utilisateur est au courant de la perte de son nom d'utilisateur et/ou mot de passe ou d'une quelconque utilisation inappropriée de son nom d'utilisateur et/ou mot de passe par des tiers ou lorsqu'il soupçonne une telle perte ou utilisation inappropriée, il doit prendre immédiatement toutes les mesures nécessaires et en informer le conseiller en sécurité de l'information de l'hôpital. Dans les plus brefs délais de la réception de cette communication et dans les limites du raisonnable, tout sera mis en œuvre pour éviter tout abus. Chaque prescripteur continue à assumer la responsabilité de chaque usage légitime de son nom d'utilisateur et /ou de son mot de passe et de chaque usage illégitime suite à négligence de son nom d'utilisateur et /ou de son mot de passe avant l'inactivation du nom d'utilisateur et du mot de passe

2°. authentification au moyen d'une procédure d'authentification plus forte que le nom d'utilisateur / mot de passe, plus précisément au moyen du certificat d'authentification sur la carte d'identité électronique ou d'un autre certificat répondant aux dispositions de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification.

I.2. Procédure de hachage, enregistrement de la prescription électronique et du hash-code y afférent et logging [16]

Au sein de l'hôpital, la prescription médicale électronique est conservée de façon qu'il ne soit plus possible de la modifier ou de la supprimer de manière inaperçue. La procédure de hachage, horodatage, signature électronique et enregistrement du résultat, décrite ci-après, est appliquée à cet effet.

Une procédure de hachage est appliquée à chaque prescription électronique. L'algorithme utilisé est au moins un SHA 256. Le résultat du hachage (hash-code) est calculé sur base du contenu spécifique du fichier ayant fait l'objet du hachage. En d'autres termes, sur base d'un hachage déterminé, il n'y a qu'un seul hash-code qui correspond à un contenu déterminé. Si le contenu d'un fichier est modifié, le hash-code sera différent lors d'un nouveau hachage avec le même algorithme de hachage. Le hash-code original permet également de déterminer si le fichier a été modifié par la suite.

L'hôpital prévoit un système de loggings de sécurité permettant de réaliser un logging de toute création, modification ou destruction de la prescription électronique et du hash-code y afférent ayant fait l'objet d'un horodatage.

Pour l'horodatage des prescriptions électroniques, une banque de données spécifique est créée au sein de chaque hôpital. Après avoir soumis le hash-code à la procédure d'horodatage décrite dans le présent protocole, chaque prescription électronique et le hash-code horodaté y afférent sont enregistrés dans cette banque de données sous forme de fichier spécifique.

Les prescriptions électroniques sont enregistrées dans la banque de données spécifique dans un format KMEHR version 1bis d'un niveau 1 ou 4.

I.3. Pour la procédure d'horodatage et enregistrement des TSBags pourvus d'une estampille temporelle et d'une signature électronique[17] :

Les hash-codes calculés à partir de la prescription électronique sont horodatés par la plate-forme eHealth. Pour éviter une surcharge du service d'horodatage, un horodatage de chaque hash-code de chaque prescription électronique individuelle n'est pas prévu. Cependant,

---

[16]. INAMI, « Protocole dans le cadre de la prescription hospitalière électronique », p.3.

[17]. INAMI, « Protocole dans le cadre de la prescription hospitalière électronique », pp.3-4.

plusieurs hash-codes sont regroupés (dans un *time stamp bag* ou TSBag) et ensuite une seule demande d'horodatage est introduite.

Toutes les cinq minutes, un programme installé au sein de l'hôpital sélectionnera et regroupera dans un TSBag les nouvelles prescriptions électroniques du dépôt provisoire. L'hôpital transmet le TSBag au service d'horodatage de la plate-forme eHealth et demande un horodatage au niveau du TSBag. La plate-forme eHealth attribue ensuite une estampille temporelle et une signature électronique au TSBag. Elle transmet alors à l'hôpital le TSBag pourvu d'une estampille temporelle et d'une signature électronique. Le logiciel de l'hôpital enregistre les hash-codes concernés des prescriptions électroniques, le TSBag, l'estampille temporelle et la signature dans les archives de l'hôpital.

L'hôpital prévoit la possibilité de lecture des prescriptions électroniques pendant une période de 10 ans à compter de leur création.

Le service d'horodatage de la plate-forme eHealth archive également, dans une banque de données créée à cet effet, tous les TSBAgs reçus et les estampilles temporelles délivrées, afin de soutenir les parties concernées en cas de litige.

L'hôpital prévoit la possibilité de consultation des archives et la visualisation des prescriptions électroniques enregistrées. Il est également prévu qu'un extrait puisse être créé, comprenant une sélection de prescriptions électroniques, des TSBags et estampilles temporelles y associés. Le cas échéant, ceux-ci doivent être transmis aux instances de tutelle. Dans l'hypothèse où ceci s'avère impossible, les prescriptions électroniques concernées ne seront pas valides.

Section2. La gestion et le contrôle de l'usage des médicaments

L'objectif ultime visé par le recours à la distribution automatisée des médicaments est d'en rationaliser la gestion et le contrôle.

Qui plus est, s'agissant de médicaments comme les stupéfiants, il s'avère que l'instauration de la distribution automatisée représente un moyen efficace de lutte contre leur mauvaise gestion.

En effet, si, d'une part, les accès au système automatisé de distribution des médicaments sont identifiés et, d'autre part, le dosage unitaire du médicament, la mention du nombre d'unités dans le conditionnement et du nombre de conditionnements, ou la mention de la durée de la thérapie en semaines et/ou jours imposées par l'arrêté royal du 7 juin 2009 sont respectées, il y aura moyen, contrairement à une gestion non automatisée, de savoir qui a accédé aux machines et qui y a pris quoi pour en faire quoi.

Cependant, si le système vanté offre des avantages indéniables, il augure un certain traçage des travailleurs par l'employeur, mais aussi un traitement des données à caractère personnel des travailleurs et des patients qui implique un risque d'attenter à leurs libertés fondamentales, notamment celles relatives au respect du droit à leur vie privée et à la protection de leurs données à caractère personnel. D'où l'érection de certaines limites contre ce système. Notre dernier chapitre y est consacré.

CHAPITRE III. DISTRIBUTION AUTOMATISEE DES MEDICAMENTS AU REGARD DU CADRE JURIDIQUE

La distribution automatisée des médicaments doit fonctionner sans enfreindre les libertés fondamentales des utilisateurs et des patients. La présente étude ne s'intéresse qu'au respect du droit à la vie privée et du droit à la protection des données à caractère personnel de ces derniers. Vu sous cet angle, la distribution automatisée des médicaments doit, s'agissant de la Belgique, obéir à un certain nombre de règles de droit contenues notamment dans les instruments ci-après:

- La loi du 08/12/1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[18];
- L'arrêté royal réglementant la prescription médicale électronique[19];
- La convention collective de travail n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau.

Le propos n'ambitionne pas de tout dire sur ces instruments qui ne seront utilisés que dans un cadre précis en vue de répondre à certaines questions soulevées dans notre introduction. Ces questions sont à l'origine de deux grandes articulations qui composent le présent chapitre:

- L'introduction et l'usage du système automatisé au sein de l'hôpital (section I);
- Les limites au système automatisé de distribution des médicaments (section II).

Section I. L'introduction et l'usage du système automatisé au sein de l'hôpital

Il s'agit des préalables à observer avant l'introduction ou l'utilisation de la distribution automatisée des médicaments au sein de l'hôpital. Ils concernent particulièrement les travailleurs et touchent à la consultation du conseil d'entreprise (§1) et à la formation des travailleurs (§2). D'autres préalables, non spécifiques aux travailleurs, existent également et sont analysés dans le cadre des limites imposées au système automatisé (section II)

§1. La consultation du conseil d'entreprise

L'article 20, alinéa 1° de la loi du 3 juillet 1978 relative aux contrats de travail[20] exige que l'employeur fasse travailler le travailleur, notamment en mettant à sa disposition, s'il y échet et sauf stipulation contraire, l'aide, les instruments et les matières nécessaires à l'accomplissement du travail.

C'est fort de cette disposition que l'hôpital, en tant qu'employeur, peut, s'il le juge nécessaire à l'accomplissement du travail, mettre à la disposition des travailleurs un système automatisé de distribution des médicaments.

Il semble cependant que l'introduction d'une telle technologie de travail au sein de l'entreprise (hôpital) induit une profonde mutation au niveau de l'organisation ou des conditions de travail.

Dans ces conditions, l'employeur n'est pas libre de procéder à l'introduction du dispositif en cause. Car, en effet, lorsqu'il a décidé d'un investissement dans une nouvelle technologie qui a des ''conséquences collectives importantes''[21] en ce qui concerne l'emploi, l'organisation du

---

[18]. *M.B.*, 18 mars 1993.

[19]. *M.B.*, 7 juin 2009.

[20] *M.B.*, 22-08-1978, n°: 1978070303, p. 9277.

[21] Il y a conséquences collectives importantes lorsque 50 % et 10 travailleurs au moins d'une catégorie professionnelle déterminée, sont concernés par l'introduction de la nouvelle technologie au sein de l'entreprise, et ce jusqu'à l'expiration du

travail ou les conditions de travail, il est tenu, au plus tard trois mois avant le début de l'implantation de la nouvelle technologie, d'une part de fournir une information écrite sur la nature de la nouvelle technologie, sur les facteurs qui justifient son introduction ainsi que sur la nature des conséquences sociales qu'elle entraîne et d'autre part, de procéder à une concertation avec les représentants des travailleurs sur les conséquences sociales de l'introduction de la nouvelle technologie[22].

Dans ce même ordre d'idées, le conseil d'entreprise doit donner son avis et formuler toutes suggestions ou objections sur toutes mesures qui pourraient modifier l'organisation du travail, les conditions de travail et le rendement de l'entreprise[23]. Cette exigence est à la base de l'obligation pour l'employeur d'informer le conseil d'entreprise des projets et mesures susceptibles de modifier les circonstances et les conditions dans lesquelles s'exécute le travail dans l'entreprise ou dans une de ses divisions[24].

L'objet et la nature des informations à fournir sont définis par la convention précitée[25].

§2. La formation des travailleurs

Le travailleur a l'obligation d'exécuter personnellement les tâches qui lui sont assignées par l'employeur. Il en découle implicitement un devoir de maîtrise de l'outil de travail. L'introduction d'une nouvelle technologie de travail en général et, d'un système automatisé de distribution des médicaments en particulier, nécessite que les travailleurs s'y adaptent ou apprennent à l'utiliser. Et, ainsi que le remarque Jean-Michel SERVAIS[26], ''comme toujours, en période de transition, certains s'adaptent immédiatement, ou du moins rapidement, aux nouveaux instruments de travail; d'autres prennent plus de temps ou même n'y arrivent pas"**.**

Les travailleurs doivent donc être formés ou initiés à l'utilisation du nouveau matériel. L'article 8 de la CCT n°9 précitée mentionne d'ailleurs l'importance de la formation et de la réadaptation professionnelles.

---

délai indiqué par l'employeur dans le cadre de son obligation d'information ou à défaut, jusqu'a la mise en œuvre effective de la nouvelle technologie. Les 50 % et les 10 travailleurs ne sont pas calculés sur la base de chaque catégorie professionnelle envisagée isolément mais sur l'ensemble des catégories professionnelles dans lesquelles intervient une modification de l'emploi, de l'organisation du travail ou des conditions de travail résultant de l'introduction de la nouvelle technologie, lorsque l'ensemble de ces catégories professionnelles comprend moins de 100 travailleurs. Voy. Art. 2, §2 CCT n° 39 du 13 décembre 1983 concernant l'information et la concertation sur les conséquences sociales de l'introduction des nouvelles technologies (ratifiée par l'AR du 25 janvier 1984 (articles 1 à 7), *M.B.*, 8 février 1984).

[22]. Voy. art. 2, al. 1 CCT n° 39 du 13 déc. 1983 concernant l'information et la concertation sur les conséquences sociales de l'introduction des nouvelles technologies.

[23]. Voy. art. 15 de la loi du 20 sept 1948 portant organisation de l'économie (*M.B.*, 27-09-1948);

[24]. Voy. art. 10 CCT n°9 du 9 mars 1972 coordonnant les accords nationaux et les conventions collectives de travail relatifs aux conseils d'entreprise conclus au sein du Conseil national du Travail, modifiée par les conventions collectives de travail n° 15 du 25 juill. 1974, n° 34 du 27 févr. 1981, n° 37 du 27 nov. 1981, n° 9*bis* du 29 oct. 1991 et n° 9*ter* du 27 févr. 2008 (ratifiées par les AR des 12 sept. 1972, 5 sept. 1974, 21 sept. 1981, 9 déc. 1981, 17 déc. 1991 et 5 juin 2008, parus au *M.B.* des 25 nov. 1972, 9 oct. 1974, 6 oct. 1981, 6 janv. 1982, 10 janv. 1992 et 18 juin 2008).

[25]. Voy. art. 3. Les informations et consultations doivent être préalables aux décisions; elles doivent permettre au conseil d'entreprise de procéder, en connaissance de cause, à des échanges de vues au cours desquels les membres pourront formuler leurs avis, suggestions ou objections; lorsqu'elles sont données par écrit, les informations sont complétées par un commentaire oral du chef d'entreprise ou de son délégué; pour assurer la continuité du dialogue au sein du conseil d'entreprise, le chef d'entreprise indique, soit immédiatement, soit au cours de la réunion suivante, la suite qu'il entend donner ou qu'il a donnée aux avis, suggestions ou objections formulés conformément à l'alinéa premier de cet article; il ne doit pas être porté préjudice aux dispositions déjà prévues sur le même objet, lorsqu'elles sont plus avantageuses pour les travailleurs.

[26]. Jean-Michel SERVAIS, « Nouvelles technologies et fragmentations des relations de travail », in *Revue tunisienne de droit social*, n°12, 2007, pp. 30-53.

Section II. Les limites au système automatisé de distribution des médicaments

§1. Préalable lié au pouvoir de contrôle de l'employeur sur ses travailleurs

Le système automatisé de distribution des médicaments est un outil de travail que l'hôpital met à la disposition du personnel soignant conformément à la loi qui oblige l''employeur « de faire travailler le travailleur […], notamment en mettant à sa disposition, s'il y échet et sauf stipulation contraire, l'aide, les instruments et les matières nécessaires à l'accomplissement du travail »[27]. Il importe donc que l'employeur qui en est le propriétaire en contrôle l'utilisation.

Le pouvoir de contrôle des travailleurs par l'employeur est une caractéristique ou une conséquence qui découle des obligations réciproques des parties au contrat de travail. Il est, en effet, logique que l'employeur qui engage et donne du travail à l'employé puisse en contrôler tant l'exécution que l'utilisation des instruments de travail par le travailleur[28].

En droit belge, le principe de contrôle patronal de l'outil de travail peut se déduire de la convention collective de travail n°81 dans laquelle « les travailleurs reconnaissent le principe selon lequel l'employeur dispose d'un droit de contrôle sur l'outil de travail et sur l'utilisation de cet outil par le travailleur dans le cadre de l'exécution de ses obligations contractuelles, y compris lorsque cette utilisation relève de la sphère privée,… »[29].

L'on reconnait, en outre, à l'employeur un pouvoir d'autorité sur ses travailleurs[30]. C'est en vertu de ce pouvoir qu'il peut aussi exercer un certain contrôle de l'exécution du travail par ses salariés car, « vouloir contrôler l'activité du salarié pendant son temps de travail afin de s'assurer que celui-ci exécute correctement la mission pour laquelle il est rémunéré, constitue l'une des préoccupations de l'employeur, soucieux d'exercer son pouvoir de direction au sein de l'entreprise »[31].

La doctrine[32] a davantage fondé ce pouvoir de contrôle patronal sur le lien de subordination, la propriété des matériels que l'employeur met à la disposition des travailleurs et la responsabilité de l'employeur en cas de dommage du fait de ses travailleurs.

Mais, s'il est donc vrai que l'hôpital a un pouvoir de contrôle sur ses travailleurs quant à l'utilisation du système automatisé de distribution des médicaments, ce pouvoir n'est pas absolu et trouve certaines limites imposées particulièrement par le respect de la vie privée tant de ces derniers que des patients s'agissant des traitements de leurs données à caractère personnel récoltées tout au long du processus.

§2. Le respect du droit à la vie privée des travailleurs et des patients

Dans ses deux phases de fonctionnement, la distribution automatisée des médicaments collecte des données concernant les travailleurs et les patients. En effet, dans la phase de la prescription médicale électronique, l'arrêté royal du 7 juin 2009 précité impose que le

---

[27] Art. 20, 1° de la loi du 3 juin 1978 relative aux contrats de travail. (*M.B.*, le 22-08-1978, n°:1978070303, p. 9277).

[28]. Voy. Jean Philippe Dunand et al., *Internet au lieu de travail*, CEDIDAC, Lausanne, 2004, p.96 .

[29]. Art. 3, CCT n° 81 du 26 avril 2002.

[30]. L'article 17, 2° de la loi du 3 juin 1978 relative aux contrats de travail oblige le travailleur d'agir conformément aux ordres et aux instructions qui lui sont données par l'employeur, ses mandataires ou ses préposés, en vue de l'exécution du contrat. De même, la définition donnée du contrat de travail, aux articles 2, 3, 4 et 5 de la loi précitée veut que « … un travailleur s'engage contre rémunération à fournir un travail *sous l'autorité* d'un employeur ».

[31]. Isabelle de Benalcázar, *Droit du travail et nouvelles technologies*, Gualino éditeur, EJA-Paris, 2003, p. 83.

[32]. Pour plus de détails à ce sujet, voy. Thierry CLAEYS, « L'utilisation des nouvelles technologies et de l'e-mail durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », in *Le contrat de travail et la nouvelle économie*, éd. du Jeune Barreau de Bruxelles, 2001, pp. 258-260; Romain ROBERT et Karen ROSIER, « Réglementation et contrôle de l'utilisation des technologies de la communication et de l'information sur le lieu de travail », in *Le droit du travail à l'ère du numérique*, Anthemis s.a., 2011, pp. 233-234.

document électronique contienne les renseignements visés à l'article 2 de l'arrêté royal du 10 août 2005 fixant des modalités de la prescription à usage humain[33]. Tandis que dans la phase de l'accès à l'armoire à médicaments, il faut l'identification au moyen d'un login (2 lettres + 4 chiffres) ou le scan du code barre du badge ainsi qu'une authentification au moyen de l'empreinte digitale.

Quelle que soit la phase considérée, les données collectées permettent l'identification du malade et/ou du travailleur qui a prescrit le médicament ou qui a accédé au système. Ces données sont susceptibles d'être utilisées et traitées à diverses fins.

Le risque d'attenter à la vie privée des personnes concernées semble donc plus qu'évident. Dans ce contexte, examiner les conditions auxquelles doit obéir une telle activité revêt une importance capitale en vue de prévenir ce risque. Il sied, pour ce faire, d'établir la notion de ''vie privée'' (I) et d'analyser les incidences de la distribution automatisée des médicaments sur la vie privée tant des travailleurs que des patients (II).

I. La vie privée : notion

Le contour de ce qu'il faut entendre par ''vie privée'' est difficile à cerner. La notion y relative est fluctuante et imprécise[34]. C'est d'autant plus vrai que la vie privée est « une notion large, non susceptible d'une définition exhaustive »[35]; la Cour européenne des droits de l'homme (Cour EDH) a d'ailleurs précisé que « le terme ''vie privée'', ne doit pas être interprété de façon restrictive »[36]. C'est l'article 8 de la Convention européenne des droits de l'homme (CEDH) qui prévoit le droit au respect de la vie privée et familiale[37] et, c'est par le biais de cette disposition que la Cour et la Commission européennes des droits de l'homme sont parvenues à préciser ce qui rentre dans la notion de ''vie privée''.

Le droit à la vie privée peut donc comporter un droit à l'épanouissement, une liberté d'être soi, un droit à l'autonomie et, un pouvoir de poser certains choix existentiels[38]; l'idée d'une sphère privée ou publique[39]; la protection des données personnelles relatives à la santé[40]; les activités professionnelles ou commerciales[41];….

---

[33]. Ces renseignements concernent le nom, prénom et l'adresse du prescripteur concerné; le numéro d'identification à l'Institut National d'Assurance Maladie - Invalidité (INAMI) en chiffres et en code-barres, s'il échet; le nom ou la dénomination commune du médicament; le prénom et le nom du patient, la posologie journalière du médicament et, s'il échet, la mention précisant que le médicament est destiné à un enfant ou à un nourrisson; la signature datée du prescripteur, et, le cas échéant, la date de délivrance déterminée par lui; la forme d'administration; le dosage unitaire du médicament; la mention du nombre d'unités dans le conditionnement et du nombre de conditionnements, ou la mention de la durée de la thérapie en semaines et/ou jours.

[34]. Voy. J.-F. RENUCCI, *Droit européen des droits de l'Homme*, LGDJ, 2001, N°85.

[35]. Cour EDH, Pretty C. Royaume-Uni, n°/no 2346/02, 29. 04. 2002, §61.

[36]. Cour EDH, Amann c. Suisse, 16–02-2000, n°/no. 27798/95, § 65.

[37]. Cet article dispose : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

[38]. Cour EDH, Pretty c. R.U., *op. cit.*, § 61, 62 et 65

[39]. Cour EDH, Rotaru c. Roumanie, 4 mai 2000, n°/no 28341/95, § 43. (« Des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics. Cela vaut davantage encore lorsque ces données concernent le passé lointain d'une personne »)

[40]. Cour EDH, Z. C. Finlande, 25-02-1997, *Recueil des arrêts et décisions* 1997-I, p. 347, § 95. (Dans cette affaire, la Cour a tenu compte « du rôle fondamental que joue la protection des données à caractère personnel – les informations relatives à la santé n'en étant pas les moindres – pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8. Le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les parties contractantes à la Convention ») ; Cour EDH, M.S. c. Suède, 27-08-1997, § 41. (La Cour a précisé que

Bref, la vie privée est un concept qualifié de ‘’fourre-tout’’[42] ; il comporte l'idée d'un droit à l'intimité qui comprend notamment: le respect du droit de l'individu de vivre à l'abri des regards étrangers; le respect de son domicile privé ou professionnel; le respect du secret de ses opinions privées; la protection contre des écoutes téléphoniques ou contre des atteintes à la correspondance privée; le respect du droit d'accès aux données et renseignements personnels; et le respect du droit à la confidentialité des informations sur la santé[43].

II. Incidences de la distribution automatisée des médicaments sur la vie privée et le traitement de données à caractère personnel

II.1. Instruments juridiques de protection

Il existe, en Europe, plusieurs instruments qui protègent le droit à la vie privée[44]. En Belgique, ce droit est protégé notamment par l'article 22 de la Constitution[45]; la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[46]; l'article 314*bis* du Code pénal en ce qu'il punit l'écoute, la prise de connaissance ou l'enregistrement de (télé)communications privées pendant leur transmission; l'article 124 de la loi du 13 juin 2005[47] relative aux communications électroniques; la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance[48]; les conventions collectives de travail n°68 du 16 juin 1998 et n°81 du 26 avril 2002 relatives à la protection de la vie privée des travailleurs à l'égard respectivement de la surveillance par caméras sur le lieu du travail et du contrôle des données de communication électroniques en réseau.

Quant au droit à la protection des données à caractère personnel, Jean Herveg[49] écrit : « après avoir été construit sur la base du droit au respect de la vie privée, le droit à la protection des données à caractère personnel a été formellement consacré en tant que tel par la Charte des droits fondamentaux de l'Union européenne[50] dans une disposition distincte de celle qui concerne le droit au respect de la vie privée[51]. Le Praesidium de la Convention, qui a élaboré la Charte, a énuméré les bases de cette nouvelle disposition. Parmi celles-ci se retrouvent l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés

---

« la législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 »).

41. Cour EDH, Niemietz c. Allemagne, 16-12-1992, n° 251-B, §29. (La Cour a estimé qu''il n'y avait « aucune raison de principe de considérer cette manière de comprendre la notion de ‘’vie privée’’ comme excluant les activités professionnelles ou commerciales: après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur »). Voy. Vincent Berger, *Jurisprudence de la Cour Européenne des Droits de l'Homme*, 7ème éd., *Dalloz*, Paris, 2000, p.410.

42. S. van DROOGHENBROECK, *La Convention européenne des droits de l'homme*, Les dossiers du J.T., vol.57, Bruxelles, Larcier, 2006, n°309. Cité par Fabienne Kéfer, « La légalité de la preuve confrontée au droit à la vie privée du salarié », in *La vie privée au travail*, Marc Verdussen et Pierre Joassart, Anthemis, 2011, p. 17.

43. NGONDANKOY NKOY-ea-LOONGYA, *Droit congolais des droits de l'homme*, Bruylant, 2004, p. 253. Pour plus de détails à ce sujet, voy. Cécile de TERWAGNE, *Vie privée et TIC*, Fundp/Namur, 2011-2012.

44. Convention européenne des droits de l'homme et des libertés fondamentales du 3 nov. 1950 (art. 8), Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28/01/2981, Charte européenne des droits fondamentaux de l'Union européenne du 7 déc. 2000 (arts. 7-8), directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

45 *M.B.*, 17 févr. 1994 (deuxième éd.).

46 *M.B.*, 18 mars 1993.

47 *M.B.*, 20 juin 2005.

48 *M.B.*, 31 mai 2007.

49. Jean Herveg, *La protection des données du patient dans l'hôpital*, éd. Kluwer, 2009, pp.7-8.

50. *J.O.C.E.*, 18 déc. 2000 (C 364/1).

51. Art. 8 de la Charte des droits fondamentaux de l'Union européenne.

fondamentales ainsi que les principaux instruments juridiques européens qui ont été adoptés dans son giron pour assurer la protection des citoyens à l'égard des traitements de données à caractère personnel[52] ».

De ce qui précède, on note que les droits au respect de la vie privée et à la protection des données à caractère personnel sont intimement liés. Ils sont d'ailleurs, en droit belge, réglementés au sein d'une même loi, celle précitée du 8 décembre 1992.

Si, de manière générale, les questions de vie privée et du traitement des données à caractère personnel, qui résulteraient de la distribution automatisée des médicaments, peuvent être analysées au regard de la loi du 8 décembre 1992 (II.2), celles spécifiques aux travailleurs doivent davantage l'être en recourant à la convention collective de travail n°81 du 26 avril 2002 (II.3).

II.2. Distribution automatisée des médicaments face à la loi du 08/12/1992

II.2.1. Applicabilité de la loi du 08/12/1992 aux données collectées dans le processus de distribution automatisée des médicaments

La loi du 08/12/1992 s'applique à « tout traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier »[53].

Deux éléments du champ d'application matérielle de cette loi méritent d'être explicités avant de répondre à notre question initiale : données à caractère personnel et traitement. Ainsi, si les "données à caractère personnel" désignent « toute information concernant une personne physique identifiée ou identifiable »[54], le ''traitement'' est, par contre, « 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 de données à caractère personnel »[55].

Dans le cas de la distribution automatisée des médicaments, il appert que tant la prescription médicale que l'accès à l'armoire à médicaments utilisent un procédé automatisé qui n'appelle pas un commentaire spécial. A cela s'ajoute que les renseignements imposés par l'arrêté royal du 7 juin 2009 pour la prescription médicale électronique, d'une part, et l'identification au moyen d'un ''login (2 lettres + 4 chiffres) ou le scan du code barre du badge''[56] ainsi que l'authentification au moyen de l'empreinte digitale nécessaires à l'accès à l'armoire à médicaments, d'autre part, constituent bien des informations spécifiques, propres à l'identité physique, physiologique, ou sociale identifiant ou susceptibles d'identifier soit les patients,

---

[52]. Explications relatives à la charte des droits fondamentaux, *J.O.U.E.*, C 303/17, 14 déc. 2007.

[53]. Art. 3, §1 de la loi du 08/12/1992.

[54]. Art. 1, §1 de la loi du 08/12/1992.

[55]. Art. 1, §1 de la loi du 08/12/1992.

[56]. Il peut s'agir des données a` caractère personnel codées, c'est-à-dire, des « données a` caractère personnel démunies de tout élément permettant d'identifier la personne et munies d'un code, qui seul permet de relier la donnée à la personne concernée. Voy. Commentaire de l'art. 1e, 3° de l'A.R. du 13 févr. 2001 portant exécution de la loi du 8 déc. 1992 relative à la protection de la vie privée a` l'égard des traitements de données à caractère personnel. Disponible à l'adresse http://www.privacycommission.be. Les données codées sont un exemple classique de pseudonymisation (un traitement qui consiste à dissimuler l'identité). Les informations correspondent à des personnes physiques possédant chacune un code, la clé permettant d'établir une correspondance entre ce code et des identifiants courants de ces personnes physiques (comme le nom, la date de naissance, l'adresse) étant conservée séparément. Voy, Groupe 29, Avis 4/2007 sur le concept de données à caractère personnel, Adopté le 20 juin, pp.19-20.

soit les travailleurs-utilisateurs du système. Parmi ces informations figurent aussi les données relatives à la santé des patients; elles constituent une catégorie particulière de données soumise à des règles spéciales. En sus, dans le cadre du système automatisé de distribution des médicaments, ces données peuvent faire l'objet non seulement de collecte, d'enregistrement, d'organisation, de conservation, d'adaptation ou de modification, mais aussi d'extraction, de consultation, d'utilisation, de communication par transmission, de diffusion ou de toute autre forme de mise à disposition, de rapprochement ou d'interconnexion, ainsi que de verrouillage, d'effacement ou de destruction.

Dans ces conditions, les données collectées dans le processus de distribution automatisée des médicaments, tant à l'étape de la prescription médicale qu'à celle de l'accès à l'armoire à médicaments, rentrent bien dans le champ d'application matérielle de la loi du 08/12/1992. Le traitement est, en outre, effectué en Belgique et rentre donc dans le champ d'application territorial[57] défini par la loi du 08/12/1992.

Dans ces conditions, le traitement de telles données doit obéir à certaines conditions (II.2.1.1) et les personnes concernées ont certains droits à faire prévaloir (II.2.1.2).

II.2.1.1. Les conditions du traitement

La loi pose le principe selon lequel « lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée »[58].

Pour se conformer à cette disposition, les données à caractère personnel doivent répondre aux conditions de finalité (II.2.1.1.1), de qualité (II.2.1.1.2) et de légitimité (II.2.1.1.3).

II.2.1.1.1. Les finalités poursuivies par le traitement

Les finalités poursuivies doivent être mises au clair avant tout traitement de données à caractère personnel. C'est ainsi que la loi impose qu'elles soient déterminées, mais aussi explicites, légitimes et ne soient pas traitées ultérieurement de manière incompatible[59].

Dans le contexte de la distribution automatisée des médicaments, il sied que l'hôpital, par les personnes statutairement compétentes, définisse les raisons pour lesquelles les opérations seront effectuées sur les données à caractère personnel tant des travailleurs que des patients. Ces raisons ne doivent pas être implicites ou secrètes, mais clairement exprimées, sans ambiguïté; elles doivent aussi être conformes aux lois et règlements, à l'ordre public et aux bonnes mœurs.

Plus concrètement, ces finalités doivent s'inscrire dans les objectifs visés par l'hôpital:

- la mise en pratique des prescrits de l'arrêté royal du 7 juin 2009 réglementant la prescription médicale électronique;
- le contrôle et la gestion efficaces des opérations effectuées sur les stupéfiants en vue de *prévenir des faits illicites et contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui; lutter contre les pratiques contraires (vol des*

---

[57]. Voy. art. 3*bis*, 1°: « la présente loi est applicable au traitement de données à caractère personnel lorsque le traitement est effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge ou en un lieu où la loi belge s'applique en vertu du droit international public ».

[58]. Art 2 de la loi du 08/12/1992.

[59]. Voy. art. 4, §1e, 1° de la loi du 8 déc. 1992. Pour plus de détails à ce sujet, voy. Cécile de TERWANGNE, *op. cit.*; Jean Herveg, *op. cit.*, pp.37-3.

stupéfiant,); le respect des principes et règles d'utilisation des dispositifs de stockage et de délivrance des médicaments[60].

- la non-répudiation des opérations effectuées sur les stupéfiants par les travailleurs;

II.2.1.1.2. La qualité de données

L'article 4, § 1e, 3°- 5° énumère les exigences de qualité que les données à caractère personnel doivent remplir. Elles doivent être adéquates, pertinentes et non excessives au regard des finalités…; exactes et, si nécessaire, mises à jour…; conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement….

Par rapport à la distribution automatisée des médicaments, la conformité à ces exigences de qualité nécessite que :

- les données à récolter soient connues d'avance et limitées à celles qui sont adéquates, pertinentes et non excessives au regard des finalités poursuivies. Ces données que nous avons énumérées plus haut correspondent principalement aux renseignements visés à l'article 2 de l'arrêté royal du 10 août 2005 précité. Pour celles relatives à l'empreinte digitale (données biométriques), l'employeur devra, en sa qualité de ''responsable du traitement''[61], expliquer les finalités à la base d'un tel choix.
- pour l'exactitude des données et leur mise à jour éventuelle ou rectification, il faudra tenir compte de l'article 1, §1, al.3 de l'arrêté royal du 7 juin 2009 qui s'oppose à toute modification de manière imperceptible du document électronique après la mention de l'identité du médecin ou du praticien de l'art dentaire et après l'association à une date de référence et une heure de référence;
- le délai de conservation des données devra se conformer à la période de 10 ans mentionnée à l'article 33, § 5, de l'arrêté royal du 31 mai 1885 approuvant les nouvelles instructions pour les médecins, pour les pharmaciens et pour les droguistes.

II.2.1.1.3. La légitimité du traitement

Les finalités et la qualité de données ne suffisent pas; il faut, en outre, que le traitement soit légitime. Les données doivent, à ce titre, être traitées ''loyalement et licitement''[62]. La légitimité impose aussi au responsable du traitement, ici l'hôpital en tant que personne morale ou association de fait qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel[63], un devoir de transparence à travers l'information[64] et la notification du traitement à la CPVP[65], mais aussi un devoir de sécurité[66].

---

[60]. Voy. art. 5, §1, CCT n°81.

[61]. Par "responsable du traitement", on entend la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. (Art. 1, §4 de la loi du 08/12/1992).

[62]. Voy. art. 4, §1e, 1° de la loi du 8 déc. 1992. Pour plus de détails à ce sujet, voy. Jean Herveg, *op. cit.*, pp. 43-44.

[63]. Voy. art. 1, §4 de la loi du 08/12/1992.

[64]. Voy. art. 9 de la loi du 08/12/1992 En sa qualité de responsable du traitement, l'hôpital ou son représentant devra fournir aux travailleurs et aux malades concernés auprès desquels il obtient les données et, au plus tard au moment où ces données sont obtenues, les informations sur le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant; les finalités du traitement; l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel le concernant envisagé à des fins de direct marketing; les destinataires ou les catégories de destinataires des données ; le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse ; l'existence d'un droit d'accès et de rectification des données le concernant; sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont obtenues, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard du travailleur ou du malade concerné un traitement loyal des données.

En dehors de ce qui précède, cette légitimité comporte, dans le cas d'espèce, quelques spécificités selon qu'il s'agit de simples données ou données normales relatives aux travailleurs (1°) ou des données relatives à la santé des patients (2°). Mais, la question concernant les données biométriques (3°) ainsi que celle du transfert de données à caractère personnel vers un pays non membre de la communauté européenne (4°) méritent une attention toute particulière sur le terrain de la légitimité du traitement.

1°. S'agissant de simples données ou données normales

L'expression de ''simples données'' est utilisée par opposition aux données sensibles pour désigner toute autre donnée que sensible. Dans le cas de la distribution automatisée des médicaments, les simples données ont trait, par exemple, aux nom, prénom et adresse du prescripteur concerné; au numéro d'identification à l'INAMI en chiffres et en code-barres, à la signature datée du prescripteur, à la date, au ''login'' ou au code barre du badge…

L'article 5 de la loi sous analyse veut que le traitement de telles données s'inscrive dans l'un des cas suivants:

- la personne concernée doit avoir indubitablement donné son consentement;
- il doit être nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;
- il doit être nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance;

De même, lorsque les données n'ont pas été obtenues auprès du travailleur ou du malade concerné, l'hôpital ou son représentant devra, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données, fournir les mêmes informations énumérées ci-dessus, sauf si la personne concernée en est déjà informée.

L'hôpital sera cependant dispensé de fournir ces informations, d'une part, lorsque, en particulier pour un traitement aux fins de statistiques ou de recherche historique ou scientifique ou pour le dépistage motivé par la protection et la promotion de la santé publique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés et, lorsque, d'autre part, l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

[65]. Voy. art. 17 de la loi du 08/12/1192. La notification doit mentionner la date de la déclaration et, le cas échéant, la mention de la loi, du décret, de l'ordonnance ou de l'acte réglementaire décidant la création du traitement automatisé; les nom, prénoms et adresse complète ou la dénomination et le siège du responsable du traitement et, le cas échéant, de son représentant en Belgique; la dénomination du traitement automatisé; la finalité ou l'ensemble des finalités liées du traitement automatisé; les catégories de données à caractère personnel qui sont traitées; les catégories de destinataires à qui les données peuvent être fournies; les garanties dont doit être entourée la communication de données aux tiers; les moyens par lesquels les personnes qui font l'objet des données en seront informées, le service auprès duquel s'exercera le droit d'accès et les mesures prises pour faciliter l'exercice de ce droit; la période au-delà de laquelle les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées; une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement;…

[66]. Voy. art. 16, § 2 de la loi du 08/12/1992. L''hôpitale ou son représentant devra tenir les données à jour, rectifier ou supprimer celles qui sont inexactes, incomplètes, ou non pertinentes; veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service; informer les personnes agissant sous son autorité des dispositions de la loi et de ses arrêtés d'exécution, ainsi que de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel; s'assurer de la conformité des programmes servant au traitement automatisé des données à caractère personnel ainsi que de la régularité de leur application.

En outre, toute personne agissant sous l'autorité de l'hôpital qui accède aux données en cause ne peut les traiter que sur instruction de l'hôpital ou de son représentant, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

Et, pour garantir la sécurité des données à caractère personnel, l'hôpital ou son représentant en Belgique doit prendre les mesures techniques et organisationnelles requises pour protéger lesdites données contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

- il doit être nécessaire à la sauvegarde de l'intérêt vital de la personne concernée;
- il doit être nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées;
- il doit être nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi.

Par rapport à la distribution automatisée des médicaments, il est important d'obtenir le consentement du travailleur lors de la signature du contrat ou grâce à un avenant audit contrat.

A défaut du consentement du travailleur, le traitement pourra toujours être effectué sur base:

- d'une obligation à laquelle le responsable du traitement est soumis en vertu d'une loi, d'un décret ou d'une ordonnance. En effet, l'arrêté royal du 7 juin 2009 précité impose cette obligation dès lors que l'hôpital donne la possibilité de la prescription médicale électronique;
- de l'intérêt légitime poursuivi par le responsable du traitement car, la distribution automatisée des médicaments, avons-nous dit, s'inscrit dans une logique de gestion rationnelle des stupéfiants et de la concrétisation de l'arrêté royal du 7 juin 2009. Ces intérêts légitimes permettent à l'hôpital de traiter les données à caractère personnel des personnes concernées.
- du contrat (de travail ou de collaboration) qui lie souvent l'hôpital aux travailleurs. On estime, dans cette hypothèse, que le traitement est bien nécessaire à l'exécution dudit contrat car, la distribution automatisée des médicaments, dans sa phase de prescription médicale ou d'accès à l'armoire, est un dispositif qui permet aux travailleurs précités d'exécuter leur contrat dont l'un des devoirs consiste, pour les uns, à prescrire les médicaments et/ou à traiter les patients, pour les autres, à approvisionner l'armoire.

2°. S'agissant des données relatives à la santé des patients

Ces données sont sensibles et concernent, dans l'espèce sous examen, les informations se rapportant à la santé des patients: prénom et nom du patient associés au nom ou à la dénomination commune du médicament; à la posologie journalière du médicament et, s'il échet, à la mention précisant que le médicament est destiné à un enfant ou à un nourrisson; à la forme d'administration; au dosage unitaire du médicament; à la mention du nombre d'unités dans le conditionnement et du nombre de conditionnements, ou à la mention de la durée de la thérapie en semaines et/ou jours.

Le traitement de ces données est, en principe, proscrit dans la mesure où il ne peut avoir lieu que dans certaines hypothèses exceptionnelles[67].

---

[67]. Voy. art. 7 de la loi du 8 déc. 1992. L'interdiction de traiter ces données ne s'applique pas : a) lorsque la personne concernée a donné son consentement par écrit à un tel traitement, pour autant que ce consentement puisse à tout moment être retiré par celle-ci; b) lorsque le traitement est nécessaire afin d'exécuter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail; c) lorsque le traitement est nécessaire à la réalisation d'une finalité fixée par ou en vertu de la loi, en vue de l'application de la sécurité sociale; d) lorsque le traitement est nécessaire à la promotion et à la protection de la santé publique y compris le dépistage; e) lorsque le traitement est rendu obligatoire par ou en vertu d'une loi, d'un décret ou d'une ordonnance pour des motifs d'intérêt public importants; f) lorsque le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement; g) lorsque le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée; h) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée; i) lorsque le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice; j) lorsque le traitement est nécessaire aux fins

Dans le cas sous analyse, il est important d'obtenir, à titre principal, le consentement écrit du patient avant tout traitement des données relatives à sa santé. Le groupe 29 veut que, pour être valable, ce consentement, quelles que soient les circonstances dans lesquelles il est donné, soit une «manifestation de volonté, libre, spécifique et informée»[68]; mais la question de la validité du consentement d'une personne souffrante, partie faible ou à tout le moins en position de demande, peut toujours poser problème[69] surtout lorsque la personne concernée est dans une situation de dépendance vis-à-vis du responsable du traitement[70].

Mais en dehors du consentement du patient, l'hôpital peut toujours baser le traitement sur, par exemple, la nécessité de la promotion et de la protection de la santé publique y compris le dépistage (art. 7, §2, d); la nécessité de la défense des intérêts vitaux du patient (art. 7, §2, f) étant donné que la distribution automatisée des médicaments constitue un mécanisme qui concourt à la guérison du malade dans la mesure où certaines de ses prescriptions médicales ainsi que l'accès aux médicaments passent par elle;…

Notons aussi qu'en vertu de l'article 7, §4 de la loi du 8 décembre 1992, sauf dans le cas d'un consentement écrit de la personne concernée ou lorsque le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée, le traitement des données relatives à la santé ne peut être effectué que sous la responsabilité d'un professionnel des soins de santé. Celui-ci et ses préposés ou mandataires sont soumis au secret. Le paragraphe 5 de ce même article veut que les données à caractère personnel relatives à la santé ne soient collectées qu'auprès de la personne concernée. Elles ne peuvent être collectées auprès d'autres sources qu'à condition que la collecte soit conforme au § 3 qui vise les conditions des articles 26 à 27 de l'arrêté royal du 13 février 2001 vues ci-dessus et au § 4 qui subordonne le traitement à la double condition de la responsabilité d'un professionnel des soins de santé et de respect du secret professionnel.

Par ailleurs, le traitement des données relatives à la santé doit aussi obéir à d'autres conditions imposées par l'arrêté royal du 13 février 2001[71]. En effet, les articles 25 à 26 de cet arrêté royal exigent du responsable du traitement, ici l'hôpital, notamment :

- de faire en sorte que les personnes autorisées à traiter les données ne soient plus désignées par leur nom et que les listes des catégories de ces personnes soient mises à la disposition de la Commission de la protection de la vie privée ;
- de tenir les personnes ayant accès aux données médicales à une obligation de discrétion ou de confidentialité garantie légalement ou statutairement, ou par une disposition contractuelle équivalente ;

3°. Le cas particulier de données biométriques

a. Notion

L'accès des travailleurs aux armoires à médicaments est sécurisé. Il exige l'identification, soit en tapant son login (2 lettres + 4 chiffres), soit en scannant le code barre de son badge, mais

---

de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et les données sont traitées sous la surveillance d'un professionnel des soins de santé; k) lorsque le traitement est nécessaire à la recherche scientifique et est effectué conformément aux conditions fixées par le Roi, par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée.

[68]. Voy . Document de travail adopté le 15 février 2007 par le groupe 29 sur les données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p.9.

[69]. A ce sujet, voy. Jean Herveg, « Quelle est la nature du consentement du patient dans le traitement de données médicales en droit européen ? », Coimbra Editora, pp. 24 et ss.

[70]. Voy. art. 27 de l'A.R. du 13 mars 2001, p. 7839.

[71]. *M.B.*, 13 mars 2001.

aussi l'authentification via l'empreinte digitale du travailleur qui entend y accomplir certaines opérations[72]. La biométrie « recouvre l'ensemble des procédés tendant à identifier un individu à partir de la ‘’mesure’’ de l'une ou de plusieurs de ses caractéristiques physiques, physiologiques ou comportementales. Il peut s'agir des empreintes digitales, de l'iris de l'œil, du contour de la main, de l'ADN ou d'éléments comportementaux... »[73].

b. Les données biométriques sont-elles aussi de données à caractère personnel ?

Pour le groupe 29, « ce qui caractérise, entre autres, les données biométriques, c'est qu'elles peuvent être considérées comme contenu des informations concernant une personne physique donnée (X a ces empreintes digitales) ainsi que comme élément permettant d'établir un lien entre une information et une personne physique (cet objet a été touché par quelqu'un qui présente ces empreintes digitales et celles-ci correspondent à X; par conséquent, X a touché l'objet). Elles peuvent ainsi servir d'«identificateurs». En effet, en raison du lien unique qui les relie à une personne physique spécifique, les données biométriques peuvent être utilisées pour identifier la personne physique »[74].

Ce même groupe 29 constate qu'il est aujourd'hui souvent fait recours au traitement de données biométriques dans des procédures automatisées d'authentification/vérification et d'identification, notamment lors du contrôle de l'entrée dans des zones physiques et virtuelles (c'est-à-dire l'accès à des systèmes ou services électroniques particuliers). Les données de ce genre sont d'une nature particulière puisqu'elles ont trait aux caractéristiques comportementales et physiologiques d'une personne et peuvent permettre de l'identifier sans ambiguïté[75]. Cette identification biométrique a souvent rencontré la résistance de la société[76].

Dans le cas de la distribution automatisée des médicaments, les informations véhiculées par l'empreinte digitale sont des données à caractère personnel. Le groupe 29 est également de cet avis en estimant que selon la définition des données à caractère personnel figurant à l'article 2a de la directive 95/46/CE , « les mesures d'identification biométrique ou leur version numérisée sous forme de modèle sont, dans la plupart des cas, des données à caractère personnel. Il apparaît que des données biométriques peuvent toujours être considérées comme "des informations concernant une personne physique", puisqu'il s'agit de données qui fournissent, par leur nature même, des informations sur une personne précise. Dans le contexte de l'identification biométrique, la personne est généralement identifiable, puisque les données biométriques sont utilisées à des fins d'identification ou d'authentification/vérification au moins dans la mesure où la personne concernée est distinguée de toute autre personne »[77].

Comme il en est ainsi, les données biométriques, à l'instar des informations relatives aux empreintes digitales, doivent aussi être traitées conformément aux règles édictées par la loi du

---

[72]. Pour plus de détails sur l'identification et l'authentification, voy. Jacques Pierson, *La biométrie, l'identification par le corps*, éd. Lavoisier, 2007, pp.71-74.

[73]. CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, p. 3. Disponible à l'adresse http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf; Groupe de travail «article 29» sur la protection des données, Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin, p.9.

[74]. Groupe de travail «article 29» sur la protection des données, Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin, p.9.

[75]. Voy. Groupe 29, Document de travail sur la biométrie, 12168/02/FR, GT 80, 1/08/2003, p.2. Disponible à l'adresse http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_fr.pdf

[76]. Pour plus de détails, voy. Xavier Crettiez et Pierre Piazza, *Du papier à la biométrie. Identifier les individus*, Presses de la Fondation Nationale des Sciences Politiques, Paris, 2006.

[77]. Voy. Groupe 29, *idem*, pp. 5-6.

8/12/1992. Dans la situation présente, elles peuvent être considérées comme de simples données ou des données normales concernant les travailleurs.

c. Gestion des empreintes digitales

Le mode de gestion des empreintes digitales présente un intérêt particulier pour le respect du droit à la vie privée et le traitement des données à caractère personnel au regard du fonctionnement du processus de distribution automatisée des médicaments.

Les empreintes digitales peuvent, en effet, être gérées d'une manière centralisée ou non: si dans la gestion centralisée, on stocke les empreintes sur le terminal de lecture-comparaison ou sur un serveur avec pour conséquence que la personne perd la maîtrise de sa donnée biométrique qui est ainsi détenue par un tiers de sorte qu'en cas d'intrusion dans le terminal ou le serveur, on peut accéder à l'ensemble des empreintes ou gabarits qui y sont stockés et qui sont généralement associés aux identités des personnes, la situation est différente s'agissant de la gestion non centralisée où le stockage est fait sur un support individuel (tel que carte à puce ou clé USB), exclusivement détenu par la personne concernée entraînant ainsi la maîtrise de sa donnée biométrique qui reste sous sa responsabilité et ne peut pas être utilisée pour l'identifier à son insu de sorte qu'en cas de vol ou de perte du support de stockage, on ne peut avoir accès qu'à une seule donnée biométrique éventuellement associée à l'identité de la personne[78].

De ces deux modes de gestion, celle centralisée semble souvent plus favorable aux hôpitaux[79]. Elle utilise une base de données qui permet aux travailleurs ou aux utilisateurs d'accéder à n'importe quelle armoire.

Contrairement à la gestion non centralisée, il semble que ce mode de gestion présente beaucoup plus de risques d'atteinte aux libertés fondamentales des utilisateurs du système. En effet, « il est généralement admis que le risque de réutilisation, pour des finalités incompatibles, de données biométriques obtenues à partir de traces physiques laissées par des personnes à leur insu (empreintes digitales par exemple) est relativement faible lorsque les données sont conservées non pas dans des bases de données centralisées, mais par la personne concernée, et qu'elles sont inaccessibles aux tiers. Le stockage centralisé de données biométriques accroît également le risque que ces données soient utilisées comme une clé pour interconnecter différentes bases de données, ce qui pourrait permettre d'obtenir un profil détaillé des habitudes d'un individu, tant dans la sphère publique que dans la sphère privée. La question de la compatibilité des finalités pose également le problème de l'interopérabilité de différents systèmes reposant sur la biométrie. La standardisation qu'exige l'interopérabilité pourrait entraîner une plus forte interconnexion entre les bases de données »[80].

De ce qui précède, il est indiqué de ne pas recourir à une gestion centralisée des empreintes digitales pour minimiser le risque de violation de la vie privée des travailleurs.

---

[78]. Voy. CNIL, *op. cit.*, pp. 4-5.

[79]. C'est le système adopté par les CuSL.

[80]. Voy. Groupe 29, *op. cit.*, pp. 7-8. Ce groupe est donc d'avis que *l'utilisation, à des fins de contrôle d'accès (authentification/vérification), de systèmes biométriques se référant à des caractéristiques physiques qui laissent des traces, mais dont les données ne sont pas enregistrées dans une mémoire détenue par une personne autre que la personne concernée (autrement dit, les données ne sont pas mises en mémoire dans le dispositif de contrôle d'accès ou dans une base de données centrale), crée moins de risques pour la protection des libertés et des droits fondamentaux de la personne. […] les éléments biométriques devraient, de préférence, être conservés non pas dans une base de données, mais plutôt dans un dispositif exclusivement accessible à l'utilisateur, tel qu'une carte à puce, un téléphone portable ou une carte bancaire. En d'autres termes, les applications d'authentification/vérification qui peuvent être mises en œuvre sans enregistrement central de données biométriques ne devraient pas faire appel à des techniques d'identification excessives.*

Cependant, si on s'en tient à la gestion centralisée des empreintes digitales, il faut que, par un protocole, l'hôpital s'engage à n'utiliser la base de données constituée à cet effet qu'aux seules fins d'authentification dans les accès au dispositif de stockage et de délivrance des médicaments. Il sied de déterminer aussi les sanctions auxquelles s'exposerait l'hôpital en cas de violation dudit protocole. Il faut, en outre, installer, sur la base de données, les bonnes pratiques en matière de sécurité par des mesures techniques; il est à ce titre utile de crypter les identifications et les données biométriques tirées des empreintes digitales.

4°. Distribution automatisée des médicaments et transfert de données à caractère personnel vers un pays non membre de la Communauté européenne.

Les données à caractère personnel traitées dans le cadre de la distribution automatisée des médicaments peuvent, pour plusieurs raisons, faire l'objet de transfert vers un pays non membre de la Communauté européenne avec le risque d'y être traitées pour des finalités incompatibles, sans aucune protection légale,….

C'est pourquoi, les articles 21 et 22 de la loi du 8 décembre 1992 s'intéressent à une telle activité et, les données traitées dans le cadre de la distribution automatisée des médicaments doivent s'y conformer. Ainsi, sauf exceptions légales[81], le transfert de données à caractère personnel faisant l'objet d'un traitement après leur transfert vers un pays non membre de la Communauté européenne, ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions de la loi précitée et de ses arrêtés d'exécution. Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transfert de données; il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.

II.2.1.2. Distribution automatisée des médicaments et droits des personnes concernées

Les travailleurs comme les patients concernés par le traitement de données à caractère personnel via la distribution automatisée des médicaments ont un droit de curiosité[82], un droit d'accès[83], un droit de rectification[84], un droit d'opposition[85] et un droit de ne pas être soumis à une machine[86].

---

[81]. Voy. art. 22 de la loi du 8 décembre 1992. Le transfert de données traitées dans le cadre de la distribution automatisée des médicaments peut se baser sur les dérogations ci-après: le travailleur ou le patient concerné a indubitablement donné son consentement au transfert envisagé; le transfert est nécessaire à l'exécution d'un contrat entre le travailleur concerné et l'hôpital ou des mesures préalables à la conclusion de ce contrat, prises à la demande du travailleur; le transfert est nécessaire à la conclusion ou à la conclusion d'un contrat conclu ou à conclure, dans l'intérêt dans l'intérêt du travailleur ou du patient, entre l'hôpital et un tiers; le transfert est nécessaire ou est rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice; le transfert est nécessaire à la sauvegarde de l'intérêt vital du patient; en cas, par exemple des garanties résultant de clauses contractuelles appropriées ;… Pour ce dernier cas, voy. Décision 2001/497/CE de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE, telle que modifiée par la Décision 2004/915/CE de la Commission du 27 déc. 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers; Décision 2002/16/CE de la Commission du 27 déc. 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE.

[82]. Ce droit découle du fait que « la personne concernée qui apporte la preuve de son identité a le droit d'obtenir du responsable du traitement la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées ». Art. 10, §1, a) de la loi du 08/12/1992

[83]. Ce droit porte sur la communication, sous une forme intelligible, des données faisant l'objet des traitements; l'origine des données; la connaissance de la logique qui sous-tend tout traitement automatisé des données; la faculté d'exercer les droits

Dans le cadre de la distribution automatisée de médicaments, travailleurs comme patients bénéficieront certes de ces droits, mais il sera, par exemple difficile de rectifier les données compte tenu du fait que l'article 1, §1, 3° de l' arrêté royal du 7 juin 2009 précité impose que le document électronique ne soit plus modifié de manière imperceptible après la mention de l'identité du médecin ou du praticien de l'art dentaire et après l'association à une date de référence et une heure de référence.

II.3. Distribution automatisée des médicaments face à la CCT n°81 du 26 avril 2002

II.3.1. Applicabilité de la CCT n°81 à la distribution automatisée des médicaments

La CCT n°81 vise à garantir le droit fondamental des travailleurs au respect de leur vie privée dans la relation de travail en définissant, compte tenu des nécessités d'un bon fonctionnement de l'entreprise, pour quelles finalités et à quelles conditions de proportionnalité et de transparence un contrôle des données de communication électroniques en réseau peut être installé et les modalités dans lesquelles l'individualisation de ces données est autorisée[87].

La distribution automatisée des médicaments, avons-nous vu, pose un problème de vie privée des travailleurs utilisant le système y relatif. En effet, son recours à des dispositifs automatisés est susceptible de permettre un contrôle des données à caractère personnel relatives aux travailleurs qui y accèdent. Le personnel soignant et les administrateurs du système interagissent ou communiquent, à différents niveaux, avec les dispositifs automatisés qui sous-tendent la distribution des médicaments et ce, soit en prescrivant électroniquement les médicaments en faveur des patients, soit encore en introduisant les données à caractère personnel qui permettent d'accéder aux médicaments prescrits pour un patient déterminé et, soit enfin, en approvisionnant le dispositif de stockage en médicaments. Il s'agit donc d'un mécanisme de communication électronique susceptible de renseigner sur les données échangées en réseau. Les données de communication électroniques en réseau sont celles « relatives aux communications électroniques transitant par réseau, entendues au sens large et indépendamment du support par lequel elles sont transmises ou reçues par un travailleur dans le cadre de la relation de travail »[88].

Dans le cas spécifique de la distribution automatisée des médicaments, les travailleurs, dont les empreintes digitales sont prélevées et souvent centralisées aux fins d'accéder aux machines, transmettent des données biométriques qui aident à leur identification. De même, les médecins et les professionnels de l'art dentaire, qui prescrivent électroniquement les médicaments, transmettent également de données à caractère personnel à travers le réseau de l'hôpital ou de l'employeur. Dans ces conditions, on se rend bien compte que le contrôle de données de communication électroniques transmises par un travailleur et transitant par le

---

de rectification et d'opposition. A cette fin, la personne concernée adresse une demande datée et signée au responsable du traitement ou à toute autre personne désignée par le Roi. Les renseignements sont communiqués sans délai et au plus tard dans les quarante-cinq jours de la réception de la demande. Art. 10, §1, b, c, d de la loi du 08/12/1992.

[84]. La personne concernée par le traitement a le droit d'obtenir la rectification de toute donnée inexacte, ou la suppression de données incomplètes, non pertinentes, interdites ou conservées pour durée trop longue par rapport à finalité poursuivie. Art. 12 de la loi du 08/12/1992.

[85]. Toute personne a en outre le droit de s'opposer, pour des raisons sérieuses et légitimes tenant à une situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf lorsque la licéité du traitement est basée sur les motifs liés, d'une part, à l''exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci et, d'autre part, au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Art. 12 de la loi du 08/12/1992.

[86]. Une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité. Art. 12*bis* de la loi du 08/12/1992.

[87]. Voy. art. 1, §1 de la convention collective n°81.

[88]. Art. 2 de la CCT n° 81.

réseau de l'hôpital est, de façon permanente, ouvert à l'employeur. Un tel contrôle doit se conformer aux règles qui protègent le droit de toute personne au respect de sa vie privée. La loi du 13 juin 2005 relative aux communications électroniques[89] mérite une mention spéciale à ce sujet. Mais, puisque c'est le travailleur qui nous intéresse à ce propos, nous nous en tiendrons aux dispositions de la CCT n° 81.

II.3.2. Reconnaissance mutuelle des droits de contrôle et du respect de la vie privée

L'article 3 consacre un principe de reconnaissance mutuel des droits de contrôle de l'employeur vis-à-vis des travailleurs et au respect de la vie privée des travailleurs par l'employeur :

- Les travailleurs reconnaissent que l'employeur dispose d'un droit de contrôle sur l'outil de travail et sur l'utilisation de cet outil par le travailleur dans le cadre de l'exécution de ses obligations contractuelles, y compris lorsque cette utilisation relève de la sphère privée, compte tenu des modalités d'application prévues par la convention;
- Les employeurs respectent le droit des travailleurs à la protection de leur vie privée dans le cadre de la relation de travail et des droits et obligations que celle-ci implique pour chacune des parties.

Conséquemment à cette reconnaissance mutuelle des droits, tout contrôle des données à caractère personnel doit respecter les principes de finalité (II.3.2.1), de proportionnalité (II.3.2.2) et de transparence (II.3.2.3). La distribution automatisée des médicaments doit aussi se conformer à ces principes.

II.3.2.1. Principe de finalité par rapport à la distribution automatisée des médicaments

Pour être autorisé, le contrôle des données de communication électroniques en réseau doit poursuivre l'une des finalités suivantes[90]:

1°. La prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui. ;
2°. La protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires ;
3°. La sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise ;
4°. Le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.

Il en sera ainsi de la distribution automatisée des médicaments : lutte contre les faits illicites, faits contraires aux bonnes mœurs, aux pratiques contraires (vol des stupéfiants), la sécurité des systèmes informatiques en réseau de l'hôpital, le respect des principes et règles d'utilisation des technologies en réseau au sein de l'hôpital. Il conviendra à l'hôpital de définir clairement et de manière explicite la ou les finalités du contrôle comme le veut le §2 de l'article 5 de la CCT n°81.

---

89. *M.B.*, 20 juin 2005. Cette loi fixe, en ses articles 122 à 133, plusieurs dispositions qui protègent le secret des communications, le traitement des données et la vie privée. Le principe adopté à l'art. 124 interdit, sauf les exceptions établies à l'article 125 de la même loi, de chercher à connaître le contenu des communications électroniques ou à identifier les personnes dont elles concernent.

90. Art. 5, §1 CCT n°81.

II.3.2.2. Le principe de proportionnalité au regard de la distribution automatisée des médicaments

L'article 6 de la CCT n°81 pose le principe selon lequel « le contrôle des données de communication électroniques en réseau ne peut entraîner une ingérence dans la vie privée du travailleur. Si toutefois ce contrôle entraîne une ingérence dans la vie privée du travailleur, cette ingérence doit être réduite à un minimum».

Ce principe implique de ne traiter et plus précisément ici de ne collecter en vue du contrôle que les données de communication électroniques en réseau qui sont nécessaires au contrôle, c'est à dire les données qui, compte tenu de la finalité légitime poursuivie par le contrôle, entraînent l'ingérence la plus réduite dans la sphère privée du travailleur[91].

Pour se conformer à cette obligation, il convient que, outre l'empreinte digitale nécessaire à l'authentification pour accéder à l'armoire à médicaments, l'hôpital ne traite que les seuls renseignements visés à l'article 2 de l'arrêté royal du 10 août 2005 fixant des modalités de la prescription à usage humain.

Il vaudra mieux, en outre, conformément à l'article 10 de la CCT n°81, instaurer une évaluation régulière des systèmes au sein du conseil d'entreprise, du comité pour la prévention et la protection au travail ou avec la délégation syndicale de manière à faire des propositions en vue de les revoir en fonction des développements technologiques.

II.3.2.3. Le principe de transparence par rapport à la distribution automatisée des médicaments

La transparence passe généralement par le respect de l'obligation d'information. Celle-ci peut être collective[92] ou individuelle[93].

Dans le cadre de la distribution automatisée des médicaments, il est certes souvent fourni des consignes d'utilisation de l'outil, mais il faudra encore, avant toute chose, donner, par une circulaire, l'information aux travailleurs concernés. Cette information pourrait également être mentionnée dans le règlement de travail et dans le contrat individuel de travail.

L'article 9 de la CCT n°81 précise les éléments constitutifs de l'information collective ou individuelle: la politique de contrôle ainsi que les prérogatives de l'employeur et du personnel de surveillance; la ou les finalités poursuivies; le fait que des données personnelles soient conservées, le lieu et la durée de conservation ; le caractère permanent ou non du contrôle.

En outre, l'information individuelle porte sur l'utilisation de l'outil mis à la disposition des travailleurs pour l'exécution de leur travail, en ce compris les limites à l'utilisation fonctionnelle; les droits, devoirs, obligations des travailleurs et les interdictions éventuelles prévues dans l'utilisation des moyens de communication électronique en réseau de l'entreprise; les sanctions prévues au règlement de travail en cas de manquement.

---

[91]. Voy. Commentaire repris à l'article 6 CCT n°81.

[92]. L'article 7 CCT n°81 impose que l'employeur qui souhaite installer un système de contrôle des données de communication électroniques en réseau, informe le conseil d'entreprise sur tous les aspects du contrôle. A défaut de conseil d'entreprise, cette information est fournie au comité pour la prévention et la protection au travail ou, à défaut, à la délégation syndicale ou, à défaut, aux travailleurs.

[93]. Lors de l'installation du système de contrôle des données de communication électroniques en réseau, l'employeur informe les travailleurs concernés sur tous les aspects du contrôle. L'information fournie est effective, compréhensible et mise à jour. Le choix de son support est laissé à l'employeur. (Voy. Art. 8 CCT n°81).

II.3.3. L'individualisation des données

Cette procédure permet d'attribuer à un travailleur identifié ou identifiable une anomalie d'utilisation des moyens de communication électroniques en réseau. En effet, si l'employeur constate une anomalie dans la distribution automatisée des médicaments, il peut retracer l'identité du travailleur qui en est à l'origine. Pour être conforme, cette procédure doit observer certaines règles qui prévoient une individualisation qui peut-être directe ou indirecte[94] :

- Individualisation directe : une anomalie peut être détectée dans le cadre d'un contrôle poursuivant une ou plusieurs des finalités relatives à la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ; à la protection des intérêts économiques, commerciaux et financiers des CuSL auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires ; à la sécurité et/ou au bon fonctionnement technique des armoires à médicaments. Dans ces cas, l'employeur pourra procéder à une individualisation directe, c'est-à-dire à une identification immédiate du travailleur à l'origine de l'anomalie, sans formalités. En outre, il pourra appliquer une sanction qu'il aura prévue, par exemple, dans le règlement d'entreprise.
- Individualisation indirecte : une anomalie peut également être détectée dans le cadre d'un contrôle visant à s'assurer du respect de bonne foi des principes et règles d'utilisation des armoires à médicaments. Dans ce cas, l'individualisation des données ne sera autorisée que moyennant le respect d'une phase préalable d'information. Dans un premier temps, l'employeur doit porter à la connaissance de l'ensemble des travailleurs concernés, l'existence de l'anomalie et les avertir d'une individualisation si une nouvelle anomalie de même nature venait à être constatée. Si par la suite, de nouvelles anomalies sont constatées, l'employeur peut alors faire procéder à l'individualisation des données. Le travailleur, auquel une anomalie d'utilisation des armoires à médicaments est ainsi attribuée, sera convié à un entretien préalablement à toute décision ou évaluation susceptible de l'affecter individuellement. Cet entretien a pour but de permettre au travailleur de s'expliquer sur l'utilisation qu'il a faite des moyens de communication mis à sa disposition.

---

[94]. Voy. Stéphan Dagnelie et Marie Demoulin, « Commentaire de la convention collective de travail n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau », CRID. Disponible à l'adresse http://www.internet-observatory.be/internet_observatory/pdf/legislation/cmt/law_be_2002-04-26_cmt_fr.pdf

CONCLUSION

A l'issue de notre réflexion, il y a lieu de remarquer que la distribution automatisée des médicaments est une étape importante de l'évolution des technologies de l'information et de la communication qui aide davantage la médecine à gérer efficacement les médicaments et les prescriptions médicales.

Compte tenu du fait que, comme toute nouvelle technologie, l'avènement de la distribution automatisée des médicaments ne manque pas de s'accompagner de certains risques qui affectent les libertés fondamentales des personnes desservies, il est important qu'une telle technologie observe certaines règles susceptibles d'aider à atteindre tant les objectifs poursuivis qu'à répondre aux questions qu'elle soulève. D'où l'importance de certaines recommandations qui, dans le cas examiné, varient selon qu'il s'agit de la phase de prescription médicale électronique ou de celle de l'accès aux armoires à médicaments.

Ainsi, pour la prescription médicale électronique, nous avons vu que le système oblige le prescripteur de rédiger électroniquement son ordonnance médicale et d'envoyer l'information vers la base de données centrale en liaison avec les armoires à médicaments en vue d'une délivrance conforme à la volonté du prescripteur. L'arrêté royal du 7 juin 2009 réglemente la prescription médicale électronique et en donne les conditions en ses articles 1 et 2. Conformément à ces conditions, il convient que l'information envoyée aux armoires à médicaments:

1. comporte les renseignements ci-après: le nom et le prénom du prescripteur concerné; le numéro d'identification à l'INAMI en chiffres; le nom ou la dénomination commune du médicament; le prénom et le nom du patient, la posologie journalière du médicament et, s'il échet, la mention précisant que le médicament est destiné à un enfant ou à un nourrisson; la forme d'administration; le dosage unitaire du médicament; la mention du nombre d'unités dans le conditionnement et du nombre de conditionnements, ou la mention de la durée de la thérapie en semaines et/ou jours, ou la mention du nombre des doses à donner. Il importera, à cet effet, de veiller à ce que, par une solution technique, ces exigences fassent, par exemple, l'objet de champs obligatoires sans lesquels la prescription médicale n'est pas validée par la machine.

2. Respecte l'authentification de l'identité du prescripteur telle que voulue par l'INAMI[95] qui propose deux systèmes dont le premier est vivement conseillé: l'authentification au moyen d'un nom d'utilisateur et d'un mot de passe.

3. S'agissant des procédures de hachage, enregistrement de la prescription électronique et du hash-code y afférent et logging; d'horodatage et enregistrement des TSBags pourvus d'une estampille temporelle et d'une signature électronique: il convient d'appliquer fidèlement celles proposées par l'INAMI[96].

4. Quant au délai de conservation des prescriptions médicales électroniques: prévoir la possibilité de leur lecture pendant une période de 10 ans à compter de leur création. Il est important, pour ce faire, de mettre en place une solution technique qui empêche la suppression d'une prescription médicale électronique qui n'a pas encore dépassé 10 ans.

5. Prévoit, conformément à l'article 2 de l'arrêté royal du 7 juin 2009 réglementant la prescription médicale électronique, que toutes ces informations (1 à 4) figurent dans un protocole informatique conclu entre, d'une part, la direction de l'hôpital, le médecin en

[95]. INAMI, « Protocole dans le cadre de la prescription hospitalière électronique », p.3.
[96]. INAMI, « Protocole dans le cadre de la prescription hospitalière électronique », pp.3-4.

chef, le pharmacien titulaire ou le pharmacien en chef et le responsable du système informatique et, d'autre part, chaque médecin et praticien de l'art dentaire prescripteur. Le modèle proposé par l'INAMI et intitulé « Protocole dans le cadre de la prescription hospitalière électronique » mérite, *mutatis mutandis*, d'être adopté.

Par contre, pour l'armoire à médicaments et les opérations sur les médicaments, les données enregistrées aux fins du fonctionnement du système automatisé permettent de tracer les opérations y effectuées et ce, en traitant de données relevant de la vie privée des travailleurs et des malades. Un tel traitement doit:

1. Définir clairement les finalités poursuivies par le traitement de données, ces finalités doivent être déterminées, explicites et légitimes. Dans le cas d'espèce, les finalités ont été précisées au point relatif aux finalités poursuivies par le traitement.

2. Veiller à ce que le processus soit transparent vis-à-vis du conseil d'entreprise, des travailleurs et des patients en leur donnant les informations nécessaires quant aux *finalités poursuivies par le traitement, au nom et à l'adresse du responsable du traitement et, le cas échéant, de son représentant; l'existence d'un droit d'opposition; les destinataires ou les catégories de destinataires des données; le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse; l'existence d'un droit d'accès et de rectification des données*[97]. Particulièrement aux travailleurs, cette information précisera aussi *la politique de contrôle ainsi que les prérogatives de l'employeur et du personnel de surveillance; le fait que des données personnelles soient conservées, le lieu et la durée de conservation; le caractère permanent ou non du contrôle ; l'utilisation de la distribution automatisée des médicaments pour l'exécution de leur travail, en ce compris les limites à l'utilisation fonctionnelle; leurs droits, devoirs, obligations et les interdictions éventuelles prévues dans cette utilisation; les sanctions prévues au règlement de travail en cas de manquement*[98]. Cette information pourrait être donnée aux travailleurs par n'importe quel support, une circulaire, par exemple, et ce, avant ou dès l'instauration du système; tandis que pour les malades, elle sera donnée à chacun d'eux dans les conditions générales transmises lors de l'accueil à chaque hospitalisation. Ces derniers doivent consentir au traitement de leurs données à caractère personnel en apposant, par eux-mêmes ou par un de leurs membres de famille, leur signature sur ces conditions générales.

3. Etre notifié à la Commission de Protection de la Vie Privée (CPVP): la loi impose cette notification à titre de préalable à tout traitement de données à caractère personnel. Il semble aussi indiqué d'en faire un préalable à l'installation du système automatisé. En effet, la gestion centralisée d'empreintes digitales est souvent envisagée comme le meilleur moyen pour authentifier les utilisateurs dans leur accès aux armoires à médicaments face à une gestion ''armoire par armoire'' qui pourrait entrainer un disfonctionnement dans l'organisation de la gestion des informations. Compte tenu du *risque d'une (ré)utilisation des données pour des finalités différentes, ainsi que des risques spécifiques inhérents à un accès non autorisé, le groupe de travail 29 recommande de les soumettre au contrôle préalable de la CPVP, car un tel traitement des données présentera probablement des risques particuliers pour les droits et libertés des personnes concernées*[99]. Si donc le système est mis en place en fonction de la gestion centralisée d'empreintes digitales et que, par après, la CPVP s'y oppose, il en résulterait un dommage pour l'entreprise. La

---

[97]. Voy. Art. 9 de la loi du 8 décembre 1992.

[98]. Voy. Art. 9, CCT n°81.

[99]. Voy. Groupe 29, « Document de travail sur la biométrie », *op. cit.*

consultation de la CPVP avant l'installation du système permet à l'entreprise de choisir le système de gestion qui sera conforme aux lois et règlements.

4. Obtenir le consentement indubitable de chaque travailleur-utilisateur ou de chaque patient donné aux fins d'autoriser le traitement de ses données. A défaut de ce consentement, recourir aux exceptions telles que décrites, selon le cas, s'agissant de ''simples données ou données normales'' ou de ''données relatives à la santé''.

5. Veiller à ce que les données à récolter se limitent à celles qui sont adéquates, pertinentes et non excessives au regard des finalités poursuivies. Il sied, à cet effet, de les limiter :

   - Pour le prescripteur : à son code utilisateur en tant que prescripteur concerné; au numéro d'identification à l'INAMI en chiffres, à l'empreinte digitale ;
   - Pour le personnel soignant: à son code utilisateur concerné; à l'empreinte digitale ;
   - Pour les administrateurs : à son code administrateur concerné, à l'empreinte digitale ;
   - Pour le patient: au nom et au prénom, au nom ou à la dénomination commune du médicament, à la posologie journalière du médicament, à la mention précisant que le médicament est destiné à un enfant ou à un nourrisson, à la forme d'administration, au dosage unitaire du médicament, à la mention du nombre d'unités dans le conditionnement et du nombre de conditionnements, à la mention de la durée de la thérapie en semaines et/ou jours, ou à la mention du nombre des doses à donner.

6. Adopter une gestion centralisée qui tient compte des dispositions d'ordre pratique dont nous avons parlé[100].

7. Conserver les données biométriques du travailleur-utilisateur tant que celui-ci sera habileté à accéder aux armoires à médicaments pour le besoin des soins nécessaires aux malades. Veiller cependant à les supprimer immédiatement dès que le travailleur n'est plus en fonction pour quelque motif que ce soit ou dès que la nature de ses fonctions change de manière telle qu'il n'aura plus besoin de travailler avec les armoires à médicaments. A ce titre, une intégration avec un gestionnaire des ressources humaines est souhaitable pour automatiser les ouvertures, clôtures et suspensions d'accès.

8. Veiller à la sécurité et à la confidentialité de données à caractère personnel :

   - Dans le chef de l'employeur ou de ses représentants : il faut prévoir que *l'accès aux données et les possibilités de traitement soient limités à ce dont les utilisateurs ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service; ils ne peuvent traiter les données que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance; informer les utilisateurs des dispositions de la loi et de ses arrêtés d'exécution, ainsi que de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel; s'assurer de la conformité des programmes servant au traitement automatisé des données à caractère personnel ainsi que de la régularité de leur application; prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé; ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application*

[100]. Voy. p. 21.

de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels[101].

- Dans le chef du fournisseur: exiger, avant l'acquisition des armoires à médicaments, qu'il produise la documentation descriptive du degré d'agrément desdites armoires. Cette information permet à l'hôpital de s'engager à bon escient. Il faut, en outre, conclure un contrat de maintenance avec lui. Dans ce contrat, des obligations de confidentialité et de sécurité doivent lui être imposées. Les techniciens envoyés par le fournisseur ne peuvent, par exemple, pas copier, lors de l'entretien des armoires à médicaments ou des mécanismes de leur fonctionnement, en tout ou partie, la base de données exploitée par le système. Il faut exiger du fournisseur de préciser *les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé, ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels*[102]. Cette obligation sera scellée par des sanctions déterminées à encourir par le fournisseur en cas de violation. Le contrat de maintenance prévoira aussi la procédure à suivre en cas de violation de l'obligation de sécurité et de confidentialité.

9°. Veiller à ce que le transfert de données à caractère personnel traitées vers des pays non membres de la Communauté européenne s'effectue conformément aux règles établies par les articles 21 et 22 de la loi du 8 décembre 1992.

10°. Quant à la procédure à suivre par l'employeur en cas d'anomalie constatée dans l'utilisation de l'armoire à médicaments par les travailleurs : adopter la procédure proposée à cet effet[103].

[101]. Voy. Art. 16, §2-§4 de la loi du 8 décembre 1992.
[102]. Voy. Art. 16, §2-§4 de la loi du 8 décembre 1992.
[103]. Voy. p. 26; Stéphan Dagnelie et Marie Demoulin, *op. cit.*

BIBLIOGRAPHIE

Ouvrages

BERGER V., *Jurisprudence de la Cour Européenne des Droits de l'Homme*, 7ème éd., Dalloz, Paris, 2000, p.410

CRETTIEZ X. et PIAZZA P., *Du papier à la biométrie. Identifier les individus*, Presses de la Fondation Nationale des Sciences Politiques, Paris, 2006

De BENALCAZAR I., *Droit du travail et nouvelles technologies,* Gualino éditeur, EJA-Paris, 2003, p. 83.

DEBRAY O. et al., *Le contrat de travail et la nouvelle économie*, éd. du Jeune Barreau de Bruxelles, 2001, 342 pages.

DUNAND J Ph. et al., *Internet au lieu de travail*, CEDIDAC, Lausanne, 2004, p.96.

FENOLL-TROUSSEAU M-P. et HAAS G., *Internet et protection des données personnelles*, éd. Litec, Paris, 2000, p.1.

HERVEG J., *La protection des données du patient dans l'hôpital*, éd. Kluwer, 2009, pp.7-8.

NGONDANKOY NKOY-ea-LOONGYA, *Droit congolais des droits de l'homme*, Bruylant, 2004, p. 253.

PIERSON J., *La biométrie, l'identification par le corps*, éd. Lavoisier, 2007, pp.71-74

RENUCCI J.-F., *Droit européen des droits de l'Homme*, *LGDJ*, 2001, N°85

ROSIER K. et al., *Le droit du travail à l'ère du numérique*, Anthemis s.a., 2011, 511 pages

VAN DROOGHENBROECK S., *La Convention européenne des droits de l'homme*, Les dossiers du J.T., vol.57, Bruxelles, Larcier, 2006, n°309

VERDUSSEN M. et JOASSART P., *La vie privée au travail*, Anthemis, 2011, 163 pages

Textes de droit

Arrêté royal n° 78 du 10 nov. 1967 relatif à l'exercice des professions des soins de santé. *M.B.*, 14-11-1967

Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001, p. 7839

Arrêté royale du 10 août 2005 fixant les modalités de la prescription à usage humain, *M.B.*, 20 sept. 2005

Arrêté royal réglementant la prescription médicale électronique. *M.B.*, 7 juin 2009.

Charte des droits fondamentaux de l'Union européenne du 7 déc. 2000

Convention européenne des droits de l'homme et des libertés fondamentales du 3 nov. 1950

Convention collective de travail n° 9 du 9 mars 1972 coordonnant les accords nationaux et les conventions collectives de travail relatifs aux conseils d'entreprise conclus au sein du conseil national du travail, modifiée par les conventions collectives de travail n° 15 du 25juillet 1974, n° 34 du 27 février 1981, n° 37 du 27 novembre 1981, n° 9 bis du 29 octobre 1991 et n° 9 ter du 27 février 2008

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28/01/2981

Convention collective de travail n°39 du 13 décembre 1983 concernant l'information et la concertation sur les conséquences sociales de l'introduction des nouvelles technologies

Convention collective de travail N° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau

Directive européenne 93/42/CEE du 14/06/1993 relative aux dispositifs médicaux (*J.O.* n° L 169, 12/07/1993) telle que modifiée par la directive européenne 2007/47/CE du 5 septembre 2007, *J.O.*, 21 sept. 2007

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.* n° L 201, 31/07/2002

Loi du 20 sept 1948 portant organisation de l'économie, *M.B.*, 27-09-1948

Loi du 3 juin 1978 relative aux contrats de travail, *M.B.*, le 22-08-1978,

Loi du 08/12/1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993

Loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005

Articles, documents officiels et cours

CLAEYS T., « L'utilisation des nouvelles technologies et de l'e-mail durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », in *Le contrat de travail et la nouvelle économie,* éd. du Jeune Barreau de Bruxelles, 2001, pp.258-259

CNIL, *Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données*, p. 3. Disponible à l'adresse http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf

CPVP, Avis n° 09/06 du 21 avril 2009 relatif au projet d'arrêté royal réglementant le document électronique remplaçant, dans les hôpitaux, la prescription du professionnel des soins de santé compétent, en exécution de l'article 21, alinéa 2, de l'arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions des soins de santé

CPVP, Décision 2001/497/CE de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE

CPVP, Décision 2002/16/CE de la Commission du 27 déc. 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE

DAGNELIE S. et DEMOULIN M., « Commentaire de la convention collective de travail n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des

données de communication électroniques en réseau », CRID. Disponible à l'adresse http://www.internet-observatory.be/internet_observatory/pdf/legislation/cmt/law_be_2002-04-26_cmt_fr.pdf

DELORME A. et al. « La gestion des stupéfiants ». Disponible à l'adresse http://lickirider.free.fr/ifsi/3eme_ann%E9e/expos%E9s/La_gestion%20des%20stup.ppt

De TERWAGNE C., *Vie privée et TIC*, Fundp/Namur, 2011-2012

Document de travail adopté le 15 février 2007 par le groupe 29 sur les données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), p.9.

EASYDENTIC, « La biométrie et les produits de contrôle d'accès ». Disponible à l'adresse http://easydentic.skynetblogs.be/tag/entreprises

Groupe 29, *Document de travail sur la biométrie*, 12168/02/FR, GT 80, 1/08/2003, p.2. Disponible à l'adresse http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_fr.pdf

Groupe 29, Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin, p.9.

HERVEG J., « Quelle est la nature du consentement du patient dans le traitement de données médicales en droit européen ? », Coimbra Editora, pp. 24 et ss.

INAMI, *Protocole dans le cadre de la prescription hospitalière électronique.*

Kéfer F., « La légalité de la preuve confrontée au droit à la vie privée du salarié », in *La vie privée au travail*, Marc Verdussen et Pierre Joassart, Anthemis, 2011, p. 17.

LEVY L., « Stockage et distribution automatisée des médicaments dans l'hôpital Dodoens à Malines ». Disponible à l'adresse http://www.sixi.be/Stockage-et-distribution-automatises-des-medicaments-dans-l-hopital-Dodoens-a-Malines_a166.html

ROBERT R. et ROSIER K., « Réglementation et contrôle de l'utilisation des technologies de la communication et de l'information sur le lieu de travail », in *Le droit du travail à l'ère du numérique*, Anthemis s.a., 2011, pp. 233-234

SERVAIS J-M., « Nouvelles technologies et fragmentations des relations de travail », in *Revue tunisienne de droit social*, n°12, 2007, pp. 30-53

YLEA, « Armoire à pharmacie ». Disponible à l'adresse http://www.ylea.eu/armoire-pharmacie-d45.html

Jurisprudence

Cour EDH, Niemietz c. Allemagne, 16-12-1992, n° 251-B

Cour EDH, Z. C. Finlande, 25-02-1997, in *Recueil des arrêts et décisions* 1997-I, p. 347

Cour EDH, Amann c. Suisse, 16–02-2000, n°/no. 27798/95

Cour EDH, Rotaru c. Roumanie, 4 mai 2000, n°/no 28341/95

Cour EDH, Pretty c. R.U., n°/no. 2346/02, 29. 04. 2002

TABLE DE MATIERES P.