L'accès du patient aux *log files* de son dossier informatisé

Jean HERVEG[1]

Le déploiement des technologies de l'information et de la communication se poursuit dans le secteur des soins de santé et, chaque jour, les patients progressent dans l'appropriation de ces nouveaux outils. Ceux-ci semblent s'habituer aux dossiers informatisés, à correspondre par courrier électronique avec leur praticien professionnel ou tout simplement à trouver ses coordonnées via l'Internet. Les patients se voient offrir des dispositifs médicaux ambulatoires intégrés dans des systèmes d'information et ils peuvent ouvrir des comptes auprès de Microsoft HealthVault ou Google Health pour gérer les informations relatives à leur santé. Cette appropriation prend d'autres formes encore et c'est ainsi que, au-delà du succès bien réel du droit à la consultation du dossier de patient consacré par la loi du 22 août 2002 relative aux droits des patients, les hôpitaux et autres praticiens professionnels de la santé commencent à recevoir des requêtes de personnes désireuses d'accéder aux *log files* de leur dossier de patient. Que faut-il leur répondre ?

1. Qu'est-ce qu'un *log file* ?

Le *log file*, également appelé «fichier journal» ou «fichier de trace», est un fichier informatique conçu pour enregistrer des actions ou des événements prédéfinis susceptibles de se produire dans un système ou un logiciel informatique.

Cette définition, qui peut certainement être améliorée, appelle deux précisions. D'abord, il n'y a pas automatiquement un enregistrement des actions ou des événements qui peuvent survenir dans un système ou un logiciel informatique. Ensuite, le *log file* n'enregistre que les actions ou les événements pour lesquels il a été paramétré. Autrement dit, ce fichier ne va pas enregistrer tout ce qui peut se passer dans un système ou un logiciel informatique. Il ne contiendra que l'information qu'il lui aura été demandé de retenir, ni plus ni moins.

Présentement, nous nous intéressons aux *log files* du dossier de patient informatisé et aux informations qu'ils sont susceptibles d'enregistrer, comme l'identité de la personne ayant accédé au dossier, le moment de l'accès, l'information consultée, et les opérations réalisées lors de l'accès au dossier (quels document ou informations ont-ils été lus, copiés, modifiés, effacés, téléchargés, communiqués à un tiers, etc.?).

[1] Centre de Recherches Informatique et Droit, Faculté de droit de Namur. Avocat au barreau de Bruxelles.

2. Quel dossier de patient?

Le dossier de patient est celui que le patient est en droit de voir être tenu à jour et conservé en un lieu sûr par son praticien professionnel[2]. Ce dossier peut exister sous une forme informatique, ce qui signifie simplement que le praticien utilise un logiciel informatique pour le créer, le gérer et le conserver.

Dans cette définition[3] :

– le patient est la personne physique à laquelle des soins de santé sont dispensés, peu importe que ce soit à sa demande ou non[4];

– les soins de santé sont les services dispensés par un praticien professionnel en vue de promouvoir, déterminer, conserver, restaurer ou améliorer l'état de santé d'un patient ou de l'accompagner en fin de vie[5];

– et le praticien professionnel est soit[6] :

  • un des praticiens visés dans l'arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions des soins de santé, c'est-à-dire un praticien de l'art médical, de l'art dentaire, de l'art pharmaceutique, un(e) kinésithérapeute, un praticien de l'art infirmier, une sage-femme, un(e) secouriste-ambulancier ou un(e) paramédical(e)[7];

  • un des praticiens visés dans la loi du 29 avril 1999 relative aux pratiques non conventionnelles dans les domaines de l'art médical, de l'art pharmaceutique, de la kinésithérapie, de l'art infirmier et des professions paramédicales, c'est-à-dire un(e) homéopathe, un(e) chiropracteur, un(e) ostéopathe, un(e) acupuncteur(trice) ou tout autre praticien d'une discipline pour laquelle le Roi installerait une chambre spécifique – ce qu'il n'a pas encore fait à ce jour.

Il faut rappeler que le praticien professionnel n'est tenu de respecter les dispositions de la loi relative aux droits des patients que dans la mesure où le patient y apporte son concours[8]. Ceci a pour conséquence que si le patient empêche, de l'une ou l'autre façon, le praticien professionnel de tenir à jour ou de conserver un dossier à son nom, il ne

---

2 Article 9, § 1er, de la loi du 22 août 2002 relative aux droits des patients. Conformément à son article 3, § 1er, la loi s'applique aux rapports juridiques contractuels et extracontractuels de droit privé et de droit public dans le domaine des soins de santé dispensés par un praticien professionnel à un patient.

3 Voy. l'article 2 de la loi du 22 août 2002 précitée.

4 Article 2, 1°, de la loi du 22 août 2002 précitée.

5 Article 2, 2°, de la loi du 22 août 2002 précitée.

6 Article 2, 3°, de la loi du 22 août 2002 précitée.

7 Le Roi a fixé la liste des professions paramédicales dans un arrêté royal du 2 juillet 2009.

8 Article 4 de la loi du 22 août 2002 précitée.

pourra pas lui reprocher ultérieurement l'absence ou le caractère incomplet dudit dossier. Il est, cependant, entendu que, dans pareil cas, le praticien n'est libéré de son obligation que dans la mesure de l'empêchement qui lui aurait été opposé par le patient. Ainsi, si le patient ne s'oppose qu'à l'insertion d'une information, cela ne délivre pas le praticien professionnel de son obligation pour le surplus.

Il convient de préciser que cette interprétation ne vaut que sous l'angle de la loi relative aux droits des patients. Elle ne préjuge donc pas de l'incidence de la même opposition du patient sur l'obligation faite à son praticien professionnel de tenir un dossier à son nom en exécution d'autres dispositions légales ou réglementaires. En effet, si le droit du patient à un «dossier de patient» a pour corollaire l'obligation dans le chef de son praticien professionnel de le tenir à jour et de le conserver en lieu sûr dans la mesure où le patient exercerait son droit en ce sens[9], il n'en demeure pas moins que d'autres règles obligent des praticiens à tenir des dossiers sur leurs patients. Il ne s'agit plus seulement du corollaire d'un droit dans le chef du patient, mais bien d'une obligation formelle et expresse imposée par d'autres dispositions légales ou réglementaires au praticien professionnel concerné dans l'exercice de son activité professionnelle. Il peut donc y avoir un conflit entre la volonté du patient de ne pas voir tenu à jour ou conservé un dossier à son nom, et l'obligation faite à son praticien professionnel de le faire.

Pour s'opposer utilement à la tenue et à la conservation d'un dossier à son nom en tout ou en partie en dehors du seul champ de la loi relative aux droits du patient, le patient doit pouvoir se prévaloir d'une disposition légale ou réglementaire qui lui permette de s'y opposer, sans que cela ne soit préjudiciable au praticien professionnel. Autrement dit, la demande du patient ne peut pas faire obstacle aux obligations légales ou réglementaires qui obligent le praticien professionnel de tenir à jour ou de conserver un dossier au nom de ses patients, pas plus qu'elle ne peut l'empêcher de conserver l'information nécessaire pour se défendre en cas de mise en cause de sa responsabilité professionnelle ou empêcher l'hôpital de remplir ses obligations en matière d'agrément, de financement et de prophylaxie, surtout lorsque leur méconnaissance est érigée en infraction, comme c'est le cas pour le dossier unique du patient à l'hôpital (voy. *infra* sur ce point).

La possibilité d'un pareil conflit est d'autant plus aiguë que les obligations légales ou réglementaires imposant aux praticiens professionnels la tenue d'un dossier au nom de leurs patients sont nombreuses et diverses.

[9] Article 9, § 1er, de la loi du 22 août 2002 précitée.

De manière générale, le Code de déontologie médicale prévoit que chaque médecin doit, en principe, tenir un dossier médical pour chaque patient[10]. Cependant, le dossier médical général/dossier médical global (le DMG en abrégé dans les deux cas) ne peut être ouvert qu'à la demande du patient et c'est ce dernier qui choisira le médecin généraliste à qui il le confiera[11].

L'arrêté royal n° 78 relatif à l'exercice des professions des soins de santé impose que les prestations de soins infirmiers soient consignées dans un dossier infirmier[12].

Le médecin généraliste agréé peut obtenir une intervention annuelle de l'I.N.A.M.I. dans les frais des logiciels qu'il utilise pour la gestion électronique des dossiers médicaux, à condition que ces logiciels aient été acceptés par la Commission nationale médico-mutualiste sur avis conforme de la plate-forme eHealth, celle-ci fondant son avis sur les critères qu'elle aura fixés à ce effet après les avoir soumis à l'approbation de la même Commission nationale médico-mutualiste[13].

De même, les praticiens de l'art infirmier peuvent obtenir une intervention financière annuelle de l'I.N.A.M.I. pour l'utilisation de la télématique et pour la gestion électronique de leurs dossiers dans la mesure où ces logiciels sont homologués[14].

---

[10] Article 38 du Code de déontologie médicale.

[11] Voy. déjà l'arrêté royal du 3 mai 1999 relatif au dossier médical général.

[12] Voy. l'article 21*quinquies*, § 2, de l'arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions des soins de santé.

[13] Voy. l'arrêté royal du 6 février 2003 fixant les conditions et les modalités selon lesquelles l'assurance obligatoire soins de santé et indemnités accorde une intervention financière aux médecins pour l'utilisation de la télématique et pour la gestion électronique des dossiers médicaux.

[14] Voy. l'arrêté royal du 21 avril 2007 fixant les conditions et dispositions en vertu desquelles l'assurance obligatoire soins de santé et indemnités accorde une intervention financière aux praticiens de l'art infirmier pour l'usage de la télématique et la gestion électronique des dossiers. En exécution de l'article 33 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth, le Roi a, par arrêté du 13 janvier 2010 fixant la date d'abrogation de l'arrêté royal du 3 mai 1999 portant création d'une Commission «Normes en matière de télématique au service du secteur de soins de santé» et fixant les modalités de reprise de ses missions par la plate-forme eHealth, abrogé l'arrêté royal du 3 mai 1999 portant création de cette Commission avec effet au 1er juillet 2009. L'arrêté du 13 janvier 2010 prévoit que la plate-forme eHealth reprend d'initiative ou à la demande des ministres compétents pour ce faire, les missions particulières suivantes de la Commission «Normes en matière de télématique au service du secteur de soins de santé» :

1° formuler des recommandations techniques concernant tous les aspects susceptibles d'avoir une influence sur l'échange électronique de données en matière de soins de santé, en particulier les techniques de télécommunication, la protection, le stockage de données, l'identification de patients, le codage de données médicales, les conversions entre systèmes de codage et la structuration des messages;

2° formuler des propositions et de développer des instruments afin de pouvoir évaluer leur conformité en fonction de normes techniques;

Le Roi est également habilité à fixer les critères de base auxquels devraient répondre les logiciels de gestion du dossier médical et infirmier électronique pour pouvoir être homologués par le ministre en charge de la Santé publique[15]. Il n'a cependant pas encore fait usage de cette faculté-là à ce jour.

Le pharmacien doit tenir un dossier pharmaceutique du patient ainsi qu'un dossier de suivi des soins pharmaceutiques[16]. Chaque pharmacien-titulaire d'une officine ouverte au public a droit à une intervention unique de 500 EUR, payée par le biais des offices de tarification, pour les frais relatifs à la sécurité et à l'informatique[17].

Les hôpitaux doivent tenir[18] un dossier unique de patient qui se compose d'un dossier médical[19] et d'un dossier infirmier[20], sans oublier les obligations spécifiques imposées à certains services hospitaliers[21]. Il faut attirer l'attention sur le fait que la négligence de constituer ou de tenir à jour, pour chaque patient, un dossier médical ou infirmier hospitalier a récemment été érigée en infraction[22], ce qui semble largement excessif d'autant que cette sanction pénale n'existe pas dans d'autres situations comparables.

3° formuler des propositions en vue d'accorder entre elles les normes nationales et d'appliquer les normes européennes et internationales en matière de standardisation;

4° formuler des recommandations concernant les fonctions minimales d'un dossier médical électronique et les applications télématiques médicales en général.

[15] Ce que lui permet l'article 45*bis* de l'arrêté royal n° 78 du 10 novembre 1967, précité.

[16] Voy. l'arrêté royal du 21 janvier 2009 portant instructions pour les pharmaciens et le guide des bonnes pratiques pharmaceutiques officinales qu'il contient en annexe.

[17] Arrêté royal du 1er juillet 2006 portant application de l'article 36*undecies* de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994. Il faut noter que le Roi avait prévu 2 687 500 euros pour cette mesure – montant qui fut inscrit aux comptes de l'année comptable 2005.

[18] La direction d'un hôpital doit être assistée d'un docteur en médecine, de préférence choisi par ses pairs, conseiller technique de la direction, responsable vis-à-vis de celle-ci du fonctionnement technique, des mesures de sécurité pour le personnel et les malades, de l'application des règles de déontologie et des prescriptions légales ou réglementaires (Annexe N1, Annexe A, II. Normes d'organisation, 9°, de l'arrêté royal du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre).

[19] Articles 20, § 1er, 120, § 1er, 4°, de la loi du 10 juillet 2008 sur les hôpitaux. Le dossier médical hospitalier est mis en œuvre par l'arrêté royal du 15 décembre 1987 portant exécution des articles 13 à 17 (anciens) de la loi sur les hôpitaux, ainsi que par l'arrêté royal du 3 mai 1999 déterminant les conditions générales auxquelles le dossier médical, visé à l'article 15 de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre.

[20] Article 25, alinéa 1er, de la loi du 10 juillet 2008 sur les hôpitaux. Le dossier infirmier hospitalier est mis en œuvre par l'arrêté royal du 28 décembre 2006 déterminant les conditions générales minimales auxquelles le dossier infirmier, visé à l'article 17*quater* de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre.

[21] Voy. à ce sujet les annexes de l'arrêté royal du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre.

[22] Article 128, 11°, de la loi du 10 juillet 2008 sur les hôpitaux. À lire les dispositions relatives à l'entrée en vigueur de la loi en combinaison avec celles de la loi du 14 janvier 2002 portant des mesures en matière de soins de santé, c'est au Roi à déterminer le moment à partir duquel cette disposition entrerait en vigueur.

Le dossier médical hospitalier peut être tenu et conservé sous forme électronique[23], ainsi que le dossier infirmier hospitalier[24].

Les dossiers médicaux hospitaliers des patients doivent être classés et conservés dans des archives médicales organisées de préférence de manière centrale et électronique ou tout au moins groupées au niveau du service avec un numéro unique par patient au sein de l'hôpital. Ces dossiers doivent être accessibles en permanence aux médecins associés au traitement du patient[25].

Les dossiers infirmiers hospitaliers des patients sont classés et conservés dans des archives infirmières organisées de préférence de manière centrale et électronique ou tout au moins groupées au niveau du service avec un numéro unique par patient au sein de l'hôpital. Ces dossiers doivent être accessibles en permanence aux infirmiers associés aux soins au patient[26].

Le règlement relatif à la protection de la vie privée qui doit être établi par chaque hôpital et communiqué à chaque patient doit indiquer les catégories de personnes ayant accès ou étant autorisées à obtenir les données médicales à caractère personnel du traitement[27].

Les kinésithérapeutes peuvent aussi obtenir une intervention financière annuelle de l'I.N.A.M.I. pour l'utilisation de la télématique et pour la gestion électronique de leurs dossiers dans la mesure où ces logiciels sont homologués[28].

Les maisons de repos doivent établir pour chacun de leurs résidents, dès leur admission, un dossier individuel de soins en plus d'un dossier administratif[29].

---

[23] Article 1er, §2, de l'arrêté royal du 3 mai 1999 précité. La même disposition prévoit que le ministre qui a la Santé publique dans ses attributions peut fixer des modalités pratiques concernant l'échange électronique de données provenant du dossier médical.

[24] Article 1er, §2, de l'arrêté royal du 28 décembre 2006 précité. La même disposition prévoit que le ministre qui a la Santé publique dans ses attributions peut fixer des modalités pratiques concernant l'échange électronique de données provenant du dossier infirmier et concernant l'archivage électronique et la transformation digitale des documents du dossier infirmier.

[25] Article 6 de l'arrêté royal du 3 mai 1999 précité.

[26] Article 7 de l'arrêté royal du 28 décembre 2006 précité.

[27] Annexe N1, Annexe A, II. Normes d'organisation, 9°, de l'arrêté royal du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre.

[28] Voy. l'arrêté royal du 18 février 2005 fixant les conditions et les modalités selon lesquelles l'assurance obligatoire soins de santé et indemnités accorde une intervention financière aux kinésithérapeutes pour l'utilisation de la télématique et pour la gestion électronique des dossiers. Comme indiqué ci-dessus pour l'intervention financière aux praticiens de l'art infirmier, c'est la plate-forme eHealth qui a repris les missions de la Commission «Normes en matière de télématique au service du secteur de soins de santé».

[29] Voy. l'arrêté royal du 21 septembre 2004 fixant les normes pour l'agrément spécial comme maison de repos et de soins, comme centre de soins de jour ou comme centre pour lésions cérébrales acquises et ses annexes.

Ceci étant, il faut bien constater que toutes ces réglementations portent essentiellement sur le contenu du dossier de patient et certains de ses aspects organisationnels et techniques, mais qu'aucune n'impose de conserver les traces des accès au dossier de patient. Cette mesure n'apparaît pas plus dans les domaines énumérés pour la fixation des critères d'homologation des logiciels de gestion du dossier médical et du dossier infirmier électronique[30].

De même, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, qui s'applique au dossier de patient informatisé en raison du fait qu'il constitue un traitement automatisé de données à caractère personnel, ne contient pas non plus d'obligation expresse de mettre en œuvre des *log files*.

Par contre, elle permet d'envisager la question sous deux angles différents : celui des mesures techniques et organisationnelles destinées à assurer la sécurité du traitement de données, d'une part, et, d'autre part, celui du droit d'accès de la personne aux données à caractère personnel qui la concernent.

3. Quel lien entre les mesures techniques et organisationnelles destinées à assurer la sécurité du traitement de données et les *log files* ?

A. La prévention des usages non autorisés de données

La Cour européenne des droits de l'homme a souligné à plusieurs reprises le rôle fondamental de la protection des données pour l'exercice du droit au respect de la vie privée et familiale, d'abord en se focalisant sur les informations relatives à la santé[31], puis en étendant explicitement son propos à toutes les données à caractère personnel[32].

---

[30] En effet, l'article 45*bis*, §2, de l'arrêté royal n° 78 du 10 novembre 1967 précité dispose que :
«Les critères auxquels doivent répondre, pour être homologués, les logiciels de gestion du dossier médical et infirmier électronique peuvent concerner, entre autres, les domaines suivants : les fonctions qu'ils remplissent, les banques de données médicales et infirmières internes au logiciel et leur interchangeabilité, l'architecture du dossier du patient, la codification des affections, les applications de statistiques, d'aide au diagnostic, d'aide à la thérapeutique et à la prescription, la liste des données médicales et infirmières, anonymisées ou non, relatives à des patients, qui doivent pouvoir être échangées, ainsi que l'utilisation de la carte de sécurité sociale et la facturation aux organismes assureurs».

[31] Cour eur. D.H., arrêt du 25 février 1997, *Z c. Finlande*, n° 22009/93, §95 ; arrêt du 27 août 1997, *M.S. c. Suède*, n° 20837/92, §41 ; arrêt du 17 juillet 2008, *I. c. Finlande*, n° 20511/03, §38. Voy. aussi : Cour eur. D.H., arrêt du 25 novembre 2008, *Biriuk c. Lituanie*, n° 23373/03, §§39 et 43 ; arrêt du 25 novembre 2008, *Armonas c. Lituanie*, n° 36919/02, §§40 et 44 ; arrêt du 28 avril 2009, *K.H. et autres c. Slovaquie*, n° 32881/04, §55 ; arrêt du 6 octobre 2009, *C.C. c. Espagne*, n° 1425/06, §31.

[32] Cour eur. D.H., arrêt du 4 décembre 2008, *S. et Marper c. Royaume-Uni*, n° 30562/04 et 30566/04, §103.

S'agissant des informations sur la santé, la Cour a insisté sur le fait que le respect de leur caractère confidentiel constituait un principe essentiel du système juridique de toutes les parties contractantes à la Convention et qu'il était capital non seulement pour protéger la vie privée des malades, mais également pour préserver leur confiance dans le corps médical et les services de santé en général[33]. Faute d'une telle protection, la Cour a formulé la crainte selon laquelle les personnes nécessitant des soins médicaux pourraient être dissuadées de fournir les informations à caractère personnel et intime nécessaires à la prescription du traitement approprié et même de consulter un médecin, ce qui pourrait mettre en danger leur santé, voire, dans le cas des maladies transmissibles, celle de la collectivité[34].

La Cour a attiré l'attention sur le fait que ces considérations valaient particulièrement lorsqu'il s'agissait de protéger la confidentialité des informations relatives à la séropositivité puisque leur divulgation pouvait avoir des conséquences dévastatrices sur la vie privée et familiale de la personne concernée ainsi que sur sa situation sociale et professionnelle, l'exposant à l'opprobre et à un risque d'exclusion. Elle a exprimé la crainte que certaines personnes se laissent dissuader de se soumettre à un diagnostic ou à un traitement, sapant ainsi les efforts de la collectivité pour contenir la pandémie. Par voie de conséquence, elle a indiqué que l'intérêt à protéger la confidentialité des informations relatives à la séropositivité devait peser lourdement dans la balance lorsqu'il s'agissait de déterminer si une ingérence était proportionnée au but légitime poursuivi, celle-ci ne pouvant se concilier avec l'article 8 que si elle vise à défendre un aspect primordial de l'intérêt public[35].

C'est dans ce contexte que la Cour a affirmé que la législation interne des parties contractantes à la Convention devait 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 de la Convention[36]. Elle a, ensuite, étendu cette obligation à toutes les données à caractère personnel[37].

---

[33] Cour eur. D.H., arrêt du 25 février 1997, *Z c. Finlande*, n° 22009/93, §95; arrêt du 27 août 1997, *M.S. c. Suède*, n° 20837/92, §41; arrêt du 17 juillet 2008, *I. c. Finlande*, n° 20511/03, §38. Voy. aussi : Cour eur. D.H., arrêt du 25 novembre 2008, *Biriuk c. Lituanie*, n° 23373/03, §§39 et 43; arrêt du 25 novembre 2008, *Armonas c. Lituanie*, n° 36919/02, §§40 et 44; arrêt du 28 avril 2009, *K.H. et autres c. Slovaquie*, n° 32881/04, §55; arrêt du 6 octobre 2009, *C.C. c. Espagne*, n° 1425/06, §31.

[34] Cour eur. D.H., arrêt du 25 février 1997, *Z c. Finlande*, n° 22009/93, §95; arrêt du 6 octobre 2009, *C.C. c. Espagne*, n° 1425/06, §31.

[35] Cour eur. D.H., arrêt du 25 février 1997, *Z c. Finlande*, n° 22009/93, §96; arrêt du 6 octobre 2009, *C.C. c. Espagne*, n° 1425/06, §33.

[36] Renvoyant, *mutatis mutandis*, aux articles 3, §2.*c*, 5, 6 et 9 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des Traités européens n° 108, Strasbourg, 1981 : Cour eur. D.H., arrêt du 25 février 1997, *Z c. Finlande*, n° 22009/93, §95; arrêt du 27 août 1997, *M.S. c. Suède*, n° 20837/92, §41; arrêt du 17 juillet 2008, *I. c. Finlande*, n° 20511/03, §38; arrêt du 6 octobre 2009, *C.C. c. Espagne*, n° 1425/06, §32; arrêt du 4 décembre 2008, *S. et Marper c. Royaume-Uni*, n^{os} 30562/04 et 30566/04, §103.

[37] Cour eur. D.H., arrêt du 4 décembre 2008, *S. et Marper c. Royaume-Uni*, n^{os} 30562/04 et 30566/04, §103.

Ceci étant, parallèlement, la Cour a admis que la protection de la confidentialité des données médicales, qui est dans l'intérêt du patient comme de la collectivité dans son ensemble, pouvait parfois s'effacer devant la nécessité d'enquêter sur des infractions pénales, d'en poursuivre les auteurs et d'assurer la publicité des procédures judiciaires (en se référant à l'article 9 de la Convention n° 108 précitée), lorsqu'il est prouvé que ces derniers intérêts revêtent une importance encore plus grande[38].

Dans l'arrêt *S. et Marper c. Royaume-Uni*, la Cour a rappelé que, s'agissant de données à caractère personnel soumises à un traitement automatique à des fins policières, le droit interne devait, notamment, assurer que ces données étaient pertinentes et non excessives par rapport aux finalités pour lesquelles elles étaient enregistrées et qu'elles étaient conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles étaient enregistrées. Elle a souligné le fait que le droit interne devait contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs. La Cour a encore souligné le fait que ces considérations valaient tout spécialement lorsqu'était en jeu la protection de catégories particulières de données plus sensibles, notamment des données ADN, qui, dans la mesure où elles contenaient le patrimoine génétique de la personne, revêtaient une grande importance tant pour elle-même que pour sa famille[39].

B. Un aspect de cette prévention : les mesures techniques et organisationnelles destinées à assurer la sécurité d'un traitement de données

Afin de garantir la protection de la personne concernée contre les usages non autorisés de données à caractère personnel, la loi du 8 décembre 1992 impose au responsable de leur traitement de veiller à ce que les données soient traitées loyalement et licitement, que leur collecte soit faite pour des finalités déterminées explicites et légitimes et qu'elles ne soient pas traitées ultérieurement de façon incompatible, qu'elles soient adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et traitées, et aussi qu'elles soient 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 ont été obtenues et traitées[40]. La loi consacre dans le chef de la personne concernée un droit à l'information sur le traitement des données qui

[38] Cour eur. D.H., arrêt du 25 février 1997, *Z c. Finlande*, n° 22009/93, §97.
[39] Cour eur. D.H., arrêt du 4 décembre 2008, *S. et Marper c. Royaume-Uni*, n^{os} 30562/04 et 30566/04, §103.
[40] Article 4 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.

la concerne, des droits d'accès et de rectification, ainsi qu'un droit d'opposition et un droit à réparation dans des hypothèses précises[41].

Outre la déclaration préalable du traitement auprès de la Commission de la protection de la vie privée, la loi du 8 décembre 1992 impose aussi au responsable du traitement de prendre toute une série de mesures destinées à assurer la confidentialité et la sécurité du traitement des données à caractère personnel. Il doit, notamment, veiller à ce que, pour les personnes agissant sous son autorité ou celle de son sous-traitant, 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 requis pour les nécessités du service, étant précisé que les personnes agissant sous l'autorité du responsable du traitement ou de son sous-traitant et qui accèdent à des données à caractère personnel ne peuvent les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance[42]. S'agissant de données à caractère personnel relatives à la santé, le responsable du traitement ou son sous-traitant doit désigner les catégories de personnes ayant accès aux données avec une description précise de leur fonction par rapport au traitement des données[43].

Plus particulièrement, afin d'assurer la sécurité du traitement de données, la même loi prévoit que le responsable du traitement doit «(…) 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 de données à caractère personnel» étant entendu que «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»[44].

C. Qu'en est-il des log files*?*

À s'en tenir à la lettre de ces dispositions dont le libellé coïncide quasiment avec celui des dispositions correspondantes de la directive 95/46/CE 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, la loi du 8 décembre 1992 ne prévoirait que l'obligation de prendre des mesures de sécurité *préventives* afin de garantir la protection de la personne à l'égard des traitements de données à caractère personnel. Ceci signifierait que le respon-

[41] Articles 9 à 15*bis* de la loi du 8 décembre 1992.
[42] Article 16 de la loi du 8 décembre 1992.
[43] Article 25, 1°, de l'arrêté royal du 13 février 2001.
[44] Article 16, §4, de la loi du 8 décembre 1992.

sable du traitement ne serait pas obligé de prendre des mesures de sécurité *a posteriori*, comme, par exemple, des mesures de contrôle. Pour le dire autrement, la prévention des usages (traitements) non autorisés de données à caractère personnel n'imposerait que la mise en place de polices d'accès, mais pas de *log files*, ces derniers répondant en ce sens à une mesure de contrôle, c'est-à-dire à une mesure de sécurité *a posteriori*.

Cette interprétation, même si elle peut se prévaloir d'arguments tirés d'une lecture (trop) littérale des textes, ne nous paraît pas devoir être retenue. En effet, il ne peut être sérieusement contesté que les *log files* représentent une mesure de sécurité majeure dans les traitements de données à caractère personnel, fut-ce par leur effet dissuasif à l'encontre des contrevenants potentiels, et qui ne se conçoit que liée à un système performant d'identification des personnes et de leurs actions.

Mais le fait que les *log files* fassent partie de l'éventail des mesures techniques et organisationnelles susceptibles d'assurer la sécurité d'un traitement de données n'implique pas que tout système ou logiciel informatique qui tombe sous le coup de la loi du 8 décembre 1992 doit en être pourvu, contrairement à ce que semble affirmer la Commission de la protection de la vie privée dans sa note sur les mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel. En effet, les mesures techniques et organisationnelles destinées à garantir la sécurité d'un traitement de données «(…) 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»[45]. Leur mise en œuvre n'est donc pas automatique.

Le rapport explicatif de la Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ne dit pas autre chose lorsqu'il expose que «Des mesures spécifiques de sécurité devraient être prises pour chaque fichier en fonction de sa vulnérabilité, de la nécessité d'en restreindre l'accès dans le cadre de l'organisation, des impératifs d'un enregistrement à long terme, etc. Les mesures de sécurité doivent être appropriées, c'est-à-dire adaptées aux fonctions spécifiques du fichier et proportionnées aux risques encourus. Enfin, elles doivent être fondées sur l'état actuel des connaissances relatives aux méthodes et techniques de sécurité dans le domaine de l'informatique»[46].

La directive 95/46/CE le confirme aussi lorsqu'elle considère que «(…) la protection des droits et libertés des personnes concernées à l'égard du traitement de données à caractère personnel exige que des mesures techniques et d'organisation appropriées soient prises

[45] Article 16, §4, de la loi du 8 décembre 1992.

[46] Rapport explicatif de la Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, n° 108, point 49.

tant au moment de la conception qu'à celui de la mise en œuvre du traitement, en vue d'assurer en particulier la sécurité et d'empêcher ainsi tout traitement non autorisé; qu'il incombe aux États membres de veiller au respect de ces mesures par les responsables du traitement; que ces mesures doivent assurer un niveau de sécurité approprié tenant compte de l'état de l'art et du coût de leur mise en œuvre au regard des risques présentés par les traitements et de la nature des données à protéger»[47].

La réponse à la question de savoir si des *log files* doivent être prévus pour un traitement de données à caractère personnel dépend donc d'une analyse au cas par cas et mettant en œuvre ces différents critères[48].

À cet égard, il n'est pas inutile de rappeler que plus un traitement de données présente des risques pour la personne concernée, que ce soit par la finalité poursuivie ou par le contenu informationnel de la donnée traitée, plus grande sera la nécessité de prévenir et réprimer les usages (traitements) non autorisés des données à caractère personnel.

De la même façon, la détermination des actions ou événements à enregistrer va dépendre de ce qui va fonder l'effet dissuasif et rendre efficace la répression des usages (traitements) non autorisés.

Il faut bien percevoir que la mise en œuvre de cette mesure est de nature à influencer favorablement l'analyse de la légitimité du traitement de données considéré, comme son absence pourrait produire l'effet contraire.

---

[47] Considérant n° 46 de la directive 95/46/CE 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. En conséquence, l'article 17.1 de cette directive dispose que :
«Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.
Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger».
L'article 4.1*bis* de la 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) dispose que les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité des services offerts par un fournisseur d'un service de communications électroniques accessible au public doit pour le moins assurer la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.

[48] Par contre, le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et les organes communautaires et à la libre circulation de ces données, prévoit expressément qu'il doit être gardé une trace des données à caractère personnel qui ont été communiquées, du moment où elles l'ont été et de leur destinataire, et qu'il soit garanti qu'il sera possible de vérifier *a posteriori* quelles données à caractère personnel ont été traitées, à quel moment et par quelles personnes (art. 22.2, points *f* et *g*).

En matière de protection des données médicales, le Comité des ministres du Conseil de l'Europe recommande que les mesures techniques et d'organisation garantissent que l'on puisse vérifier et constater *a posteriori* qui a eu accès au système d'information et quelles données y ont été introduites, à quel moment et par quelle personne[49].

Dans son document de travail sur les dossiers médicaux électroniques, le Groupe 29 indique que le cadre juridique concernant les mesures de sécurité devrait prévoir, en particulier, la nécessité «de l'enregistrement et de la documentation exhaustifs de toutes les étapes de traitement qui ont eu lieu dans le système, en particulier les demandes d'accès pour lecture ou écriture, assortis de contrôles internes réguliers et du contrôle de l'authenticité de l'autorisation»[50].

La Cour européenne des droits de l'homme a été saisie du cas d'une infirmière qui avait vu son contrat de travail non renouvelé après que des rumeurs aient circulé sur son état de santé. Celle-ci avait échoué à obtenir la réparation de son préjudice devant les juridictions finlandaises qui considéraient qu'elle ne rapportait pas la preuve d'un accès non autorisé à son dossier médical tenu dans l'hôpital où elle travaillait[51]. Devant la Cour, la requérante s'est plaint de la défaillance de l'hôpital à garantir la sécurité de ses données médicales contre des accès non autorisés, ou, au sens de la Convention, d'un manquement de la Finlande à son obligation positive de garantir le respect de sa vie privée par un système de règles de protection de données et de sauvegardes[52].

La Cour a noté qu'au regard du droit finlandais, le responsable du traitement devait garantir que les données à caractère personnel étaient protégées de manière adéquate contre les accès non autorisés et que seul le personnel en charge du patient pouvait accéder à son dossier[53].

La Cour a noté qu'il était incontestable que l'objectif de ces dispositions légales était de protéger les données à caractère personnel contre le risque d'accès non autorisés. Elle a rappelé, à cet égard, que le besoin de garanties suffisantes était particulièrement important lors du traitement de données hautement intimes et sensibles comme en l'espèce, où, de plus, la personne concernée travaillait dans l'hôpital où elle était soignée[54].

---

[49] Annexe à la Recommandation n° R (97) 5 du Comité des ministres aux États membres relative à la protection des données médicales adoptée le 13 février 1997 lors de la 584e réunion des délégués des ministres, point 9.2. Dans le même sens, voy. le point 11.2 de l'annexe à la Recommandation Rec (2002) 9 du Comité des ministres aux États membres sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance adoptée le 18 septembre 2002 lors de la 808e réunion des délégués des ministres.

[50] Groupe de travail «Article 29» sur la protection des données, «Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)», adopté le 15 février 2007, WP 131, p. 22.

[51] Cour eur. D.H., arrêt du 17 juillet 2008, *I. c. Finlande*, n° 20511/03.

[52] Cour eur. D.H., arrêt du 17 juillet 2008, *I. c. Finlande*, n° 20511/03, §37.

[53] Cour eur. D.H., arrêt du 17 juillet 2008, *I. c. Finlande*, n° 20511/03, §39.

[54] Cour eur. D.H., arrêt du 17 juillet 2008, *I. c. Finlande*, n° 20511/03, §40.

Mais, ici, le système des dossiers médicaux ne permettait pas de connaître l'usage qui avait été fait des dossiers patients dans la mesure où il ne mentionnait que les cinq consultations les plus récentes et que cette information était elle-même effacée dès que le dossier retournait aux archives. Pour cette raison, il n'était pas possible de savoir s'il y avait eu, ou non, un accès non autorisé aux dossiers de patient de la requérante et de sa famille. La Cour a noté, pour sa part, qu'il n'était pas contesté qu'à l'époque, le système qui prévalait à l'hôpital permettait aussi la lecture des dossiers par du personnel qui ne participait pas directement aux soins de la requérante[55].

Dans la mesure où la requérante avait perdu son procès en réparation au motif qu'elle ne rapportait pas la preuve de la relation causale entre les déficiences dans les règles relatives à la sécurité de l'accès et la divulgation des informations relatives à sa condition médicale, la Cour a considéré que mettre cette preuve à sa charge négligeait le fait que les déficiences dans la conservation du dossier par l'hôpital étaient reconnues. Elle a souligné le fait qu'il était évident que si l'hôpital avait mieux protégé l'accès aux dossiers médicaux en restreignant leur accès aux professionnels de la santé directement impliqués dans le traitement de la requérante ou en conservant un registre de toutes les personnes qui avaient eu accès au dossier médical de la requérante, celle-ci aurait été mise dans une situation moins défavorable devant les juridictions internes ayant eu à connaître de son action en responsabilité. Pour la Cour, ce qui est décisif, c'est que le système de dossiers mis en place à l'hôpital n'était clairement pas en conformité avec les exigences légales qui lui étaient applicables, élément auquel les juridictions nationales n'avaient pas accordé l'importance qu'il convenait de lui reconnaître à son estime[56].

La Cour a relevé, en outre, que le Gouvernement finlandais n'avait pas expliqué les raisons pour lesquelles les garanties offertes par le droit national n'avaient pas été respectées dans cet hôpital et elle a noté que ce ne fut qu'après la plainte de la requérante qu'un contrôle rétrospectif de l'accès aux données fut mis en place[57].

La Cour a indiqué que la possibilité d'obtenir une indemnisation pour le dommage causé par une divulgation non autorisée de données à caractère personnel n'était pas suffisante pour protéger le droit à la vie privée. Ce qui était requis en premier est une protection réelle et effective qui exclut toute possibilité d'accès non autorisé[58].

Il ressort des développements qui précèdent que, s'agissant du dossier de patient informatisé, il est raisonnable de soutenir que des *log files* doivent enregistrer les événements per-

[55] Cour eur. D.H., arrêt du 17 juillet 2008, *I. c. Finlande*, n° 20511/03, §41.
[56] Cour eur. D.H., arrêt du 17 juillet 2008, *I. c. Finlande*, n° 20511/03, §44.
[57] Cour eur. D.H., arrêt du 17 juillet 2008, *I. c. Finlande*, n° 20511/03, §45.
[58] Cour eur. D.H., arrêt du 17 juillet 2008, *I. c. Finlande*, n° 20511/03, §47.

mettant à tout le moins de savoir qui a fourni ou modifié quelle information, qui a accédé à quoi, quand et ce qu'il en a fait, même dans le cas d'une pratique libérale isolée.

D. Quel est le statut de la personne dont les actions sont enregistrées par les log files*?*

Sauf à leur enlever une grande partie de leur utilité, le fonctionnement des *log files* d'un dossier de patient informatisé requiert de pouvoir identifier les utilisateurs et tracer leurs actions dans le système ou le logiciel informatique. Il s'agit donc bien d'un traitement de données à caractère personnel devant répondre à l'ensemble des conditions posées par la loi du 8 décembre 1992. La personne dont les actions sont enregistrées par les *log files* possède, dès lors, la qualité de personne concernée. Il faut insister, à cet égard, sur son droit à être informée de l'existence de cet enregistrement[59] et à pouvoir accéder aux données qui la concernent et qui font l'objet du traitement. Il faut aussi rappeler que ce traitement de données ne sera légitime que dans la mesure où cette mesure de sécurité est elle-même justifiée.

E. Que faut-il faire avec les log files*?*

Il ne suffit pas de savoir que les *log files* représentent une mesure de sécurité obligatoire pour les dossiers de patient informatisés, encore faut-il savoir ce qu'il faut en faire. La réponse à cette question est fort simple : il convient de les éplucher afin de détecter toute opération non autorisée dans le dossier de patient informatisé[60]. Certains pourraient considérer que cette mesure serait excessivement coûteuse en temps et en personnel. Il existe, toutefois, des logiciels susceptibles de réaliser ce contrôle de manière tout à fait satisfaisante.

4. Quel est le lien entre le droit d'accès de la personne aux données qui la concernent et les *log files*?

La personne concernée a le droit d'obtenir de la personne responsable du traitement de ses données à caractère personnel, la confirmation du fait que des données la concernant sont ou non traitées, ainsi que des informations portant au moins sur les catégories de données

[59] Sauf à pouvoir se prévaloir de l'impossibilité visée à l'article 30 de l'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.

[60] Le Groupe 29 le confirme : «il faut prévoir des contrôles internes et externes réguliers des listes d'accès. (…)» (Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007, WP 131, p. 24).

sur lesquelles porte le traitement et les catégories de destinataires auxquels les données sont communiquées. Elle a également le droit d'obtenir la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données[61].

Toutefois, la personne concernée n'a que le droit, directement ou avec l'aide d'un praticien professionnel en soins de santé, de *prendre connaissance* des données à caractère personnel traitées en ce qui concerne sa santé[62]. Cette restriction au droit d'accès s'appuie sur la faculté qui serait offerte en ce sens par l'article 13.1 de la directive 95/46/CE.

En tout état de cause, ces dispositions ne portent pas préjudice au droit du patient à la consultation du dossier le concernant à l'exclusion des annotations personnelles du praticien professionnel et des données concernant des tiers[63].

À première vue, rien de tout ceci ne permet de justifier un quelconque droit du patient d'accéder aux *log files* de son dossier informatisé.

Heureusement, la Cour de justice de l'Union européenne a apporté quelques éclaircissements à ce sujet dans un arrêt du 7 mai 2009[64]. Dans cette affaire, M. Rijkeboer avait demandé au Collège de Rotterdam de l'informer de tous les cas où des informations le concernant et provenant de l'administration communale avaient été communiquées à des personnes tierces au cours des deux années précédant sa demande. Il désirait connaître l'identité de ces personnes et le contenu de l'information qui leur avait été transmise. Il avait déménagé dans une autre commune et souhaitait savoir, en particulier, à qui son ancienne adresse avait été communiquée. Il n'a reçu de réponse que pour l'année précédant sa demande, les données antérieures ayant été automatiquement effacées conformément à la loi des Pays-Bas relative aux données personnelles détenues par les administrations communales.

C'est à l'occasion de ce litige que la Cour de justice eut l'occasion de répondre à la question de savoir si le droit d'accès d'une personne à l'information sur les destinataires ou les catégories de destinataires de données à caractère personnel la concernant ainsi que sur le

---

[61] Article 10, §1er, de la loi du 8 décembre 1992. L'exercice du droit d'accès est décrit aux articles 32 à 35 de l'arrêté royal du 13 février 2001. Elle a aussi le droit d'obtenir connaissance de la logique qui sous-tend tout traitement automatisé des données le concernant, dans le cas des décisions automatisées, et un avertissement de la faculté d'exercer ses droits de rectification et d'opposition, et, éventuellement, de consulter le registre public des traitements de données à caractère personnel.

[62] Article 10, §2, de la loi du 8 décembre 1992. La loi précise que la communication peut être effectuée par l'intermédiaire d'un professionnel des soins de santé choisi par la personne concernée, à la demande du responsable du traitement ou de la personne concernée.

[63] Article 9, §2, alinéa 1er, de la loi du 22 août 2002.

[64] C.J.U.E., arrêt du 7 mai 2009, C-553/07, *College van burgemeester en wethouders van Rotterdam c. M. E.E. Rijkeboer*.

contenu des données communiquées pouvait être limité à la période d'un an précédant la demande d'accès.

La Cour de justice a d'abord rappelé que le droit d'accès doit, notamment, permettre à la personne concernée de s'assurer de l'exactitude des données qui la concernent et qui font l'objet d'un traitement, ainsi que de la licéité de leur traitement[65]. Elle a aussi rappelé que la personne concernée devait disposer d'un recours juridictionnel en cas de violation des droits qui lui étaient reconnus et que le responsable du traitement lui devait réparation pour le dommage subi du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales en matière de traitements de données[66].

La Cour de justice a, ensuite, constaté que l'obligation de conserver les données sous une forme permettant l'identification de la personne concernée durant une période qui n'excède pas celle nécessaire à la réalisation de la finalité poursuivie par le traitement des données, ainsi que le droit d'accès et le droit à l'information sur les destinataires et les catégories de destinataires des données visaient à protéger la personne concernée.

Elle a noté que la juridiction de renvoi cherchait à savoir s'il existait un lien entre ces deux éléments, en ce sens que le droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données à caractère personnel ainsi que sur le contenu des données transmises, pourrait dépendre de la durée de conservation des données[67]. Pour les uns, une fois les données effacées, le droit d'accès disparaissait par voie de conséquence. Pour les autres, le droit d'accès concerne non seulement le temps présent, mais également la période antérieure à la demande d'accès, sans qu'il y ait toutefois unanimité sur la durée précise du droit d'accès[68], lequel n'est pas précisé par la directive[69].

Afin de trancher la question, la Cour de justice va prendre en compte les données concernées et puis se référer à la finalité du droit d'accès tel que considéré dans le cas d'espèce[70].

Elle a ainsi opéré une distinction, judicieuse, entre, d'une part, les données (à caractère personnel) de base et, d'autre part, les informations sur les destinataires ou les catégories de destinataires auxquels les données de base sont communiquées et sur le contenu des données de base. Autrement dit, cette seconde catégorie d'informations porte sur le traitement des données de base[71]. La Cour constate qu'en l'espèce, la limitation du droit d'accès ne porte que sur les informations portant sur le traitement des données de base.

---

65 Considérant n° 6 de l'arrêt du 7 mai 2009 précité.
66 Considérant n° 18 de l'arrêt du 7 mai 2009.
67 Considérants nos 32 à 35 de l'arrêt du 7 mai 2009.
68 Considérants nos 36 à 39 de l'arrêt du 7 mai 2009.
69 Considérant n° 54 de l'arrêt du 7 mai 2009.
70 Considérant n° 40 de l'arrêt du 7 mai 2009.
71 Considérant n° 43 de l'arrêt du 7 mai 2009.

La question à résoudre porte alors sur la conformité de cette limitation dans le temps du droit d'accès à ces données au regard de sa finalité[72]. À cet égard, la Cour de justice rappelle que le droit d'accès est nécessaire à la personne concernée pour exercer ses droits de rectification, d'effacement, de verrouillage des données et son droit d'obtenir la notification de ces rectification, effacement ou verrouillage aux tiers auxquels les données ont été communiquées si cela ne s'avère pas impossible ou ne présuppose pas un effort disproportionné[73]. Elle rappelle aussi que le droit d'accès permet à la personne concernée d'exercer son droit d'opposition au traitement de ses données et son droit de recours en cas de dommage[74].

La Cour de justice considère que, pour assurer l'effet utile de ces différents droits, le droit d'accès concerne nécessairement le passé. En effet, si tel n'était pas le cas, la personne intéressée ne serait pas en mesure d'exercer de manière effective son droit de faire rectifier, effacer ou verrouiller les données présumées illicites ou incorrectes ainsi que d'introduire un recours juridictionnel et d'obtenir la réparation du préjudice subi[75].

Il ne demeure, dès lors plus, que la question de l'étendue du droit d'accès dans le passé[76].

À ce propos, la Cour a rappelé que le délai du droit d'accès à l'information sur les destinataires ou les catégories de destinataires et le contenu des données communiquées devait permettre à la personne concernée d'exercer les différents droits prérappelés[77] et que la durée de conservation des données de base pouvait constituer un paramètre utile, mais pas nécessairement déterminant[78].

Elle a indiqué que lorsque la durée de conservation des données de base était très longue, l'intérêt de la personne concernée d'exercer les droits qui lui sont reconnus, pouvait, dans certains cas, diminuer. Ainsi, lorsque les destinataires des données sont nombreux ou que la fréquence de communications à un nombre plus restreint de destinataires est élevée, l'obligation de conserver aussi longtemps que les données de base l'information sur les destinataires ou les catégories de destinataires ainsi que sur le contenu des données communiquées, pourrait représenter une charge excessive pour le responsable du traitement[79], ce qui, à ses yeux, ne peut pas être exigé sur pied de la directive 95/46/CE[80]. Pour appuyer une telle interprétation, la Cour de justice a rappelé plusieurs cas dans lesquels la directive 95/46/CE permettait d'échapper à des charges excessives[81] :

---

72 Considérant n° 45 de l'arrêt du 7 mai 2009.
73 Considérant n° 51 de l'arrêt du 7 mai 2009.
74 Considérant n° 52 de l'arrêt du 7 mai 2009.
75 Considérant n° 54 de l'arrêt du 7 mai 2009.
76 Considérant n° 55 de l'arrêt du 7 mai 2009.
77 Considérant n° 57 de l'arrêt du 7 mai 2009.
78 Considérant n° 58 de l'arrêt du 7 mai 2009.
79 Considérant n° 59 de l'arrêt du 7 mai 2009.
80 Considérant n° 60 de l'arrêt du 7 mai 2009.
81 Considérants n^{os} 61 à 63 de l'arrêt du 7 mai 2009.

– lorsque l'obligation du responsable du traitement de notifier aux tiers auxquels les données ont été communiquées les rectifications, effacement ou verrouillage s'avérait impossible ou impliquait un effort disproportionné;

– lorsque le nombre des personnes concernées et l'ancienneté des données peuvent être pris en compte pour justifier une exception à l'obligation d'informer la personne sur le traitement de données qui la concernent;

– lorsque le responsable du traitement doit mettre en œuvre des mesures techniques et d'organisation destinées à assurer un niveau de sécurité qui soit approprié au regard des risques présentés par le traitement et de la nature des données à protéger, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre.

La Cour de justice a, par voie de conséquence, considéré qu'un raisonnement identique était pertinent pour fixer le délai d'accès à l'information sur les destinataires ou les catégories de destinataires et sur le contenu des données communiquées. Ainsi, outre le fait que le délai du droit d'accès doit permettre à la personne concernée d'exercer les différents droits qui lui sont reconnus en matière de traitements de données, il fallait aussi tenir compte du délai prévu par le droit national pour introduire un recours, la nature plus ou moins sensible des données de base, la durée de conservation des données de base et le nombre de destinataires concernés[82].

En résumé, la Cour de justice a jugé qu'il appartenait «(…) aux États membres de fixer un délai de conservation de l'information sur les destinataires ou les catégories de destinataires et le contenu des données communiquées et de prévoir un accès à cette information qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des droits de rectification, d'effacement et de verrouillage des données, en cas de non-conformité du traitement de celles-ci avec la directive, ainsi que des droits d'opposition et d'introduction d'un recours juridictionnel et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement»[83], tout en tenant compte de l'obligation de conserver les données sous une forme permettant l'identification de la personne concernée pendant une durée qui n'excède pas celle nécessaire pour réaliser les finalités pour lesquelles elles ont été collectées ou pour lesquelles elles sont traitées ultérieurement[84].

Dans le cas de M. Rijkeboer, la Cour de justice a estimé que la limite à la conservation et, par là, à l'accès à l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an, alors que les données de base sont conservées beaucoup plus longtemps, ne représentait pas un juste équilibre

[82] Considérant n° 63 de l'arrêt du 7 mai 2009.
[83] Considérant n° 64 de l'arrêt du 7 mai 2009.
[84] Considérant n° 65 de l'arrêt du 7 mai 2009.

des intérêts et obligations en présence, à moins qu'il ne soit démontré qu'une conservation plus longue constituerait une charge excessive pour le responsable du traitement[85].

Il résulte de cet arrêt que le droit d'accès aux données à caractère personnel comporte assurément en germe celui d'accéder aux *log files*.

Toutefois, en droit belge, il convient de tenir compte de la restriction au droit d'accès de la personne concernée de seulement *prendre connaissance* des données à caractère personnel traitées en ce qui concerne sa santé. Si cette restriction peut être défendue en ce qui concerne les données de base du traitement, il ne semble toutefois pas possible de la défendre en ce qui concerne la seconde catégorie d'informations dégagée par la Cour de justice, étant celles qui portent sur le traitement des données de base, comme les informations sur les destinataires ou les catégories de destinataires auxquels les données de base sont communiquées et sur le contenu des données de base[86]. À mon sens, cette restriction serait disproportionnée et donc non conforme à l'article 13.1 de la directive 95/46/CE, sans préjudice de son appréciation au regard du droit au respect de la vie privée. Le même raisonnement me paraît devoir être tenu en ce qui concerne le droit d'obtenir toute information disponible sur l'origine des données.

Il reste, toutefois, à s'entendre sur la durée de ce droit d'accès dans le passé aux informations sur le traitement des données de base et sur les informations à conserver en ce qui concerne le dossier de patient informatisé. Il me semble que la durée de ce droit d'accès doit coïncider au minimum avec les délais de prescription des droits en cause et que les informations sur les traitements de données de base doivent permettre la mise en œuvre des droits du patient tant au regard de la loi relative aux droits des patients que de la loi du 8 décembre 1992, c'est-à-dire, à tout le moins, savoir qui a fourni ou modifié quelle information, qui a accédé à quoi, quand et ce qu'il en a fait, même dans le cas d'une pratique libérale isolée.

Conçu de cette façon, le droit d'accès aux informations sur le traitement de données de base consoliderait la légitimité de la finalité poursuivie par le traitement de données.

---

[85] Considérant n° 66 de l'arrêt du 7 mai 2009.

[86] La raison qui justifierait que la personne concernée n'aurait pas non plus le droit d'obtenir la confirmation que des données la concernant sont ou ne sont pas traitées, d'obtenir des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte, d'obtenir toute information disponible sur l'origine de ces données et la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant dans le cas des décisions automatisées, d'obtenir un avertissement de la faculté d'exercer les droits de rectification et d'opposition et, éventuellement, de consulter le registre public des traitements de données à caractère personnel, n'apparaît pas au premier coup d'œil.

5. La communication spontanée des *log files* au patient

Même s'il porte aussi sur les destinataires ou catégories de destinataires des données, le droit d'information de la personne sur le traitement de données qui la concernent n'est pas pertinent pour fonder une quelconque obligation dans le chef du responsable du traitement de lui communiquer les *log files* de son dossier de patient informatisé, pour le simple motif que cette obligation d'informer doit être réalisée au plus tard au moment où les données sont obtenues lorsqu'elles sont collectées auprès de la personne, et dès l'enregistrement des données ou, si une communication à un tiers est envisagée, au plus tard au moment de la première communication des données, lorsque les données n'ont pas été collectées auprès de la personne[87].

Toutefois, ainsi que le suggère le Groupe 29 : «afin de susciter la confiance, une procédure spéciale visant à informer les personnes concernées de l'identité de ceux qui ont accédé à leur DME et de la date de cet accès pourrait être instaurée. La fourniture à intervalles réguliers d'une liste des personnes ou institutions qui ont eu accès à leur dossier rassurerait les patients quant à leur capacité de savoir ce qu'il advient de leurs données dans le système de DME»[88].

De même, il considère que «(…) La liste annuelle des accès susmentionnée envoyée aux personnes concernées constituerait un moyen efficace supplémentaire de vérifier la légalité de l'utilisation des données des DME. (…)»[89].

Cette mesure participerait aussi à consolider la légitimité de la finalité poursuivie par le traitement de données.

Conclusions

Au terme de ces développements, il est acquis que, de manière générale, des *log files* doivent enregistrer les informations portant sur les traitements des données de base, comme les informations sur les destinataires ou les catégories de destinataires auxquels les données de base sont communiquées, et sur le contenu des données de base, au titre du res-

[87] Article 9 de la loi du 8 décembre 1992. C'est ce qu'a rappelé la Cour de justice dans l'arrêt précité du 7 mai 2009 dans ses considérants n^{os} 68-69.

[88] Groupe de travail «Article 29» sur la protection des données, «Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)», adopté le 15 février 2007, WP 131, p. 24.

[89] Groupe de travail «Article 29» sur la protection des données, «Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)», adopté le 15 février 2007, WP 131, p. 24.

pect du droit d'accès de la personne concernée, la réponse étant plus nuancée au titre de mesure de sécurité du traitement de données.

Ceci étant, la mesure de sécurité prise en ce sens coïnciderait avec la mise en œuvre du droit d'accès du patient, tous deux renforçant la légitimité de la finalité poursuivie par le responsable du traitement de données concernant le patient.

Dans la double approche de la loi relative aux droits des patients et de la loi du 8 décembre 1992, les *log files* doivent permettre de savoir qui a fourni ou modifié quelle information (information sur le contenu des données de base ou information sur l'origine des données), qui a accédé à quoi et quand, ainsi que ce qu'il en a fait, même dans le cas d'une pratique libérale isolée.

Leur communication à intervalles réguliers à la personne concernée participerait aussi à la légitimité poursuivie par le responsable du traitement de données concernant le patient.

Enfin, le responsable du traitement doit veiller à auditer régulièrement les *log files* dans le cadre d'une politique globale de sécurité et ce, avec un système performant d'identification des utilisateurs et d'enregistrement de leurs actions.