Un nouveau métier de la santé

Herveg, Jean; Van Gyseghem, Jean-Marc

Published in:
Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde

Publication date:
2018

Document Version
le PDF de l'éditeur

TITRE 14
Un nouveau métier de la santé : la sous-traitance des données du patient*

Jean HERVEG et Jean-Marc VAN GYSEGHEM**

Introduction

1. Le sous-traitant est devenu un acteur important, si pas incontournable dans de nombreux cas, en matière de traitements de données à caractère personnel, surtout depuis le développement des services de *cloud computing*, du *big data* ou encore des applications de téléphonie mobile. Le sous-traitant offre l'expertise technique, les équipements et les ressources matérielles et personnelles, que le responsable de traitement ne peut pas ou ne veut pas prendre en charge pour réaliser ses projets informatiques.

Dans le domaine des soins de santé, la sous-traitance de données est omniprésente, que ce soit au sein des hôpitaux ou des cabinets de médecins généralistes, soit dans le cadre de la gestion des données des patients, soit dans le cadre de la communication de données relatives au patient entre professionnels de la santé au travers des réseaux télématiques régionaux et fédéral. Il est, de plus en plus, fait appel à des sous-traitants qui apportent leurs compétences particulières dans la gestion des données de leurs patients[1].

* This work has been done with the financial support from the European Union's Horizon 2020 research and innovation program under Grant Agreements n° 688520 (TeSLA) & 730953 (Inspex) and in part by the Swiss Secretariat for Education, Research and Innovation (SERI) under Grant 16.0136 730953. La publication ne reflète que l'opinion de ses auteurs et la Commission européenne ne peut être tenue responsable de l'usage qui en serait fait.

** Avocats au barreau de Bruxelles et directeurs de recherche au Centre de Recherche Information, Droit et Société (www.crids.eu) de l'Université de Namur.

[1] Ceci n'empêche pas qu'il faut vérifier si, dans certaines hypothèses, le recours à un sous-traitant ne serait pas incompatible. Il faut aussi vérifier s'il ne faut pas informer la personne concernée, ici, le patient, de l'intervention d'un sous-traitant. Voy. aussi l'article 28.4 du Règlement pour la question du recrutement d'un ou plusieurs sous-traitants par le premier sous-traitant.

2. Le Règlement général sur la protection des données ((UE) 2016/679 du 27 avril 2016, ci-après, « le Règlement ») a repris la substance des règles relatives à la sous-traitance des données qui étaient contenues dans 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 (ci-après, « la directive 95/46/CE »), tout en les précisant et en étoffant leur contenu dans une certaine mesure, le but étant de renforcer l'étanchéité du circuit des traitements de données (sa confidentialité) et, par-là, de garantir l'effectivité de la protection de la personne concernée[2].

La présente contribution analyse la sous-traitance dans le contexte particulier du domaine des soins de santé avec des réalités différentes dans la gestion des données des patients, que l'on travaille dans un hôpital ou en privé.

CHAPITRE 1. La notion de sous-traitant de données

3. Le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »[3]. Cette définition appelle les observations et explications suivantes.

Tout d'abord, le sous-traitant est une organisation *extérieure* à celle du responsable du traitement et qui possède une entité juridique distincte de la sienne[4].

Ceci étant, le fait d'être une organisation extérieure ne signifie pas qu'il suffise de loger ses activités de traitements de données dans une société dotée d'une personnalité juridique distincte pour qu'il y ait sous-traitance de données. Le sous-traitant ne peut pas, en outre, agir sous l'autorité directe du responsable du traitement (même s'il ne peut traiter les données que sur les instructions [documentées[5]] de ce dernier). Pour le dire autrement, il ne peut pas y avoir de relation hiérarchique entre le responsable du traitement et le sous-traitant de données (au sens opérationnel

[2] Voy. Groupe de l'Article 29, avis n° 1/2010 sur les notions de « responsable de traitement » et de « sous-traitant », adopté le 16 février 2010, *WP* 169, p. 26.

[3] Art. 4.8 du Règlement.

[4] Voy. Groupe de l'Article 29, avis n° 1/2010 sur les notions de « responsable de traitement » et de « sous-traitant », adopté le 16 février 2010, *WP* 169, p. 26.

[5] Conformément à l'article 28.3 du Règlement.

et organisationnel, et pas seulement entendu comme une absence de relation de subordination au sens du droit du travail).

Le sous-traitant ne peut donc pas être une personne qui fait partie de l'organisation du responsable du traitement. L'exemple type est celui du médecin hospitalier qui n'est pas lié par un contrat de travail : il répond bien à la condition de la personnalité juridique distincte, mais il ne répond pas à l'exigence de l'organisation extérieure à celle de l'hôpital. Ses activités sont, en effet, totalement intégrées dans celles de l'hôpital. Il n'agit, dès lors, pas en qualité de sous-traitant de données pour l'hôpital, mais bien en qualité de personne agissant sous l'autorité directe de l'hôpital (au sens opérationnel et organisationnel). De même, la secrétaire personnelle d'un médecin généraliste libéral agit sous l'autorité directe de ce dernier ; elle n'intervient donc pas en qualité de sous-traitant lorsqu'elle prend des rendez-vous dans l'agenda électronique ou qu'elle encode des protocoles ou rédige son courrier.

4. La qualification à donner à la société juridiquement distincte qui preste des services de traitements de données dans un contexte de mutualisation de services (entre hôpitaux ou médecins libéraux) s'analyse de la même façon. Si la première condition (personnalité juridique distincte) est souvent remplie, il convient encore de vérifier si ce prestataire de services mutualisés intervient bien en dehors de l'organisation des activités du responsable du traitement et sans être sous son autorité directe. Si la réponse est positive, nous serons en présence d'un sous-traitant. Sinon, d'une personne agissant sous l'autorité directe du responsable du traitement. Ainsi, le secrétariat extérieur auquel fait appel un médecin généraliste libéral pour la gestion de ses rendez-vous revêt la qualité de sous-traitant dans la mesure des traitements de données qu'il effectue pour le compte de ce médecin.

5. Une difficulté peut surgir lorsque le prestataire de services est une organisation extérieure dotée d'une personnalité juridique distincte, mais qui détache un travailleur au sein de l'organisation du responsable du traitement. Le tout sera de savoir si le travailleur extérieur est ou non soumis à l'autorité directe du responsable du traitement. Un cas fréquent est celui du travailleur d'une société de maintenance informatique qui, dans les faits, est installé à demeure, à durée déterminée ou non, dans les murs de l'hôpital, et qui traite des données pour compte de ce dernier. Par contre, la société extérieure qui réalise une migration de données au sein de l'hôpital sans être sous l'autorité directe du responsable du traitement, mais qui, pour ce faire, est bien obligée de dépêcher du personnel

sur place pendant plusieurs jours ou semaines, ne perd pas de ce fait sa qualité de sous-traitant de données.

Le tout est, bien sûr, de ne pas autoriser les montages de toutes sortes destinés à faire échapper l'un ou l'autre intervenant dans les traitements de données aux obligations qui lui incombent ou de jouer sur les qualifications pour en tirer profit. Ceci pose la question de la qualification à donner aux services mutualisés au sein d'un grand groupe – question qui, elle-même, renvoie à la question de l'identification des véritables responsables de traitements au sein de ce groupe.

6. La distinction entre les sous-traitants de données et ceux qui agissent sous l'autorité directe du responsable du traitement pose une question qui peut paraître malaisée à trancher : quelle est la différence entre l'obligation faite au sous-traitant d'agir uniquement et exclusivement sur instruction du responsable du traitement et le fait d'agir sous l'autorité directe du responsable du traitement ? Autrement dit, quelle est la différence entre recevoir une instruction et être sous l'autorité directe du responsable du traitement ?

Dans le premier cas, le sous-traitant reçoit une mission à accomplir au profit du responsable du traitement (et il peut la refuser), et il la réalise dans le cadre d'une organisation extérieure et juridiquement distincte de celle du responsable du traitement en choisissant les moyens techniques et d'organisation à mettre en œuvre à cet effet dès lors qu'il est justement fait appel à lui pour ses compétences particulières, comme ce sera souvent le cas pour les services de *cloud computing*[6]. Ceci étant, il ne faut pas perdre de vue qu'à partir du franchissement d'un certain seuil, le sous-traitant pourrait devenir un responsable de traitement conjoint en raison de sa participation au choix des finalités et des moyens du traitement des données par l'hôpital[7].

Dans le second cas, la personne réalise la prestation qui lui est demandée en utilisant les moyens mis à sa disposition par le responsable du traitement sans pouvoir refuser la mission, car elle se trouve dans le cadre d'une relation hiérarchique ou subordonnée. Dans cette situation, elle

[6] Voy., à ce propos, J.-M. Van Gyseghem, « *Cloud computing* et protection des données à caractère personnel : mise en ménage possible ? », *R.D.T.I.*, issue 42, pp. 35-50. Voy. également Groupe de l'Article 29, « Avis 05/2012 sur l'informatique en nuage », http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf.

[7] Voy. Groupe de travail « Article 29 » sur la protection des données, avis n° 1/2010 sur les notions de « responsable de traitement » et de « sous-traitant », adopté le 16 février 2010, *WP* 169, p. 27.

peut apporter son expertise dans le choix des finalités et des moyens sans courir le risque de devenir un responsable de traitement conjoint.

C'est en tout cela qu'il faut comprendre que le sous-traitant est une entité extérieure et juridiquement distincte de celle de l'hôpital en sa qualité de responsable du traitement. À défaut, il n'y a pas sous-traitance de données, mais une intervention sous l'autorité du responsable du traitement. Le tout revient maintenant à se demander s'il n'est pas artificiel de distinguer entre ces deux catégories qui, *in fine*, doivent répondre aux mêmes obligations…

7. En tout cas, il faut rappeler que le sous-traitant doit informer « immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du [règlement] ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données »[8].

Par ailleurs, le sous-traitant doit traiter des données pour compte du responsable du traitement. À cet effet, il doit, conformément à la définition même de la notion de *traitement*[9], réaliser des opérations ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et qui sont appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. Changer le câblage, les écrans ou les imprimantes d'un service hospitalier n'est pas constitutif d'un traitement de données, pas plus que l'installation d'un logiciel, pour autant que son installation ne requière pas de traitement de données. Par contre, la question est plus ardue en matière de *cloud computing*. Il faut raisonner à cet effet en partant de la classification pédagogique en trois services du *cloud computing*.

En principe, le recours à un service de *cloud computing* « *Infrastructure as a service* » ne consiste pas, dans le chef du responsable du traitement, à demander au fournisseur du service de traiter pour son compte des données ; il consiste « seulement » à lui louer du matériel informatique (du *hardware*) (comme de l'espace disque, mais sans système d'exploitation). Pour le dire autrement, le fournisseur de services « *Infrastructure as a service* » loue au responsable du traitement l'équipement dont ce dernier a besoin pour, le cas échéant, traiter des données. Le responsable du

[8] Art. 28, 3, h, du Règlement.
[9] Voy. art. 4.2° du Règlement.

traitement ne demande pas au fournisseur de service « *Infrastructure as a service* » de traiter les données à sa place (pour son compte) – même si le responsable du traitement peut utiliser cet équipement pour héberger des données à caractère personnel. D'ailleurs, le fournisseur de ce service va facturer la location du *hardware*, et non des opérations de traitement de données. Le plus souvent, c'est un administrateur réseau qui recourt à ce type de service. En règle, le contrat entre le responsable du traitement et le fournisseur de ce type de service doit inclure des clauses par lesquelles le fournisseur s'engage à ne pas tenter d'accéder aux données qui seraient stockées sur ses serveurs et de protéger ces dernières de tout accès non autorisé. Il arrive aussi que le responsable du traitement impose au fournisseur de lui garantir que personne d'autre n'utilise le même serveur pour éviter toute tentative d'accès non autorisé par un autre utilisateur du même serveur.

Par contre, il y a nécessairement sous-traitance de données lorsque le responsable du traitement recourt à un service de *cloud computing* de type « *Software as a service* » dont l'exemple le plus fréquent est celui où le responsable du traitement (ici, l'hôpital) demande au fournisseur d'héberger des données (comme des dossiers médicaux). L'hôpital demande au fournisseur de ce service d'héberger des données pour son compte. La facturation sera, d'ailleurs, différente de celle qui peut exister pour le service « *Infrastructure as a service* ».

Le troisième type de service de *cloud computing* est celui d'« *Infrastructure as a platform* » dans lequel le fournisseur loue du *hardware*, mais fournit aussi le système d'exploitation. Ce service est habituellement destiné aux développeurs de logiciels. Dans cette hypothèse, il faut analyser de manière encore plus approfondie au cas par cas dans quelle mesure le fournisseur de service intervient dans le traitement de données en tant que tel.

8. Enfin, si, à une certaine époque, on aurait pu être tenté de soutenir que les médecins n'étaient que les sous-traitants de leurs patients en termes de traitements de données, ce modèle n'a guère prospéré – aussi tentant fût-il au regard du droit fondamental à l'autodétermination informationnelle des individus. À l'heure actuelle, on considère habituellement que les hôpitaux ou les professionnels de la santé exerçant en privé sont les responsables des traitements de données liés à leurs activités professionnelles.

Une fois identifié, le sous-traitant doit se conformer à une série d'obligations dont l'intensité est liée aux caractéristiques du traitement de données en cause.

CHAPITRE 2. Le choix du sous-traitant

9. Alors que, sous la directive 95/46/CE, le responsable du traitement devait choisir un sous-traitant qui apportait « des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer » et qu'il devait veiller au respect de ces mesures par le sous-traitant, le Règlement exige maintenant que le responsable du traitement choisisse un sous-traitant qui présente « des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du [Règlement] et garantisse la protection des droits de la personne concernée »[10].

Il faut rappeler que l'idée de base est de garantir l'étanchéité du circuit du traitement des données (sa confidentialité) et, par-là, la protection de la personne concernée. Le sous-traitant ne peut donc pas être un panier percé (dans tous les sens du terme d'ailleurs). À cet effet, il doit prouver au responsable du traitement qu'il est en mesure de réaliser la mission que ce dernier entend lui confier, d'une manière qui soit totalement conforme au Règlement. Ceci peut se faire par la preuve de la conformité de ses activités à un code de conduite (le cas échéant approuvé) ou par la certification de ses activités[11]. Sous la législation précédente, les codes de conduite et les mécanismes de certification n'ont pas vraiment prospéré. Il reste à espérer que les temps changent et que ces nouveaux métiers de la société de l'information prennent enfin leur envol.

De manière générale, la sous-traitance de données doit être régie par un contrat ou tout acte juridique qui lie le responsable du traitement et le sous-traitant. Ce contrat ou cet acte doit, principalement, définir l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement[12].

Enfin, il ne serait pas vain d'exiger que les activités du sous-traitant soient couvertes par une assurance qui garantirait la couverture de tout dommage qui affecterait la personne concernée, sans que celle-ci ait à rapporter la preuve d'une faute dans le chef du responsable du traitement ou du sous-traitant. Ce serait une véritable garantie de sérieux, d'autant plus si les compagnies d'assurances s'assurent alors elles-mêmes des garanties offertes par le sous-traitant.

---

[10] Art. 28.1 du Règlement.
[11] Voy. art. 40 et s. du Règlement.
[12] Voy. art. 28.3 du Règlement pour le surplus.

CHAPITRE 3. Les obligations du sous-traitant

SECTION 1. – Les obligations en matière de sécurité

10. Le Règlement a renforcé les dispositions relatives à la sécurité des traitements en reprenant des dispositifs déjà présents dans d'autres législations européennes, comme la directive 2002/58/CE 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 »).

§ 1. Le principe

11. Le Règlement met à charge tant du responsable du traitement que du sous-traitant la mise en œuvre de « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque », « compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques »[13].

L'on voit donc, d'entrée de jeu, que le sous-traitant est un acteur (pro) actif dans la sécurité nécessaire à la confidentialité du traitement de données à caractère personnel. Afin de donner quelques pistes, le Règlement fixe ainsi une série de mesures à prendre, le cas échéant, à savoir :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- la mise en œuvre des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- la mise en œuvre des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- l'existence de procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles destinées à assurer la sécurité du traitement.

[13] Art. 32 du Règlement.

L'on constate que nombre de ces mesures sont, techniquement, à charge, partiellement ou totalement, du sous-traitant en fonction de ses compétences spécifiques et de son intervention réelle dans le traitement. Il doit ainsi garantir la sécurité, et corrélativement la confidentialité, du traitement – même s'il est vrai que le responsable de traitement est, en principe, le premier et seul interlocuteur de la personne concernée, ici, le patient.

12. Par ailleurs, « le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée [légalement] »[14]. Ces mesures doivent être tant techniques (*Access management*, etc.) qu'organisationnelles (formation, règlement d'ordre intérieur, etc.).

Du *point de vue organisationnel* au niveau du sous-traitant, ce dernier doit s'assurer que les personnes agissant sous son autorité soient informées des dispositions du Règlement[15]. Il doit également veiller à mettre en place une structure ou une organisation pour éviter la perte de données, des destructions ou modifications de données non autorisées, des accès non autorisés, etc. En d'autres termes, il doit prendre des dispositions en termes d'organisation qui garantiront la personne concernée contre de tels faits. Par exemple, le sous-traitant – au même titre que le responsable de traitement au demeurant – doit s'assurer que seules les personnes devant effectivement avoir accès à des données à caractère personnel y aient effectivement accès, à l'exclusion des autres. Il lui appartient donc de prévoir une organisation adéquate et efficace.

Ce niveau organisationnel se retrouve également au stade de la formation des personnes à n'accéder qu'aux données à caractère personnel dont elles ont réellement besoin. Par exemple, en matière de données relatives à la santé, le sous-traitant devra s'assurer que son personnel n'accède aux données relatives à des patients que si, et seulement si, sa mission le requiert. Si tel n'est pas le cas, il devra s'en abstenir au risque de se trouver confronté à de très lourdes sanctions…

Au niveau technique, le sous-traitant doit s'assurer qu'il a mis en place des mesures adéquates de protection de ses traitements du point de vue technique. Ainsi, il doit s'assurer que son système informatique réunit les conditions nécessaires pour éviter toute intrusion non autorisée via

[14] Art. 32.4 du Règlement.

[15] Cela découle, entre autres, de l'économie du Règlement.

une bonne gestion d'accès, toute perte, destruction ou modification de données, etc. À noter que la notion de sécurité s'entend aussi des accès physiques au réseau informatique du responsable de traitement. Il faudra donc être attentif à ce que l'accès au serveur, par exemple, soit réglementé et ouvert aux seules personnes pour qui cela représente une nécessité. Il serait bien inutile de prévoir des règles d'accès strictes aux données si le serveur les contenant n'était pas suffisamment protégé et si, en conséquence, son contenu venait à être subtilisé…

L'ensemble de ces éléments doit se retrouver dans le contrat de sous-traitance qui sera signé entre le responsable de traitement et son sous-traitant.

§ 2. L'obligation de notifier ou de communiquer les failles de sécurité

13. Si, d'aventure, une faille de sécurité devait intervenir, le responsable du traitement doit procéder à une notification à l'autorité de contrôle nationale dans tous les cas et à la personne concernée dans certaines situations.

L'on doit relever que, si le sous-traitant a connaissance d'une faille de sécurité, il doit le notifier au responsable du traitement dans les meilleurs délais après cette prise de connaissance[16]. En outre et afin de permettre au responsable du traitement de remplir son obligation de notification/communication, le sous-traitant a une obligation de documenter complètement l'incident. En conséquence, le contenu de cette notification/communication sera nourri ou documenté par le sous-traitant. Cette documentation produite par le sous-traitant doit être de nature à permettre au responsable du traitement d'évaluer s'il se trouve dans les exceptions de communication à la personne concernée prévues par le Règlement.

SECTION 2. – L'obligation de recourir aux services d'un Délégué à la protection des données

14. Le Règlement a repris et renforcé le rôle et la fonction du détaché à la protection des données, devenu le délégué à la protection des données (en abrégé, « DPO » pour *Data protection officer*)[17].

[16] Art. 33.2 du Règlement.
[17] Art. 37 et s. du Règlement.

Il s'agit d'une fonction importante au sein de l'organisation du responsable du traitement, mais également du sous-traitant dès lors qu'il doit vérifier, entre autres, le respect du Règlement par ce dernier.

Tout responsable du traitement et tout sous-traitant doivent nommer un DPO dans les hypothèses suivantes :

- le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
- les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou
- les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données sensibles et de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Ces critères sont assez flous hormis celui qui se réfère aux catégories particulières de données comme les données relatives à la santé. Le Groupe 29 en a précisé les contours[18]. Ainsi, à titre d'exemple :

- le Groupe 29 considère comme « *activité de base* » le traitement de données relatives à la santé par un hôpital. Cette analyse doit, à notre sens, être reprise pour tout sous-traitant dont l'activité de base est d'assister le responsable du traitement dans ce type de traitement ;
- il en va de même pour le concept de « *grande échelle* » dès lors que le Groupe 29 prend, comme exemple, l'hôpital qui traite des données relatives aux patients dans le cours régulier de ses activités. Cela est transposable pour un sous-traitant dans un tel traitement. Par contre, le médecin lui-même est exclu.

Le DPO peut être soit interne à la structure du responsable du traitement ou du sous-traitant, soit externe. Le DPO peut également travailler pour plusieurs responsables du traitement ou sous-traitants, mais doit, à notre sens, être transparent à ce sujet.

15. Appliqué au niveau de la sous-traitance dans le domaine médical, l'on pourrait avoir un responsable du traitement qui ne soit pas soumis à l'obligation de désignation d'un DPO (comme les médecins généralistes), mais que le sous-traitant le soit au regard des critères mis en place par le

[18] Groupe de l'Article 29, *Guidelines on Data Protection Officers (« DPOs »)*, *WP* 243rev.01, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Groupe 29. Cela sera le cas, par exemple, pour un fournisseur de service de *cloud computing* qui traiterait, comme sous-traitant, des données relatives à la santé à grande échelle pour plusieurs médecins, ce qui est de plus en plus fréquent dans les programmes de gestion de patientèle qui utilisent le cloud. Il en est de même pour les réseaux santé qui, en réalité, sont les sous-traitants des hôpitaux ou autres professionnels de santé ; ils doivent nommer un DPO compte tenu du fait qu'il y a un traitement à grande échelle de catégories particulières de données.

16. Le DPO remplit une réelle fonction au sein de l'organisation du responsable du traitement dès lors que[19] :

- il doit être associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ;
- il doit recevoir les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et les moyens d'entretenir ses connaissances spécialisées ;
- il ne reçoit aucune instruction en ce qui concerne l'exercice des missions. Le DPO doit, en effet, remplir sa fonction en toute indépendance, ce qui explique qu'il « ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions »[20] ;
- il doit être un point de contact pour l'autorité de contrôle et la personne concernée.

17. Par ailleurs, le DPO doit avoir les qualités professionnelles et, en particulier, des connaissances spécialisées du droit et des pratiques en matière de protection des données nécessaires pour exercer sa fonction et remplir les missions qui sont les siennes.

Concernant les qualités professionnelles, doit-on en exiger de particulières dans le cadre de traitement de données relatives à la santé ou peut-on se satisfaire des critères habituels ? Il nous semble que la catégorie à laquelle appartiennent les hôpitaux exige que le DPO ait une connaissance minimale de la législation relative à cette matière outre le Règlement afin de pouvoir remplir adéquatement sa mission. Pour le dire autrement, il doit connaître les droits du patient, l'organisation des circuits d'information au sein des hôpitaux, les règles relatives aux dossiers de patients, sans parler des règles relatives à la communication de données à des fins de santé publique et de financement des soins de santé.

[19] Art. 38 du Règlement.
[20] Art. 38.3 du Règlement.

SECTION 3. – L'obligation de tenir un registre des activités de traitement

18. Le Règlement a supprimé l'obligation, dans le chef du responsable du traitement, de notifier à l'autorité de contrôle toute une série d'informations à propos des traitements de données qu'il entendait réaliser. Cependant, en contrepartie de cette suppression, le responsable du traitement doit tenir un registre des activités de traitement effectuées sous sa responsabilité reprenant un certain nombre d'informations précisées à l'article 30 du Règlement.

Cette obligation n'est pas applicable à une entreprise ou organisation comptant moins de deux cent cinquante employés sauf si le traitement effectué « est susceptible de comporter un risque pour les droits et [l]es libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 »[21].

19. Une telle obligation, et cela est également nouveau, est aussi mise à charge du sous-traitant qui doit tenir « un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :

a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et ce[ux] du délégué à la protection des données ;

b) les catégories de traitements effectués pour le compte de chaque responsable du traitement ;

c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1 »[22].

[21] Art. 30.5 du Règlement.
[22] Art. 30.2 du Règlement.

L'exception à cette obligation telle qu'elle existe pour le responsable du traitement est également applicable pour le sous-traitant.

20. On doit cependant bien constater que le sous-traitant de traitement de données relatives à la santé ne pourra jamais bénéficier de l'exception dès lors qu'il ne s'agit pas d'un traitement « occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1 »[23].

CHAPITRE 4. Le sous-traitant et la notion de responsable conjoint du traitement de données

21. Le Règlement prévoit, en son article 26, que :

« **1.** Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

3. Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement ».

La coresponsabilité du traitement, qui existait déjà sous la directive 95/46/CE, s'applique quand plusieurs responsables de traitement

[23] *Ibid.*

déterminent ensemble les finalités (le « pourquoi ») et les moyens (le « comment ») de certaines activités de traitement[24]. L'on doit également noter que, « pour qu'une personne puisse être considérée comme un responsable du traitement, au sens de l'article 2, sous d), de la directive 95/46, il n'est pas nécessaire que cette personne dispose d'un pouvoir de contrôle complet sur tous les aspects du traitement. Comme le gouvernement belge l'a indiqué à juste titre lors de l'audience, un tel contrôle existe de moins en moins en pratique. De plus en plus, les traitements ont une nature complexe, en ce sens qu'il s'agit de plusieurs traitements distincts impliquant plusieurs parties exerçant elles-mêmes différents degrés de contrôle. Par conséquent, l'interprétation privilégiant l'existence d'un pouvoir de contrôle complet sur tous les aspects du traitement est susceptible d'entraîner de sérieuses lacunes en matière de protection des données à caractère personnel »[25] et que « l'interprétation large de la notion de "responsable du traitement", au sens de l'article 2, sous d), de la directive 95/46, qui doit, selon nous, prévaloir dans le cadre de la présente affaire, est de nature à éviter les abus. En effet, il suffirait sinon pour une entreprise de recourir aux services d'un tiers pour se soustraire à ses obligations en matière de protection des données à caractère personnel »[26].

22. En matière de santé, on peut se poser la question si un sous-traitant ne doit pas, en réalité, le plus souvent, être considéré comme un responsable conjoint du traitement tant il est impliqué dans les moyens mis en œuvre pour atteindre la finalité du traitement. Prenons l'exemple du service de second avis qui est souvent presté en dehors de l'Union européenne (Inde, Chine), mais offert par des sociétés européennes aux médecins. Pour ce faire, les médecins qui requièrent ce second avis doivent passer par un traducteur chargé de traduire les dossiers médicaux afin de permettre au médecin se trouvant dans un pays tiers de pouvoir rendre un second avis sur la base de documents qu'il comprend.

---

[24] Sur la détermination des finalités et des moyens, voy. not. Groupe de l'Article 29, avis n° 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », *WP* 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 14.

[25] C.J.U.E., *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, concl. av. gén. 24 octobre 2017, pt 62, http://curia.europa.eu/juris/document/document.jsf?text=&docid=195902&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=254071 ; si l'argumentation porte sur la directive 95/46, cela peut être transposé pour le Règlement.

[26] *Idem*, pt 64 ; si l'argumentation porte sur la directive 95/46, cela peut être transposé pour le Règlement.

S'il ne fait aucun doute que le médecin est responsable du traitement comme analysé ci-dessus, qu'en est-il exactement de la société chargée de la traduction qui, elle-même, fait appel à des traducteurs indépendants ?

Cette société offre un service qui ne met pas l'accent sur le traitement de données, mais sur la traduction de dossiers médicaux ou partie de ceux-ci, sur base contractuelle. Le traitement de données est en lien avec la finalité du contrat, mais n'est pas son objectif. Par ailleurs, la société travaille sur la base d'instructions peu spécifiques ne correspondant pas nécessairement au concept de sous-traitant. Par conséquent, et si nous considérons que cette société de traduction ne remplit pas les critères fixés par le Règlement, elle ne pourra pas être considérée comme un sous-traitant du responsable du traitement.

Pourrait-elle être responsable de traitement alors que le médecin l'est déjà, ainsi que nous l'avons analysé ci-dessus ? Dans la relation entre parties, la société offre un service de traduction et traite nécessairement des données à caractère personnel, même si elle ne met pas l'accent sur un tel traitement pour exécuter le contrat. Au regard de ce service, nous pourrions considérer que la société détermine tant la finalité (traduction) que les moyens (appel à des traducteurs indépendants). Si tel est le cas, nous avons donc affaire à un nouveau responsable du traitement, mais qui n'a cependant aucun contact avec les patients qui sont pourtant les personnes concernées. Elle ne pourra donc pas exécuter les obligations en matière d'information ou d'accès au profit de la personne concernée alors que ces obligations sont pourtant à sa charge en sa qualité de responsable de traitement.

Ainsi que le rappelle l'avocat général près la Cour de justice de l'Union européenne, il y a lieu de « préciser que l'existence d'une responsabilité conjointe ne signifie pas une responsabilité sur un pied d'égalité. Au contraire, les différents responsables du traitement peuvent être impliqués dans un traitement de données à caractère personnel à différents stades et à différents degrés »[27]. Par ailleurs, le Groupe de l'article 29 a également précisé que « la participation des parties à la détermination des finalités et des moyens de traitement dans le cadre d'une coresponsabilité peut revêtir différentes formes et n'est pas nécessairement partagée de façon égale. […] De plus, il est tout à fait possible que, dans des systèmes complexes qui font intervenir de multiples acteurs, l'accès aux données à caractère

[27] C.J.U.E., *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, concl. av. gén. 24 octobre 2017, pt 75, http://curia.europa.eu/juris/document/document.jsf?text=&docid=195902&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=254071.

personnel et l'exercice des autres droits des personnes concernées puissent aussi être garantis à différents niveaux par différents acteurs »[28].

Il nous semble que la situation du médecin et du service de traduction pourrait s'inscrire dans cette définition donnée tant par l'avocat général que par le Groupe de l'Article 29. Nous aurions dès lors une responsabilité conjointe agissant à divers niveaux, mais assurant une protection adéquate des données à caractère personnel des patients qui sont, au surplus, des catégories particulières de données au sens de l'article 9 du Règlement.

Cette situation montre la difficulté de pouvoir déterminer de manière univoque si un acteur est sous-traitant ou responsable du traitement.

Conclusions

23. La sous-traitance des données relatives aux patients est un phénomène incontestable qui prend de plus en plus d'ampleur. Elle présente souvent la difficulté d'être internationale, sinon à tout le moins intra-européenne.

Si le Règlement fournit un cadre juridique plus étoffé pour la réalisation des missions qui peuvent être confiées au sous-traitant, sous réserve néanmoins du fait que les États membres peuvent prendre des mesures au niveau national en ce qui concerne les données relatives à la santé, il n'en demeure pas moins que nous sommes en présence d'un tronc commun qui ne tient pas compte du contexte spécifique des soins de santé.

À nos yeux, il manque des règles relatives aux qualifications professionnelles à remplir pour traiter des données relatives à la santé. Il est difficile, sinon périlleux, de vouloir répondre à cette question par les règles actuelles relatives à l'exercice des professions des soins de santé. Pour le dire autrement, celles-ci peuvent intervenir dans une certaine mesure pour les actes qui relèvent indubitablement de leur exercice, comme l'établissement d'un protocole en imagerie médicale. Mais cela ne couvre absolument pas les nouveaux métiers qui sont apparus depuis plusieurs années dans le secteur de la santé et qui sont en lien avec les technologies de l'information et de la communication. Il existe bien de-ci de-là quelques formations éparses qui tentent de répondre à ce nouvel environnement, mais il faut bien constater que le cadre législatif et réglementaire est très

[28] Groupe de l'Article 29, avis n° 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », *WP* 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 35.

en retard, ce qui est de nature à retarder le développement de technologies utiles, ce qui est préjudiciable tant pour les patients que pour l'économie de la santé.

Il est donc grand temps que les pouvoirs publics se saisissent de la question du cadre juridique des nouveaux métiers de la santé qui doit venir compléter la protection des données du patient au-delà de la réglementation des infrastructures télématiques dans le domaine de la santé.

Pour le dire autrement, après avoir réglementé les traitements de données et les infrastructures télématiques, il est maintenant urgent de réglementer les nouveaux métiers et les nouvelles fonctions dans le domaine de la santé.

Il va sans dire qu'il manque toujours une sensibilisation suffisante des acteurs de terrain et des formations appropriées pour garantir effectivement la protection des données sur le terrain, en ce compris dans le chef des patients.