DOI: 10.1051/odf/2018010
Éditorial

Rev Orthop Dento Faciale 2018;52:131-132

Éditorial

Protection des données, la nouvelle donne !

« Entre le fort et le faible, entre le riche et le pauvre, entre le maître et le serviteur, c'est la liberté qui opprime, et la loi qui affranchit. »

Jean-Baptiste-Henri Dominique Lacordaire (1802-1861).

À l'aube de l'ère du tout numérique, des logiciels intelligents, des numérisations, des échanges et stockages dématérialisés, de l'essor de la télémédecine ou autres big data, les données de santé se doivent de parfaire leur protection qui doit s'adapter aux nouvelles réalités du numérique.

C'est justement la finalité du *General Data Protection and Régulation* (GDPR), issu du règlement européen n° 2016/679 d'avril 2016, devant assurer à compter de mai prochain l'amélioration de la protection et de la confidentialité des informations personnelles identifiables pour chaque citoyen européen.

Fondée sur la notion même de protection de l'individu et la nécessité de protéger les données personnelles de chaque citoyen de l'Union européenne, cette nouvelle réglementation se veut universaliste et s'applique ainsi à toutes les entreprises ou organisations, non seulement européennes mais aussi hors Union européenne, dès lors qu'elles sont amenées à collecter, traiter ou stocker des données à caractère personnel (DCP) issues de citoyens de l'Union européenne.

La notion de donnée à caractère personnel (DPC) s'entend largement puisqu'elle couvre des notions évidentes comme le nom, l'adresse, le numéro de téléphone, les données médicales mais aussi l'adresse IP, des informations sur les centres d'intérêt, les cookies… Trop souvent, la majorité des patients comme des internautes n'ont pas connaissance des données récoltées ni ce pourquoi elles l'ont été. C'est pourquoi cette protection se veut opposable aussi bien au cabinet d'orthodontie libéral qu'aux géants du FAMGA (Facebook, Apple, Microsoft, Google, Amazon) dès lors qu'elle vise la protection des données individuelles de chaque individu.

Adresse de correspondance :
laurent.delprat@wanadoo.fr

Comme en matière de droit médical, cette protection du consommateur au sens du profane crédule et vulnérable est fondée essentiellement sur les deux piliers de l'information et du consentement. Les entreprises comme les structures de soins devront désormais fournir des informations précises sur leur pratique de collecte et de conservation des données personnelles. Les usagers disposeront de davantage d'informations sur les modalités non seulement de traitement des informations les concernant, mais aussi de leur protection (gestion des accès, stockage, sécurité), informations qui se voudront claires, transparentes et adaptées à leur niveau de compréhension, à l'instar de l'information médicale du patient.

Cette information, dans le prolongement des règles déjà imposées par la CNIL, renforce notamment les :

- Droit à la portabilité : qui permet à une personne de récupérer les données qu'elle a fournies sous une forme réutilisable et le cas échéant de les transférer d'un prestataire à un autre sur simple demande.
- Droit à l'oubli : qui autorise toute personne à réclamer la suppression des données la concernant.
- Droit à l'information : qui permet au citoyen d'être informé sous 72 heures du piratage de ses données.
- Protection des mineurs de moins de 16 ans : pour lesquels la collecte de données personnelles nécessitera un accord parental systématique.

Cette obligation d'information se double de la recherche d'un consentement, éclairé et positif, du citoyen, et surtout explicite, c'est-à-dire ni équivoque ni tacite avant toute utilisation de ces informations.

La sécurisation de ces données sera par ailleurs assurée par la mise en œuvre d'un certain nombre de contraintes aux structures :

- Une obligation d'assurer la protection des données : respect de la protection des données dès la conception (article 25 § 1 du règlement), obligation de sécurité par défaut (article 25 § 2), obligation de documentation (article 24), pseudonymisation « privacy by design » (article 4)…
- Obligation de nommer un délégué à la protection des données ou « Data Protection Officier » (article 37), garant des moyens mis en œuvre par la structure.
- Obligation de déclarer à la CNIL dans le délai de 2 heures tout incident susceptible d'avoir compromis l'intégrité des données informatisées, sous peine de sanctions financières.

À la fin du second millénaire, le droit a souhaité assurer la protection du patient, à l'aube du troisième millénaire, il s'évertue à protéger l'internaute. Le droit assure ainsi ses fonctions premières, la normalisation d'un risque social et la sécurisation du faible.

Maître Laurent Delprat
Avocat à la Cour, Docteur en Droit privé et sciences criminelles,
Maître de Conférences associé à la faculté de droit de Paris VIII,
Chargé de cours à la faculté d'odontologie de Paris VII Garancière

Les opinions émises n'engagent que leurs auteurs.