resse l'avait informé en temps utile, d'une part, qu'il n'en avait en réalité jamais été détenteur, et, d'autre part, que cette carte n'avait pas fait l'objet d'une utilisation frauduleuse.

En considérant que cette dernière précision permettait au demandeur de déduire qu'aucune opération réalisée au moyen de cette carte de crédit n'avait été enregistrée sur son compte, les juges d'appel n'ont pas restreint la portée de la disposition légale visée au moyen.

Le moyen ne peut être accueilli.

Par ces motifs :

La Cour

Rejette le pourvoi ;

[...]

Observations

La difficile application de la législation de protection des données à caractère personnel

Introduction

L'arrêt de la Cour de cassation du 22 février 2017 illustre la difficulté qui demeure encore aujourd'hui à appliquer dans toutes ses dimensions le « droit des nouvelles technologies ».

La Cour de cassation, et avant elle, la cour d'appel de Liège[1], écarte l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement des données à caractère personnel[2] à la suite d'une lecture erronée du champ d'application de cette loi. Appelée en outre à aborder la question de la qualité des données ainsi que celle du droit d'accès aux données reconnu par la loi, la Cour apporte un éclairage qui n'est assurément pas celui que l'on attendait et qui déconcerte plutôt le praticien.

À l'origine de cette affaire, le demandeur en cassation s'est vu reprocher un découvert bancaire qu'il a immédiatement contesté, ce découvert étant rattaché à une carte de crédit qu'il n'avait pas utilisée. La banque a reconnu son erreur et a pris à sa charge le solde négatif du compte litigieux. Toutefois, la procédure d'enregistrement du retard de paiement auprès de la Banque nationale a été automatiquement mise en œuvre par la banque, ce qui a entraîné le fichage du client dans la base de données centralisée des débiteurs défaillants (le fichier des enregistrements non régis). Cette situation dommageable pour le client qui voyait de la sorte sa capacité d'emprunt altérée, a amené celui-ci à attaquer sa banque en justice en s'appuyant sur la législation de protection des données. L'affaire suscitait en effet des questions quant à la communication à des tiers de données à caractère personnel inexactes et quant au droit d'accès d'un individu aux données qui le concernent faisant l'objet d'un traitement. Sur ce dernier aspect, en effet, le client estimait que son droit d'accès instauré par la loi Vie privée n'avait pas été respecté par la banque.

Les paragraphes qui suivent viennent reclarifier les contours de cette législation et la portée du droit d'accès qu'elle consacre. Cette démarche de clarification s'impose d'autant plus que le champ d'application matériel de la loi de 1992 et les notions de traitement des données à caractère personnel et de fichier qui sont au cœur de l'arrêt de la Cour se retrouvent dans le règlement général sur la protection des données (R.G.P.D.), règlement européen appelé à régir la matière pour l'ensemble de l'Union européenne à partir du 25 mai 2018[3]. Il est dès lors particulièrement important que les acteurs belges voient clair dans les conditions d'application de cette législation.

Champ d'application matériel de la législation de protection des données et notion de fichier

Le point le plus problématique de l'arrêt réside dans la définition erronée que la Cour donne du champ d'application matériel de la loi Vie privée.

Cette loi vise à protéger les individus à l'égard du traitement de leurs données à caractère personnel[4], c'est-à-dire de toute information qui se rapporte à eux[5] et non pas des seules informations intimes ou confidentielles comme l'évocation de la « vie privée » dans l'intitulé de la loi pourrait le laisser penser. L'intention du législateur est de garantir l'autodétermination informationnelle des personnes physiques, soit leur droit de déterminer quelles informations les concernant peuvent être traitées, par qui et à quelles fins[6]. Il s'agit de permettre à tout un chacun de décider de l'utilisation de ses données, ou à tout le moins d'être au courant de leur sort, d'être informé de qui sait quoi sur lui et pour en faire quoi. Les données liées à l'usage par une personne de sa carte de crédit et celles se rapportant aux divers contrats qui lient cette personne à sa banque sont assurément des données à caractère personnel entrant dans le champ de la loi.

Aux termes de son article 3, § 1er, la loi Vie privée s'applique « à tout traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ».

Dans l'affaire objet du présent commentaire, tant la cour d'appel que la Cour de cassation ne retiennent étrangement que la fin de cette disposition et se focalisent sur la notion de fichier. La Cour de cassation précise même : « En l'absence de fichier tel que défini à l'article 1er de la loi du 8 décembre 1992, celle-ci ne trouve pas à s'appliquer ».

Or, il s'agit là d'une conclusion totalement erronée tirée d'une lecture partielle de l'article 3, § 1er.

Pour que la législation de protection des données s'applique, il faut se trouver en présence d'un traitement de données à caractère personnel. Le traitement s'entend de n'importe quelle utilisation qui est faite des données, depuis leur collecte ou enregistrement jusqu'à leur destruction[7]. Ce traitement peut être totalement ou partiellement automatisé. En d'autres termes, la loi s'applique dès lors que recours est fait, à un moment ou à un autre, à des moyens automatisés. Les moyens automatisés englobent toutes les technologies de l'information et de la communication (TIC) : informatique, télématique, réseaux de télécommunication[8]. En clair, la loi s'applique dès que toutes les opérations effectuées avec les données sont sur support numérique mais il suffit aussi qu'une opération soit appliquée aux données en faisant intervenir, ne fût-ce qu'en partie, des moyens automatisés. Il suffit, par exemple, que les données soient au départ conservées sur un support informatisé et ensuite imprimées, ou qu'elles soient contenues dans un document papier (un formulaire, par exemple, ou un contrat) qui a été scanné par la suite.

Et, s'il n'est fait aucun recours à des moyens automatisés, la loi s'appliquera quand même mais à la condition qu'on se trouve en présence d'un fichier. Le fichier s'entend d'un « ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle

(1) Liège (6e ch.), 13 octobre 2016, 2015/IC/9, inédit.
(2) Ci-après « loi Vie privée ».
(3) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
(4) Article 2 de la loi Vie privée.
(5) Article 1er, § 1er, de la loi Vie privée.
(6) C. de Terwangne, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? - Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », *Les enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 251, disponible à l'adresse http://www.crid.be/pdf/public/7638.pdf ; E. Degrave, *L'e-gouvernement et la protection de la vie privée - Égalité, transparence et contrôle*, coll. du CRIDS no 36, Bruxelles, Larcier, 2014, no 64 ; A. Rouvroy et Y. Poullet, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie », *in* K. Benyekhlef et P. Trudel (éd.), *État de droit et virtualité*, Montréal, Thémis, 2009, pp. 157-222, disponible à l'adresse http://www.crid.be/pdf/public/6050.pdf ; Liège, 6e ch., 13 octobre 2016, 2015/IC/9, inédit.
(7) Article 1er, § 2, de la loi Vie privée : « Par "traitement", on entend toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel ».
(8) C. de Terwangne, « L'utilisation des nouvelles technologies par le secteur financier face au droit à la vie privée et à la protection des données », *in The increasing impact of human rights law on the financial world*, coll. Cahiers de AEDBF/EVB-FR-Belgium, Limal, Anthemis, 2016, p. 89.

ou géographique »[9]. En clair, pour que la loi s'applique également à un traitement effectué par des moyens non automatisés, « il faut des données ordonnées et que celles-ci soient accessibles en fonction de critères déterminés. À cet égard, l'ordre et la méthode conduisent inévitablement à l'application de la loi »[10]. C'est donc par la structuration des données personnelles qu'il contient, permettant l'accessibilité de ces données, que le fichier se caractérise[11]. Un classement sur la base des noms des personnes, par ordre alphabétique, constitue un fichier au sens de la loi vie privée. Il en est de même des classements selon un critère géographique, chronologique ou sur la base de résultats, etc. En effet, c'est la facilité d'accès aux données qui est un des principaux facteurs de risques pour les droits et libertés des individus. Cette facilité est certes caractéristique des moyens automatisés, mais on la retrouve aussi, même si à un moindre degré, en présence de données rassemblées et conservées selon des critères de classement permettant précisément un accès direct aux données.

Cela signifie que la notion de fichier ne doit intervenir que si l'on se trouve dans une situation où aucun moyen automatisé n'apparaît. Autant dire que dans le contexte actuel, cette hypothèse se réduit à peau de chagrin. Et le monde bancaire n'échappe pas à cette réalité. On n'imaginerait plus une banque conservant les informations de ses clients ou les contrats passés avec eux en format papier exclusivement.

Il convient donc de faire remarquer que, dès qu'interviennent des moyens automatisés, il ne faut pas obligatoirement que les données soient structurées d'une manière ou d'une autre pour que la loi s'applique[12]. En effet, l'efficacité de tels moyens permet d'accéder à une ou plusieurs données enregistrées dans un ensemble (qui peut être une impressionnante base de données), de les sélectionner, les extraire, les associer, les modifier, etc. sans qu'il soit nécessaire que les données aient fait l'objet d'une structuration préalable pour arriver à ces résultats. À titre d'illustration, des données à caractère personnel publiées de manière éparse (sur plusieurs pages différentes) et sans aucun ordre logique (pas par ordre alphabétique ou chronologique par exemple) sur un site Internet sont bel et bien couvertes par la législation de protection des données[13].

Dans son arrêt attaqué devant la Cour de cassation dans l'affaire objet du présent commentaire, la cour d'appel de Liège a démontré une très mauvaise compréhension du champ d'application de la loi Vie privée et de ses termes clés que sont le traitement de données et le fichier quand elle déclare « même si les contrats liant la banque à ses clients font l'objet de dossiers logiquement structurés [...], cette caractéristique ne confère pas à ces contrats la qualité d'un *fichier qui fera l'objet d'un traitement sur la base de données à caractère personnel* »[14]. Or, comme on l'a dit, ce sont les *données* et non les *fichiers* qui font l'objet d'un *traitement* automatisé ou non ; et si ce traitement n'est pas du tout automatisé, la loi s'applique à la condition que les données figurent dans un *fichier*. Cette cour et la Cour de cassation à sa suite auraient pu faire l'économie de leurs réflexions sur la présence ou non d'un fichier dans l'affaire qui leur était soumise. L'évident recours à des moyens numériques dans le monde bancaire suffisait à rendre la loi Vie privée applicable.

Exigence de traitement loyal et de qualité des données

La législation de protection des données exige du responsable du traitement des données qu'il traite loyalement les données[15] et qu'il veille à la qualité de ces dernières. Elles doivent être exactes et si nécessaires mises à jour[16]. Cette double obligation est sanctionnée pénalement, l'article 39, 1°, de la loi Vie privée punissant d'une amende celui qui traite des données à caractère personnel en infraction avec ces exigences.

Dans l'affaire qui retient notre attention, il est clair que la banque a communiqué des données erronées à la BNB puisqu'elle reconnaît elle-même son erreur. Le client y voit une violation de la double obligation de loyauté du traitement et de qualité des données. Or, la cour d'appel a estimé qu'il ne lui revenait pas d'apprécier la gestion quotidienne de la banque, ce qui sortirait du cadre de l'infraction visée. La Cour de cassation, quant à elle, a admis cette motivation comme régulière. Cette assertion de la cour de Liège étonne pourtant car il s'agit ici de vérifier simplement si la communication des données portait sur des données exactes ou non. La loi Vie privée stipule que toutes les mesures raisonnables doivent être prises pour que les données inexactes soient rectifiées. On ne voit pas en quoi la vérification de cette exigence amènerait la juridiction à porter un jugement sur la gestion quotidienne de la banque. Dans une autre affaire similaire, le tribunal civil de Bruxelles ne s'était pas embarrassé de ce genre de considération lorsqu'il a établi dans sa décision du 15 octobre 2003 que, en matière de crédit, le prêteur qui fournit des informations à la Banque nationale est responsable d'un traitement de données et que, dès lors, « il lui incombe de s'assurer que sont remplies toutes les conditions auxquelles la transmission du nom des débiteurs défaillants à [...] la Banque nationale est subordonnée »[17]. En conséquence de quoi, le tribunal sanctionna le prêteur en question. Si les juridictions s'interdisaient de vérifier l'exactitude de données litigieuses ou la prise de mesures raisonnables pour garantir cette exactitude, cela risquerait de retirer tout intérêt à l'exigence de qualité des données.

Droit d'accès aux données

Dans un but de transparence permettant de contrôler ce qui est fait avec les données à caractère personnel et d'en vérifier la qualité[18], tout individu se voit reconnaître un droit d'accès aux données qui le concernent[19].

La Cour de cassation avait déjà eu à se prononcer sur la portée du droit d'accès instauré par la loi Vie privée, dans une affaire portant sur une demande d'accès aux données détenues par la Communauté française pour établir la redevance « télé »[20]. Elle avait alors formulé de façon très nette la seule manière admissible d'honorer ce droit d'accès. Selon ses termes, « seule la transmission des informations portant, notamment, sur les catégories de données sur lesquelles porte le traitement et sur les données personnelles faisant l'objet du traitement, adressée par le responsable du traitement à la personne physique qui le demande, répond au devoir d'information mis à charge du responsable du traitement vis-à-vis de la personne concernée »[21]. Les informations sur les données doivent être transmises spécifiquement à la personne concernée qui les demande. La Cour rejeta le raisonnement de la cour d'appel qui avait considéré que la personne concernée disposait déjà des informations sollicitées par le

(9) Article 1er, § 3, de la loi Vie privée
(10) C. de Terwangne, J. Herveg et J.-M. Van Gyseghem, *Le divorce et les technologies de l'information et de la communication : introduction à la protection des données dans la preuve des causes de divorce*, Malines, Kluwer, 2005.
(11) Pour des cas d'application, voy. Cass., 16 mai 1997, *J.T.*, 1997, p. 779 ; Bruxelles, 26 juin 2007, *R.W.*, 2008-2009, liv. 14, p. 578 ; Liège, 6 février 2006, *J.L.M.B.*, 2006, liv. 15, p. 665.
(12) D'autres décisions de jurisprudence témoignent de la même mauvaise compréhension du champ d'application de la loi Vie privée que la Cour de cassation dans l'affaire commentée, en exigeant d'être en présence d'un fichier plutôt qu'en vérifiant simplement s'il y a recours à des moyens numériques pour traiter les données. Voy. ainsi Mons, 14 mars 2013, R.G. 148/13, disponible sur http://jure.juridat.just.fgov.be, cité par C. Burnet et M. Piron, « Vie privée et protection des données à caractère personnel - Juridictions judiciaires », *Chronique de jurisprudence en droit des technologies de l'information (2012-2014)*, *R.D.T.I.*, 2015, nos 59-60, p. 74.
(13) C. de Terwangne et J.-M. Van Gyseghem, « Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution », *in* C. de Terwangne (éd.), *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, chap. 3.2, pp. 29-30.
(14) Liège, 6e ch., 13 octobre 2016, précité (c'est nous qui soulignons).
(15) Article 4, § 1er, 1°, de la loi Vie privée.
(16) Article 4, § 1er, 4°, de la loi Vie privée.
(17) Civ. Bruxelles, 15 octobre 2003, *J.T.*, 2004, pp. 140-141. Voy. J.-P. Moiny et J.-M. Van Gyseghem, « Vie privée et protection des données. Jurisprudence belge », *Chronique de jurisprudence en droit des technologies de l'information (2002-2008)*, *R.D.T.I.*, 2009, no 35, p. 89.
(18) C.J.C.E., 7 mai 2009, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*, aff. C-553/07. Voy. C. Gayrel, « Chronique de jurisprudence en droit des technologies de l'information (2009-2011). Libertés et société de l'information - Cour de justice de l'Union européenne, Tribunal de première instance et Tribunal de la Fonction publique européenne », *R.D.T.I.*, nos 48 et 49, 2012, pp. 95-96.
(19) Article 10 de la loi Vie privée. Voy. E. Degrave et A. Lachapelle, « Le droit d'accès du contribuable à ses données à caractère personnel et la lutte contre la fraude fiscale », note sous C. const., 27 mars 2014, *R.G.C.F.*, 2014, p. 325 ; C. de Terwangne et J.-M. Van Gyseghem, « Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution », *op. cit.*, pt 2.2.6.2.3.
(20) Cass., 14 janvier 2013, note E. Degrave, « Transparence administrative et traitements de données à caractère personnel », *R.D.T.I.*, 2013, no 53, pp. 53-64.
(21) *Ibidem*, p. 55.

biais de la déclaration du traitement effectuée auprès de la Commission de la protection de la vie privée et dont une copie avait été transmise à cette personne.

Dans l'affaire des données traitées par la banque objet de la présente analyse, la Cour de cassation va redescendre son exigence d'un cran. En effet, plutôt que d'exiger, dans la ligne de son arrêt antérieur, que des informations sur les données traitées soient effectivement transmises, elle admettra comme valide le raisonnement de la cour d'appel qui estimait que l'information qui avait été communiquée au client lui signalant que sa carte n'avait pas fait l'objet d'une utilisation frauduleuse permettait à ce client de « déduire qu'aucune opération réalisée au moyen de cette carte de crédit n'avait été enregistrée sur son compte ». La Cour de cassation déclare que ce raisonnement ne restreint pas la portée du droit d'accès. Cela étant, il ne s'agit plus d'exiger une communication spécifique, la Cour en appelle au bon sens et à la capacité de déduction de la personne concernée.

Une telle position ne pourra plus être soutenue à l'avenir. Le règlement européen général sur la protection des données stipule en effet expressément que le droit d'accès, garanti à son article 15, impose au responsable du traitement de fournir aux personnes exerçant leur droit une copie des données à caractère personnel les concernant faisant l'objet d'un traitement[22]. Ce sont donc bien les données telles quelles qui devront être transmises, accompagnées d'une série d'informations accessoires qui, soit étaient déjà prévues dans le régime actuel de la loi Vie privée (telles que l'indication des finalités poursuivies, des catégories de destinataires, de l'origine des données, de la logique sous-tendant le traitement automatisé des données débouchant sur des décisions automatisées, et de l'existence des droits de rectification, d'effacement, d'opposition et de recours) soit sont nouvelles (telle l'information à fournir sur les flux transfrontières de données et sur la durée de conservation).

En guise de conclusion

La législation de protection des données à caractère personnel a vocation à s'appliquer à l'ensemble des acteurs de la société, issus du secteur public comme du secteur privé, de la multinationale à la P.M.E., du cabinet d'avocat à l'hôpital. Cette législation trop souvent encore méconnue 25 ans après son adoption, comme en atteste la décision commentée dans les paragraphes qui précèdent, vise à protéger les individus dans une société de l'information où la richesse et la valeur économique découlent désormais essentiellement des données, et en premier lieu des données à caractère personnel.

Il est impératif aujourd'hui d'apporter les éclairages nécessaires pour familiariser les acteurs avec les principes de protection mis en place. Cela est d'autant plus crucial que se profile l'entrée en application du règlement européen général sur la protection des données (R.G.P.D.), prévue pour le 25 mai 2018. Ce règlement ne fait pas table rase du passé mais, s'appuyant sur le régime juridique actuel, renforce la protection offerte aux personnes dont les données font l'objet de traitement et responsabilise de façon accrue les différents intervenants[23]. Là où il tranche radicalement toutefois, c'est sur le plan des sanctions. Dans un souci de garantir l'effectivité du régime mis en place, les autorités de contrôle sont dotées de pouvoirs de sanction élargis et, surtout, le règlement instaure des sanctions qui se veulent particulièrement dissuasives[24].

Le présent commentaire a eu pour objectif de mieux élucider le champ d'application de la protection offerte. En réalité, celle-ci ne dépend presque plus jamais aujourd'hui de la notion de fichier sur laquelle s'est erronément arrêtée la Cour de cassation, puisque la législation s'applique dès qu'il est fait recours, ne fût-ce que partiellement, à des moyens automatisés pour traiter les données. Dans un monde où les ordinateurs et leurs capacités ont envahi non seulement les bureaux mais aussi les cartables, les poches et les poignets et où les données se recueillent à partir d'objets connectés qui font partie du quotidien, il est clair que la législation de protection des données trouve désormais à s'appliquer tous azimuts, bien au-delà de la notion de fichier.

Cécile de TERWANGNE

DROIT JUDICIAIRE

- Appel différé des jugements avant dire droit (article 1050, alinéa 2, C. jud.)
- Appel immédiat du jugement mixte
- Appel dirigé uniquement contre les mesures avant dire droit
- Irrecevabilité

Bruxelles (41e ch.), 27 juillet 2017

Siég. : A. Jannone.

Plaid. : MMes J. Heneffe *loco* E. Degrez et M. Ngako Pounde.

(G. c. H.).

Un jugement mixte, c'est-à-dire un jugement contenant d'une part des mesures définitives et d'autre part des mesures avant dire droit, est immédiatement appelable, pour autant que l'une des mesures définitives contenues dans celui-ci soit frappée d'appel.

Lorsque seules les mesures avant dire droit contenues dans le jugement mixte sont frappées d'appel, le jugement est, en application de l'article 1050, alinéa 2, du Code judiciaire, soumis au retardement de l'appel.

[...]

Discussion.

1.1. L'article 1050, alinéa 2, du Code judiciaire, modifié par la loi du loi du 19 octobre 2015 modifiant le droit de la procédure civile et portant des dispositions diverses en matière de justice, dite loi pot-pourri I, énonce que :

« Contre une décision rendue sur la compétence ou, sauf si le juge en décide autrement, une décision avant dire droit, un appel ne peut être formé qu'avec l'appel contre le jugement définitif ».

La Cour de cassation enseigne qu'un jugement est définitif au sens de l'article 19, alinéa 1er, du Code judiciaire, lorsque le juge a épuisé sa juridiction sur une question litigieuse, c'est-à-dire une question ayant fait l'objet d'un litige entre les parties et qui a été soumise aux débats (Cass., 12 juin 2014, *Pas.*, 2014, I, p. 1485 ; Cass., 8 octobre 2001, *Pas.*, 2001, I, p. 1600 ; A. Hoc, *op. cit.*, p. 252, no 9).

Suivant l'alinéa 3 de cette disposition, le jugement *avant dire droit* est celui qui ordonne une mesure préalable destinée soit à instruire la demande ou à régler un incident portant sur une telle mesure, soit à régler provisoirement la situation des parties (*cfr* G. de Leval, « Le jugement », *in* G. de Leval [dir.], *Droit judiciaire*, t. 2, *Manuel de procédure civile*, Bruxelles, Larcier, 2015, p. 651, no 7.23 et note 2789).

Tant les jugements tendant à régler provisoirement la situation des parties dans l'attente d'un jugement définitif que les jugements prescrivant une mesure d'instruction sont donc soumis, par le nouvel article 1050, alinéa 2, au retardement de l'appel (A. Hoc, « L'appel différé des jugements avant dire droit », *in* H. Boularbah et J.-F. van Drooghenbroeck, *Pot-Pourri I et autres actualités de droit judiciaire*, C.U.P., 2016, vol. 164, pp. 240 et s. ; F. Lejeune, « Simplification de la procédure par défaut et métamorphose de l'appel », *in* J. Englebert et X. Taton [dir.], « Le procès civil efficace ? », Limal, Anthemis, 2015, p. 130, no 40 ; F. Lejeune, « L'impact de la loi pot-pourri I sur l'expertise », *in Revue belge du dommage corporel et de médecine légale*, 2016, p. 42).

1.2. Pour apprécier le contenu et la portée des décisions prises par le premier juge, il convient de lire le dispositif du jugement attaqué avec les motifs qui le précèdent, étant entendu que toute décision relative à la contestation est un dispositif et ceci même si elle est énoncée dans les motifs (motif décisoire) et ceci quelle que soit la forme dans laquelle elle est exprimée (G. de Leval, *op. cit.*, p. 644, no 7.17. Le professeur de Leval, qui cite la jurisprudence de la Cour de cassation, précise que le fait que la décision du juge se trouve à une mauvaise place ne lui fait pas perdre sa qualité).

(22) Article 15, § 3, du R.G.P.D.
(23) Voy. C. de Terwangne, K. Rosier et B. Losdyck, « Lignes de force du nouveau règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016, pp. 5-56
(24) Pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaire annuel mondial (article 83, § 5, R.G.P.D., précité).