Bureau de dépôt : Louvain 1
Hebdomadaire, sauf juillet et août
ISSN 0021-812X
P301031

larcier

strada lex
Journal des tribunaux

http://jt.larcier.be
6 septembre 2014 - 133e année
27 - N° 6571
Georges-Albert Dal, rédacteur en chef

Sommaire

Doctrine

Jurisprudence

Chronique

LA TRAITE DES ÊTRES HUMAINS ET LE TRAVAIL FORCÉ

Charles-Éric Clesse, Frédéric Kurz, Patricia Le Cocq, Véronique Truillet

Au travers de la jurisprudence des Cours (supra) nationales et de certaines Cours étrangères, les auteurs étudient afin de mieux les combattre les infractions de traite des êtres humains, de marchands de sommeil, la problématique du travail forcé.

> Collection : Grands arrêts
212 p. • 91,00 € • Édition 2014

strada lex Ouvrage disponible en version électronique sur www.stradalex.com

larcier www.larcier.com

commande@larciergroup.com
c/o Larcier Distribution Services sprl
Fond Jean Pâques, 4 b – 1348 Louvain-la-Neuve – Belgique
Tél. 0800/39 067 – Fax 0800/39 068

J.T. n° 6571 - 27/2014
larcier - © Groupe Larcier
F.U.N.D.P. /

Doctrine

La vie privée et les technologies dans l'administration, la relation de travail et le domaine de la santé

Chronique de jurisprudence 2003-2013

Ces dix dernières années sont marquées par la mise en place de nombreux outils informatiques aux fins les plus diverses. Corollairement à ce phénomène, la protection de la vie privée des citoyens requiert une attention toute particulière. Les questions soulevées sont foisonnantes et les solutions proposées par les cours et tribunaux le sont tout autant. C'est la raison pour laquelle cette chronique se concentre sur la protection de la vie privée face aux traitements de données à caractère personnel organisés dans trois secteurs particuliers : l'administration, la relation de travail et le domaine de la santé. Cette chronique ne prétend pas à l'exhaustivité et analyse les décisions de jurisprudence les plus significatives rendues dans ces trois domaines[1].

1 La vie privée, les technologies et l'administration[2]

1. L'e-gouvernement. — L'administration est désormais entrée dans l'ère de l'e-gouvernement, dite aussi « administration électronique ». L'e-gouvernement se caractérise notamment par un nouveau mode de fonctionnement de l'administration fondé sur la collaboration et l'échange maximal des données à caractère personnel des citoyens entre les institutions publiques qui en ont besoin. Par ailleurs, l'e-gouvernement est encadré par des règles récentes et particulières qui mêlent le droit administratif et le droit de la protection des données à caractère personnel. Celles-ci visent à consacrer un équilibre entre l'efficacité de l'administration et le droit fondamental à la protection de la vie privée[3]. Ainsi, désormais, des obligations nouvelles pèsent sur les administrations, tandis que les citoyens peuvent prétendre à des prérogatives supplémentaires, comme l'illustrent les décisions exposées dans les lignes qui suivent. Malheureusement, ces règles sont encore trop peu connues des avocats. D'un côté, les administrativistes semblent craindre les ordinateurs et les questions que leur utilisation soulève, tandis que les spécialistes du droit des technologies semblent peu à l'aise dans les méandres du droit administratif. Par conséquent, des arguments juridiques pertinents manquent d'être soulevés devant les cours et tribunaux, comme l'illustre par exemple un arrêt rendu par le Conseil d'État en 2011[4].

Dans cette affaire, le Syndicat national des propriétaires, notamment, intente un recours en annulation au Conseil d'État à l'encontre d'un arrêté de gouvernement portant exécution du Code bruxellois du logement. Celui-ci institue un droit de gestion publique dans le chef d'opérateurs immobiliers publics, qui porte sur certains logements, parmi lesquels figurent les « logements inoccupés ». Pour considérer que le logement est inoccupé, la norme attaquée prévoit qu'il faut notamment se référer à un seuil de consommation d'eau et un seuil de consommation d'électricité, fixés par ledit arrêté. Les requérants soutiennent notamment que ces informations sont des données à caractère personnel et critiquent le fait que l'arrêté ne précise pas « les conditions dans lesquelles ces informations peuvent être délivrées » et n'indique pas « les garanties suivant lesquelles elles

(1) Le lecteur trouvera encore d'autres informations sur ces trois matières dans *R.D.T.I.*, 2012, nos 48-49, pp. 68-146.
(2) Cette partie est rédigée par Elise Degrave.
(3) Pour de plus amples détails à ce sujet, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée - Légalité, transparence et contrôle*, Bruxelles, Larcier, coll. C.R.I.D.S., 2014.
(4) C.E., a.s.b.l. *Syndicat national des propriétaires* e.a., arrêt no 216.928 du 19 décembre 2011.

pourraient l'être »[5]. Malheureusement, les requérants n'étayent pas leur argumentation. En particulier, ils n'invoquent pas la loi du 8 décembre 1992[6] et ne précisent pas quelles dispositions légales sont violées par l'acte attaqué. Dès lors, le Conseil d'État répond que le moyen « ne vise (...) pas les dispositions ou principes qui, à l'estime des requérantes, seraient violés, ni en quoi ils l'auraient été. Il s'ensuit que, sans qu'il s'agisse de faire preuve d'un formalisme excessif, le moyen doit être déclaré irrecevable en tant qu'il prend appui sur ce grief »[7].

2. L'encadrement légal des traitements de données dans l'administration. — Traditionnellement, l'administration est soumise aux principes de légalité et de spécialité issus du droit constitutionnel et du droit administratif. Ainsi ne peut-elle agir que dans le cadre des missions qui lui ont été légalement dévolues. En outre, en vertu de l'article 22 de la Constitution, toute ingérence dans le droit fondamental à la protection de la vie privée doit être encadrée par une loi précise et prévisible. C'est pourquoi, le législateur doit rigoureusement encadrer les traitements de données mis en place au sein de l'administration, tels que la création de base de données contenant les données à caractère personnel des citoyens et l'échange de ces données entre les institutions publiques.

Le législateur fédéral est-il seul compétent pour ce faire? Il convient aujourd'hui de répondre par la négative et de reconnaître que tant le législateur fédéral que les législateurs communautaires et régionaux peuvent organiser des traitements de données à caractère personnel dans l'exercice de leurs compétences[8]. Comme l'affirme la Cour constitutionnelle, « la consécration, par la Constitution et les traités internationaux, de droits et libertés fondamentaux ne signifie en aucune manière que leur réglementation n'appartiendrait, en tant que telle, qu'à l'autorité fédérale. C'est à chaque autorité qu'il appartient d'en assurer le respect en les concrétisant lorsqu'elle exerce les compétences qui sont les siennes »[9].

Comment et jusqu'où le législateur doit-il encadrer les traitements de données à caractère personnel pour répondre au prescrit de l'article 22 de la Constitution? La Cour constitutionnelle affirme qu'elle « peut examiner si le législateur a respecté les obligations internationales qui découlent des dispositions invoquées de la directive précitée, de la Convention n° 108 précitée auxquelles la loi précitée du 8 décembre 1992 et ses modifications ultérieures donnent exécution »[10]. Et d'ajouter que « ces obligations forment un tout indissociable des garanties qui sont reproduites à l'article 22 de la Constitution. Une disposition qui est contraire à ces obligations violerait par conséquent le droit au respect de la vie privée, tel qu'il est garanti à l'article 22 de la Constitution »[11]. Pour respecter cet ensemble indissociable d'exigences, le législateur doit définir les « éléments essentiels du traitement »[12] de données à caractère personnel. C'est pourquoi il lui revient, par exemple, de définir précisément l'objectif du traitement de données[13].

3. La limitation des utilisateurs des données détenues par l'administration. — Nombre de bases de données détenues par l'administration sont encadrées par une loi particulière qui en limite l'accès à certaines personnes. Ainsi en va-t-il notamment du registre national. L'accès à cette base de données est limité principalement aux autorités publiques pour l'accomplissement de leurs missions légales[14], si bien qu'une société privée ne peut pas la consulter[15].

Durant longtemps, tel fut également le cas du répertoire des véhicules de la direction générale Mobilité et sécurité routière du S.P.F. Mobilité et Transports[16], auquel ne pouvaient pas accéder les sociétés privées ayant obtenu la concession du stationnement payant sur la voie publique. C'est pourquoi certains juges ont dispensé des automobilistes de payer la redevance de stationnement qui leur était réclamée. Le problème était le suivant : les sociétés privées ayant en concession le stationnement public dans certaines communes accédaient directement aux données enregistrées dans le répertoire de la D.I.V. pour identifier les propriétaires de véhicules ayant omis de payer le montant dû pour le stationnement de leur véhicule. Deux juges de paix ont débouté ces sociétés privées de leur action en justice, jugeant leur demande de paiement illégale. Ces juges ont constaté que les données de la D.I.V. sont des données à caractère personnel dont l'utilisation est protégée par la loi du 8 décembre 1992 qui impose notamment que les données à caractère personnel soient traitées pour une finalité déterminée. L'article 6 de l'arrêté royal du 20 juillet 2001 relatif à l'immatriculation des véhicules[17] détermine les finalités d'utilisation des données de la D.I.V. Les sociétés privées pouvaient-elles se prévaloir de l'article 6, § 2, 2°, de cette arrêté royal qui prévoit que le répertoire de la D.I.V. peut être consulté pour « l'identification de la personne physique ou morale par laquelle sont dues les taxes ou les redevances liées à l'acquisition, l'immatriculation, la mise en circulation, l'utilisation ou la mise hors circulation d'un véhicule »? À la suite d'un avis de la Commission de la protection de la vie privée[18], les deux juges de paix ont répondu par la négative[19] : les sociétés privées ne perçoivent ni une taxe, ni une redevance, si bien qu'en consultant le répertoire de la D.I.V., elles agissent en violation de la loi du 8 décembre 1992 et de l'arrêté royal relatif à l'immatriculation des véhicules. À l'époque, ces décisions judiciaires ont fait grand bruit dans la presse et ont incité les législateurs à revoir l'encadrement normatif de cette problématique. Aujourd'hui, la question est réglée au plan régional[20]. Les sociétés privées sont désormais habilitées à consulter le répertoire de la D.I.V., ce qui ne les dispense toutefois pas de l'obligation d'obtenir, au préalable, l'autorisation du comité sectoriel compétent[21].

4. L'obligation d'obtenir l'autorisation du comité sectoriel compétent[22]. — En principe, les données détenues par l'administration fédérale[23] ne peuvent être utilisées qu'à la condition, pour le demandeur de ces données, d'avoir obtenu l'autorisation du comité sec-

(5) *Ibidem*, p. 19.
(6) Il s'agit de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993. Cette loi est visée par les termes « loi du 8 décembre 1992 » dans la suite de cette étude.
(7) *Ibidem*, p. 22.
(8) Il n'en a cependant pas toujours été ainsi. Au sujet de l'évolution de la réponse à cette question, voy. E. Degrave, « L'article 22 de la Constitution et les traitements de données à caractère personnel », *J.T.*, 2009, p. 365; J. Vande Lanotte et G. Goedertier, *Handboek Belgisch Publiekrecht*, Bruges, die Keure, 2010, pp. 126-129, n° 214; N. Bonbled et M. Verdussen, « Les droits constitutionnels et le fédéralisme », *in* M. Verdussen et N. Bonbled (dir.), *Les droits fondamentaux en Belgique*, Bruxelles, Bruylant, 2011, pp. 248-251 et 259-261; M. Melchior et C. Courtoy, « La limitation des droits fondamentaux », *in* M. Verdussen et N. Bonbled (dir.), *Les droits fondamentaux en Belgique*, *op. cit.*, pp. 277-281.
(9) C. const., arrêt n° 50/2003, du 30 avril 2003, B.8.10; C. const., arrêt n° 51/2003, du 30 avril 2003, B.4.12.
(10) C. const., arrêt n° 29/2010 du 18 mars 2010, B.5.3.
(11) *Idem*.
(12) C. const., arrêt n° 202/2004 du 21 décembre 2004, B.6.2. et B.6.3.
(13) C. const., arrêt n° 15/2008 du 14 février 2008, B.22; C. const., arrêt n° 29/2010, *op. cit.*, B.11 et s; C. const., arrêt n° 1/2011 du 13 janvier 2011, B.12.1 et s. Pour de plus amples détails au sujet des éléments essentiels d'un traitement de données, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée - Légalité, transparence et contrôle*, *op. cit.*, n° 103.
(14) Voy. l'article 5 de la loi du 8 août 1983 organisant un registre national des personnes physiques, *M.B.*, 21 avril 1984.
(15) À ce sujet, voy. l'arrêt de la cour d'appel de Bruxelles, analysé au n° 4.
(16) Ci-après « répertoire de la D.I.V. ».
(17) *M.B.*, 8 août 2001.
(18) Avis n° 37/2003 du 28 août 2003 relatif à l'accès au répertoire des véhicules de la direction générale Mobilité et sécurité routière du Service public fédéral Mobilité et transports en vue de l'identification de la personne physique ou morale par laquelle sont dues des taxes ou des redevances en matière de stationnement de véhicules. Cet avis est disponible sur le site de la Commission de la protection de la vie privée, www.privacycommission.be.
(19) J.P. Arlon-Messancy, 14 mai 2004, non publié; J.P. Ostende, 22 janvier 2008, non publié.
(20) Voy., pour la Wallonie, les articles 103 et 104 du décret du 27 octobre 2011 modifiant divers décrets concernant les compétences de la Wallonie, *M.B.*, 24 novembre 2011; pour la Flandre, le décret du 9 juillet 2010 portant recouvrement de rétributions de stationnement par des sociétés de parking, *M.B.*, 26 juillet 2010 et, à Bruxelles, l'ordonnance du 22 janvier 2009 portant organisation de la politique de stationnement et création de l'agence du stationnement de la Région de Bruxelles-Capitale, *M.B.*, 30 janvier 2009 (à ce sujet, voy. également la délibération du comité sectoriel pour l'Autorité fédérale n° 23/2013 du 25 juillet 2013).
(21) Il s'agit, en l'occurrence, du comité sectoriel pour l'Autorité fédérale. Au sujet des autorisations des comités sectoriels, voy. n° 4.
(22) Un comité sectoriel est un organe de décision institué au sein de la Commission de la protection de la vie privée. Il en existe actuellement six à savoir, le comité sectoriel du registre national, le comité sectoriel pour l'Autorité fédérale, le comité sectoriel de la sécurité sociale et de la santé, le comité sectoriel Surveillance statistique, la comité sectoriel de la Banque-carrefour des entreprises, et le comité sectoriel Phénix. À ce sujet, voy. sur le site internet de la Commission de la protection de la vie privée, http://www.privacycommission.be/fr/comites-sectoriels.
(23) S'agissant des données détenues par les autorités fédérées, voy. en Flandre, le décret du 18 juillet 2008 relatif à l'échange de données administratives, *M.B.*, 29 octobre 2008 et en Wallonie, l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *M.B.*, 23 juillet 2013.

J.T. n° 6571 - 27/9/2014
Larcier © Groupe Larcier
F.U.N.D.P. /

toriel compétent. Une décision de la cour d'appel de Bruxelles illustre l'importance de cette règle. Dans cette affaire, il est question de la société Fidel ID qui a mis au point un service informatique, dénommé Freedelity[24], permettant aux consommateurs d'utiliser leur carte d'identité électronique comme carte de fidélité auprès de tous les commerçants ayant souscrit à ce service. Lorsqu'un client introduit sa carte d'identité dans le lecteur de cartes Freedelity, ses informations personnelles sont copiées dans l'ordinateur du commerçant, mais également dans une base de données détenue par la société Fidel ID. Accumulant un grand nombre de données, la société Fidel ID souhaitait pouvoir identifier de manière unique chaque consommateur, dans sa base de données, en enregistrant également leur numéro d'identification au registre national. Au préalable, elle a demandé l'autorisation du comité sectoriel du registre national qui a refusé de la lui donner, au motif, en substance, que la loi du 8 août 1983 sur le registre national n'autorise pas les sociétés privées à traiter cette information. La société Fidel ID a toutefois outrepassé cette interdiction et a enregistré le numéro d'identification au registre national de chaque consommateur dans sa base de données. Ayant connaissance de ce fait, une société concurrente, la société Fidelsys, a assigné en justice la société Fidel ID arguant notamment du fait qu'en violant la loi du 8 août 1983 sur le registre national, Fidel ID bénéficie d'un « avantage concurrentiel déloyal [la] rendant coupable d'un acte contraire aux pratiques honnêtes du marché ». En d'autres termes, Fidelsys recourt aux règles de protection des données à caractère personnel pour justifier la violation de la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur qu'elle n'était pas parvenue à démontrer en première instance. Cet argument convainc la cour d'appel de Bruxelles. Elle affirme qu'« à défaut d'autorisation du comité sectoriel du registre national, Fidel ID utilise le numéro de registre national repris sur la carte d'identité électronique en violation de la loi (...) En l'espèce, la violation de la loi du 8 août 1983 par Fidel ID porte atteinte aux intérêts professionnels de Fidelsys dans la mesure où elle crée en faveur de Fidel ID un avantage compétitif : (...) l'utilisation du numéro du registre national repris sur la carte d'identité électronique permet d'éviter des investissements importants que devrait consentir toute autre entreprise respectueuse de la loi pour concevoir, fabriquer et gérer une carte à puce susceptible de prodiguer les mêmes avantages économiques que le système Freedelity ». La cour d'appel juge la demande de Fidelsys fondée et condamne Fidel ID au paiement d'une astreinte de 5.000 EUR par utilisation du numéro du registre national[25].

5. Le risque d'une sanction disciplinaire en cas d'accès illégal à des données à caractère personnel. — Il peut arriver qu'un agent de l'administration soit tenté de consulter, par curiosité, des données auxquelles il a accès dans le cadre de ses fonctions. Il s'agit là d'une utilisation abusive de données à caractère personnel, puisque l'agent en question ne peut justifier une telle consultation par la nécessité d'accomplir les missions qui lui sont légalement dévolues. Cet agent risque alors de se voir imposer une sanction disciplinaire. Tel a été le cas, par exemple, d'un agent de la commune d'Uccle qui, connaissant des difficultés sentimentales, a succombé à la tentation de consulter les données de son ex-petite amie au registre national et d'en faire un usage d'intérêt personnel. Il a récidivé à plusieurs reprises, malgré plusieurs avertissements des dirigeants du département de l'état civil. Le conseil communal d'Uccle lui a imposé la sanction de la démission d'office. L'agent communal a attaqué cette décision devant le Conseil d'État, arguant notamment du fait que ses difficultés sentimentales et le nombre d'années de carrière constituaient des circonstances atténuantes qui justifiaient une sanction plus clémente. Le Conseil d'État a confirmé la décision du conseil communal. Il s'est référé notamment à « la gravité des faits reprochés au requérant et l'atteinte grave portée à la confiance du public » et au fait que « le requérant a agi en toute connaissance de cause par rapport à l'usage autorisé des données contenues dans le registre national »[26]. Le Conseil d'État a également soutenu que le conseil communal « a pu considérer que ni les raisons sentimentales alléguées, ni la carrière passée du requérant ne pouvaient constituer des circonstances atténuantes justifiant une sanction plus modérée »[27].

6. Le principe de la collecte unique des données à caractère personnel détenues par l'administration. — Un objectif majeur de l'e-gouvernement est de renforcer l'efficacité de l'administration tout en allégeant autant que possible les démarches administratives des citoyens. C'est pourquoi, la structure et le fonctionnement de l'administration sont progressivement repensés pour répondre au principe de la collecte unique des données. Ce principe signifie que, dès qu'une donnée à caractère personnel d'un citoyen est enregistrée dans une base de données de l'administration, elle ne peut plus être demandée une seconde fois à la personne concernée. Par conséquent, si une institution publique a besoin de cette information et ne la détient pas, elle doit l'obtenir auprès de l'institution qui la détient déjà, et ne peut plus la demander à la personne dont elle gère le dossier. Pour l'heure, le principe de la collecte unique de données est consacré notamment par la loi du 15 janvier 1990 sur la Banque-carrefour de la sécurité sociale et s'impose donc aux institutions de sécurité sociale[28]. Le principe de la collecte unique des données est également ancré dans la loi du 8 août 1983 sur le registre national[29].

Le 27 juin 2006, la cour du travail de Liège a rendu un arrêt faisant application du principe de la collecte unique des données en matière de droit à la pension[30]. L'Office national des pensions reprochait à un homme pensionné de ne pas l'avoir averti du décès de son épouse, ce qui avait des conséquences au niveau du montant de la pension qui lui était due. L'Office national des pensions exigeait de récupérer les sommes indûment payées depuis cinq ans. Or cet assuré social avait averti la commune, en temps utile, du décès de son épouse. Cette information était donc enregistrée au registre national. Faisant partie du réseau sectoriel de la sécurité sociale, l'Office national des pensions y avait donc accès par l'intermédiaire de la Banque-carrefour de la sécurité sociale. Compte tenu de ces éléments de fait et de droit, la cour affirme qu'« un assuré social ne peut se voir imposer personnellement une obligation qui doit déjà être légalement remplie par une institution dont c'est la mission. C'est donc à tort que l'O.N.P. soutient que l'information transmise par la Banque-carrefour doit être doublée par une information émanant de l'assuré social et que seule celle-ci permettrait au pensionné de remplir ses obligations envers lui [...] »[31].

Le 21 avril 2010, appliquant également le principe de la collecte unique des données, la cour du travail de Bruxelles[32] a fait droit à la demande d'un assuré social, M. E.G., qui réclamait le revenu d'intégration sociale. Le C.P.A.S. refusait l'octroi de cette indemnité au motif que M. E.G. n'avait pas fourni un certain nombre de documents et avait dès lors manqué à son devoir de collaboration. Dans sa motivation, la cour du travail affirme qu'il faut déduire de l'article 11 de la loi du 15 janvier 1990 précité qu'« un manque de collaboration du demandeur ne peut être envisagé à propos d'informations auxquelles le C.P.A.S. peut accéder, accessibles via la Banque-carrefour de la sécurité sociale »[33]. Or, en l'espèce, « la plupart des documents prétendument manquants étaient accessibles via la Banque-carrefour ou le registre national : le C.P.A.S. n'avait pas à la demander à M. E.G.; il aurait dû les recueillir d'initiative »[34]. C'est pourquoi, la cour décide que M. E.G. a droit au revenu d'intégration sociale[35].

Dans un jugement du 9 octobre 2007[36], le juge de paix de Grâce-Hollogne encourage le législateur à mettre en place une solution sem-

(24) Voy. www. freedelity.be.
(25) Pour un commentaire de cette décision, voy. E. Degrave, « La carte d'identité électronique utilisée comme carte de fidélité : un traitement de données à caractère personnel illégal sanctionné par la cour d'appel de Bruxelles », observations sous Bruxelles, 9e ch., 9 mai 2012 , *J.T.*, 2012, pp. 691-63 ainsi que J.-M. Van Gyseghem, « La carte d'identité électronique et les apprentis sorciers », *R.D.T.I.*, 2014, à paraître.
(26) C.E., *Van Merris*, 3 avril 2006, n° 157.657.
(27) *Idem*. Voy. toutefois C.T. Liège, sect. Namur, 13e ch., 10 novembre 2009, R.G. no 8.631/2008 commenté sous le no 9 de la présente contribution.
(28) Ainsi, l'article 11*bis*, § 2, de cette loi dispose que « pour autant que les données sociales nécessaires pour l'octroi d'un droit supplémentaire soient disponibles dans le réseau (...), les instances d'octroi sont obligées de les demander exclusivement auprès de la Banque-carrefour (...) »
(29) L'article 6 de la loi du 8 août 1983 organisant un registre national des personnes physiques dispose que « § 1er. Les autorités, les organismes et les personnes visés à l'article 5, qui sont autorisés à consulter les données du registre national, ne peuvent plus demander directement lesdites données à une personne (...) § 2. Dès qu'une donnée a été communiquée au registre national et enregistrée dans ledit registre, la personne concernée n'est pas tenue de la communiquer directement aux autorités, organismes et personnes visés à l'article 5, qui sont autorisés à consulter les données du registre national.
(30) C.T. Liège, 27 juin 2006, *J.L.M.B.*, 2007, pp. 1043-1047.
(31) *Ibidem*, p. 1047.
(32) C.T. Bruxelles, 8e ch., 21 avril 2010, R.G. nos 2008/AB/51591 et 2009/AB/51809.
(33) *Ibidem*, 4e feuillet.
(34) *Ibidem*, 6e feuillet.
(35) *Ibidem*, 8e feuillet.
(36) J.P. Grâce-Hollogne, 9 octobre 2007, *J.L.M.B.*, 2010, pp. 1845-1854, note de N. Bernard.

J.T. n° 6571 - 27/9/2014
Larcier © Groupe Larcier
F.U.N.D.P. /

blable pour que les personnes en situation de pauvreté n'aient plus à prouver leur statut pour prétendre à un logement social. Il affirme que le système actuel, qui fait reposer la charge de la preuve de la pauvreté sur le demandeur d'un logement social, est « suranné compte tenu de la nouvelle culture administrative que les pouvoirs publics wallons s'efforcent d'instaurer après les déboires que l'on sait, vécus par le secteur du logement social (...). Les progrès accomplis (...) du côté de la Banque-carrefour de la sécurité sociale pourraient supprimer un grand nombre de cercles vicieux et d'effets pervers liés aux difficultés que les pauvres gens ont à prouver leur pauvreté. Ceci reste cependant à réaliser, à mettre en pratique. Ceci doit pénétrer des esprits qui restent trop souvent imprégnés de la culture ancienne, autoritaire et bureaucratique, ignorant les collaborations interservices dans l'intérêt des usagers »[37].

7. La transparence des traitements de données à caractère personnel. — Comme tout responsable de traitement de données, l'administration qui traite des données à caractère personnel est soumise à deux obligations de transparence : elle doit répondre au citoyen qui demande d'accéder à ses données à caractère personnel, en vertu de l'article 10, § 1er, de la loi du 8 décembre 1992, et elle doit déclarer à la Commission de la protection de la vie privée les traitements de données à caractère personnel qu'elle effectue. Cette obligation est prévue par l'article 17 de la loi du 8 décembre 1992.

Un arrêt de la Cour de cassation du 14 février 2013[38] rappelle la distinction entre ces deux obligations[39]. Dans cette affaire, J.M.D. désire connaître les informations sur lesquelles la Communauté française s'est fondée pour calculer la téléredevance qui lui est réclamée. Il suspecte une erreur dans le calcul de celle-ci. En guise de réponse, la Communauté française lui fait parvenir une copie de la déclaration de traitement introduite auprès de la Commission de la protection de la vie privée, mais non une copie des données personnelles qui le concernent. La cour d'appel de Liège considère que la Communauté française a correctement répondu à la demande de J.M.D. Cet arrêt de la cour d'appel de Liège est cassé par la Cour de cassation. Cette dernière estime, en somme, qu'en rejetant la demande de J.M.D. formulée sur la base de l'article 10 de la loi du 8 décembre 1992 au motif qu'il a déjà obtenu les informations qui figurent dans la déclaration de traitement établie en vertu de l'article 17 de la loi du 8 décembre 1992, la cour d'appel ne justifie pas légalement sa décision.

2 La vie privée, les technologies et la relation de travail[40]

8. La loi du 8 décembre 1992 et les données professionnelles. — La loi du 8 décembre 1992 s'applique aux traitements de données, même s'il s'agit de données professionnelles. On trouve peu de jurisprudence faisant application des principes de la loi du 8 décembre 1992 par rapport à des questions liées à la gestion quotidienne des données relatives à des travailleurs (traitements relatifs au paiement des salaires, évaluations, sélection des candidats...). Cette loi a été davantage évoquée ces dernières années dans le cadre litiges impliquant l'usage des T.I.C. et de la vidéosurveillance dans les relations de travail.

La particularité des contextes dans lesquels la loi du 8 décembre 1992 est ainsi prise en compte est le fait qu'elle s'applique alors cumulativement avec d'autres dispositions légales ou conventions collectives de travail (C.C.T.). En matière de prise de connaissance de courriers électroniques, SMS, de données téléphoniques ou encore de données de trafic internet, il y a lieu de tenir compte de dispositions plus spécifiques qui s'ancrent dans la législation relative aux communications électroniques et visent à régir la protection des données à caractère personnel dans ce secteur. Les C.C.T. ont quant à elles vocation à fixer, au terme d'une négociation entre les partenaires sociaux, un cadre pour certaines formes de surveillances en tenant compte des lois applicables, notamment de la loi du 8 décembre 1992. La plupart des principes découlant de cette loi sont donc repris et contextualisés dans ces C.C.T. Nous en épinglerons deux : la C.C.T. no 81[41] et la C.C.T. no 68[42].

Une autre spécificité de la jurisprudence en la matière est que, nonobstant l'existence de dispositions légales particulières qui assurent le droit au respect de la vie privée dans un contexte particulier, nombre de décisions fondent leur analyse de la problématique de la cybersurveillance et de la vidéosurveillance sur l'article 8 de la Convention européenne des droits de l'homme (C.E.D.H.), ce qui explique également la relative rareté de décisions de jurisprudence spécifiques à la loi du 8 décembre 1992, et ce nonobstant le fait qu'elle aurait trouvé à s'appliquer dans les cas tranchés.

A. Le traitement des données par l'employeur

9. Traitement de données judiciaires. — Dans un litige opposant une société d'intérim à un de ses clients s'est posée la question de l'obligation de la société d'intérim de vérifier les antécédents judiciaires d'un travailleur placé chez ce client qui était actif dans le secteur bancaire. Le client, victime d'une indélicatesse de l'intérimaire, invoquait, devant le tribunal de commerce, un manquement dans le chef de la société d'intérim dès lors qu'une telle vérification aurait permis de constater l'existence d'antécédents judiciaires dans le chef du travailleur concerné. Le tribunal constatera qu'au regard de l'article 8 de la loi du 8 décembre 1992, la société d'intérim ne pouvait traiter ces données judiciaires en l'absence de disposition légale le permettant explicitement pour la fonction à pourvoir[43].

10. Communication de données relatives à un travailleur à des tiers. — Dans un arrêt du 1er avril 2011, la cour du travail de Bruxelles[44] a estimé qu'un employeur ne pouvait se prévaloir de la loi du 8 décembre 1992 comme cause de justification pour le non-respect de ses obligations en matière d'affichage et de conservation d'une copie du contrat de travail sur le lieu des prestations, obligations qui s'imposent en cas d'occupation d'un travailleur à temps partiel avec des horaires variables. En l'espèce, l'employeur était une société de nettoyage. La travailleuse concernée prestait chez des clients de son employeur. Ce dernier estimait qu'il ne pouvait se conformer aux obligations précitées sans violer la loi du 8 décembre 1992, dès lors que cela impliquait la communication de données à caractère personnel relatives à la travailleuse à ses clients, alors que ceux-ci étaient des tiers à la relation de travail et n'avaient pas à connaître de ces informations. Le tribunal du travail avait suivi l'employeur en première instance. La cour du travail réformera la décision au motif que la communication de ces données aux clients de l'employeur est un traitement qui peut trouver une cause de justification sociale à l'article 5 de la loi du 8 décembre 1992, notamment au regard des obligations légales de l'employeur qui exigeaient implicitement cette communication dans le présent cas de figure[45]. Elle estime par ailleurs que si la préoccupation de l'employeur de s'assurer de la préservation de ces données contre des accès non autorisés était louable, il pouvait obtenir des garanties en termes de confidentialité par le biais d'un contrat à conclure avec ses clients.

11. Détournement du droit d'accès au registre national par un employé. — La cour du travail de Liège, section de Namur, a rendu un arrêt interpellant dans un litige opposant une caisse d'assurances sociales à une ancienne travailleuse[46]. La travailleuse avait reconnu avoir consulté à plusieurs reprises le registre national auquel elle avait accès

(37) *Ibidem*, p. 1850.
(38) Cass., 14 février 2013, R.G. no C.11.0777.F.
(39) Pour un commentaire de cet arrêt, voy. E. Degrave, « Transparence administrative et traitements de données à caractère personnel », note sous Cass., 14 février 2013, no C.11.0777.F, *R.D.T.I.*, 2014, pp. 56-64.
(40) Cette partie est rédigée par Karen Rosier.
(41) Convention collective de travail no 81 du 26 avril 2002, conclue au sein du Conseil national du travail, relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau, rendue obligatoire par l'arrêté royal du 12 juin 2002.
(42) Convention collective de travail no 68, conclue le 16 juin 1998 au sein du Conseil national du travail, relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail, rendue obligatoire par arrêté royal du 20 septembre 1998.
(43) Comm. Charleroi, 2e ch., 17 décembre 2009, *J.T.T.*, 2009, p. 398.
(44) C.T. Bruxelles, 1re ch., 1er avril 2011, *J.T.T.*, 2011, p. 379.
(45) La cour cite également deux autres causes de justification qui pourraient être envisagées : le consentement de la travailleuse (dans le cadre d'un accord à conclure avec celle-ci) et la poursuite d'un intérêt légitime dans le chef de l'employeur sans que ne prévalent l'intérêt ou les droits et libertés fondamentaux de la travailleuse.
(46) C.T. Liège, sect. Namur, 13e ch., 10 novembre 2009, R.G. no 8.631/2008.

J.T. n° 6571 - 27/2014
Larcier en Ligne - Larcier
F.U.N.D.P. /

dans le cadre de ses fonctions, et ce à des fins privées, à la suite de quoi elle avait été licenciée pour motif grave. La travailleuse contestait la régularité du congé sur le fond. Au cœur des débats, on retrouve la problématique du respect du secret professionnel, mais également celle du respect de la législation relative à la protection des données et, en particulier, de la loi du 8 août 1983 organisant un registre national des personnes physiques.

La cour relève que l'employeur avait été très explicite sur les règles à respecter par son personnel concernant le caractère confidentiel des données des clients, mais non sur les règles relatives à l'utilisation du registre national. La cour en conclut que l'employeur n'avait pas informé la travailleuse sur les règles d'utilisation du registre national et ne pouvait la sanctionner en la licenciant pour motif grave sans préalablement avoir mis en garde son employée et rappelé les obligations des utilisateurs. Si l'arrêt peut paraître bien sévère à propos des manquements imputés à l'employeur (et notamment eu égard au fait qu'en l'espèce, la travailleuse avait admis qu'elle savait que la consultation du registre national était interdite), on rappellera que l'article 16 de la loi du 8 décembre 1992 impose au responsable d'un traitement, tel un employeur, d'informer les personnes agissant sous son autorité des dispositions de cette loi et de ses arrêtés d'exécution, ainsi que de toute prescription pertinente relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel, ce qui inclut le cas échéant, les dispositions de la loi du 8 août 1983.

B. Le contrôle des communications électroniques par l'employeur

12. Notion de communications électroniques. — La loi du 8 décembre 1992 s'applique dès lors que la prise de connaissance d'une communication électronique, qu'il s'agisse de données de communications ou du contenu, implique le traitement de données relatives à une personne physique, à savoir à tout le moins les participants à la communication[47]. La notion de courriers électroniques englobe également les données de trafic internet, les SMS et les communications téléphoniques[48].

C'est donc, selon nous, à tort que la cour d'appel de Gand a estimé que le travailleur expéditeur d'un courrier électronique ne pouvait s'opposer à la production de celui-ci aux débats sur la base de la loi du 8 décembre 1992, et ce au motif que le contenu du courriel portait sur des informations financières et non sur des informations relatives à sa personne[49]. Le fait que la communication soit adressée par une personne physique suffit à rendre la loi applicable lorsque le courriel fait l'objet d'un traitement.

Par ailleurs, il est indifférent que le courrier électronique ait un objet professionnel ou privé pour que la loi du 8 décembre 1992 s'applique. Dans un arrêt du 15 décembre 2004[50], la cour du travail d'Anvers constate que l'affirmation contenue dans le préambule de la C.C.T. n° 81 aux termes de laquelle « lorsque l'objet et le contenu des données de communications électroniques en réseau ont un caractère professionnel non contesté par le travailleur, l'employeur pourra les consulter sans autre procédure » et l'article 11, alinéa 3, qui la reproduit au sein de la Convention, sont contraires à l'article 8 de la C.E.D.H. ainsi qu'aux articles 314*bis* du Code pénal et à l'article 109*ter*D de la loi du 21 mars 1991[51] et à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

1. Contrôle des courriers électroniques et du trafic internet

12*bis*. — Bien que régulièrement citée par la jurisprudence en la matière comme faisant partie du cadre légal régissant le contrôle s'appliquant en cas de contrôle du trafic internet[52], des courriels[53] ou des SMS[54], peu de décisions font véritablement l'analyse de l'application de cette loi. L'explication provient sans doute du cumul des textes régissant le contrôle des communications électroniques (essentiellement les dispositions légales qui consacrent le principe du secret des communications électroniques[55] et la C.C.T. n° 81) et du fait que la C.C.T. n° 81 intègre déjà certains principes issus de la loi du 8 décembre 1992. Une décision du tribunal du travail de Liège illustre d'ailleurs ce lien étroit entre les deux textes dans un litige relatif à un contrôle de l'usage de l'internet par un ouvrier, contrôle réalisé par l'employeur. Le tribunal rappelle que si la C.C.T. n° 81 n'avait pas encore été rendue obligatoire au moment du contrôle, l'obligation d'information préalable reprise dans la C.C.T. existait bel et bien en application de l'article 9 de la loi du 8 décembre 1992[56]. Pour les employeurs non liés par les conventions collectives, il s'agit d'ailleurs du seul texte applicable.

Nous ne reviendrons pas, dans le cadre de cette chronique, sur les manières diverses dont les décisions concilient le pouvoir de contrôle de l'employeur avec le caractère quasi absolu du secret des communications électroniques, même professionnelles, et renvoyons le lecteur à d'autres publications consacrées à ce sujet[57]. Nous épinglerons en revanche quelques décisions qui donnent un éclairage sur la portée des principes de transparence, de finalité et de proportionnalité de la loi du 8 décembre 1992, en matière de contrôle des données de communications électroniques, parfois au travers de l'application de la C.C.T. n° 81.

13. Principe de transparence. — Dans un arrêt du 8 avril 2003, la cour du travail de Bruxelles s'appuie sur la loi du 8 décembre 1992 pour considérer un contrôle comme étant irrégulier[58]. L'employeur faisait valoir que c'était tout à fait fortuitement, lors d'une intervention technique à la suite d'un encombrement du réseau, qu'il avait mis en évidence une consultation anormalement élevée de sites internet dans le chef d'un travailleur. La cour fit remarquer qu'à partir du moment où les données de connexion à l'internet avait été mises en évidence, à quelque occasion que ce soit, l'analyse des données s'assimilait à un traitement de données à caractère personnel et qu'en l'absence d'information préalable, ce traitement était irrégulier[59]. Dans le même sens, le tribunal du travail d'Audenarde conclut, dans une décision du 3 février 2009, au non-respect de la C.C.T. n° 81 du fait de l'absence de preuve d'une information préalable concernant tant les règles d'utilisation de ces outils de travail, que les modalités de contrôles effectués par l'employeur[60].

Il a également été jugé que le simple fait que la messagerie électronique du travailleur soit accessible à l'employeur ne permet pas de considérer que le contrôle répond à la condition de transparence qui requiert, aux termes de la C.C.T. n° 81, une véritable information dans le chef de l'employeur quant aux finalités de contrôle[61].

---

(47) C.T. Bruxelles, 3e ch., 8 avril 2003, *Chr. D.S.*, 2005, p. 208.
(48) C.T. Bruxelles, 3e ch., 13 septembre 2005, *Computerr.* 2006, p. 100.
(49) Gand, 12e ch., réf., 16 juin 2004, *Chr. D.S.*, 2005, p. 48.
(50) C.T. Anvers, sect. Anvers, 15 décembre 2004, *Chr. D.S.*, 2006, p. 146.
(51) Remplacé entre-temps par l'article 124 de la loi du 13 juin 2005 relatives aux communications électroniques.
(52) C.T. Bruxelles, 8 avril 2003, *Chr. D.S.*, 2005, p. 208; T.T. Liège, 10e ch., 24 février 2005, R.G. n° 327.207, inédit.
(53) C.T. Bruxelles, 14 décembre 2004, *Computerr.* 2005, p. 313; C.T. Bruxelles, 13 septembre 2005, *Computerr.* 2006, p. 100; C.T. Anvers, sect. Hasselt, 2e ch., 15 novembre 2005, R.G. n° 2004-0348, www.juridat.be.
(54) T.T. Bruxelles, 3e ch., 16 septembre 2004, *J.T.T.*, 2005, p. 61.
(55) Voy. les articles 124 et 125 de la loi du 13 juin 2005 sur les communications électroniques, articles 314*bis* et 259*bis* du Code pénal.
(56) T.T. Liège, 10e ch., 24 février 2005, R.G. n° 327.207, inédit.
(57) R. De Baerdemaeker et M. Kokot, « Protection de la vie privée et contrat de travail », *J.T.T.*, 2006, pp. 1-13; K. Rosier, « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail », *R.D.T.I.*, 2009, n° 35, pp. 126-140; K. Rosier, « Usage des technologies de l'information et de la communication dans les relations de travail et droit au respect de la vie privée », *R.D.T.I.*, 2012, n° 48-49, pp. 127-145. Voy. la recommandation n° 8/2012 de la Commission de la protection de la vie privée relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail, www.privacycommission.be.
(58) C.T. Bruxelles, 8 avril 2003, *Chr. D.S.*, 2005, p. 208.
(59) Dans le même sens : C.T. Bruxelles, 13 septembre 2005, *Computerr.*, 2006, p. 100; C.T. Mons, 8e ch., 8 décembre 2010, *J.L.M.B.*, 2011, p. 715; *Chr. D.S.*, 2011, p. 399, note O. Rijckaert.
(60) T.T. Audernarde, 1re ch., 3 février 2009, *Chr.D.S.*, 2010, p. 396. Voy. également l'arrêt de la cour du travail d'Anvers qui stigmatise l'absence d'information collective et individuelle concernant l'existence et les modalité d'une procédure de contrôle qui trouvent à s'appliquer même dans une entreprise de petite taille (C.T. Anvers, sect. Hasselt, 2e ch., 15 novembre 2005, R.G. n° 2004-0348, www.juridat.be.
(61) C.T. Mons, 8e ch., 8 décembre 2010, *J.L.M.B.*, 2011, p. 715; *Chr. D.S.*, 2011, p. 399, note O. Rijckaert.

J.T. n° 6571 - 27/2014
Larcier 08/07/2014 Groupe Larcier
F.U.N.D.P. /

Dans un arrêt du 25 novembre 2009 de la cour du travail de Mons[62], c'est la question de l'absence de déclaration préalable à la Commission de la protection de la vie privée qui est soulevée. La cour estime que cette absence ne permet pas de rejeter les données collectées, dès lors que la loi du 8 décembre 1992 ne prévoirait aucune sanction à l'absence de déclaration[63].

14. Principe de finalité. — Le contrôle doit poursuivre une finalité légitime. La C.C.T. n° 81 limite ces finalités à quatre finalités décrites à l'article 5 de la C.C.T.[64]. La cour du travail d'Anvers examine la légalité d'un contrôle des courriels d'une travailleuse au regard de ces finalités et précise que la finalité relative à la prévention de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui n'est applicable que pour la prévention de comportements *actifs* dans le chef du travailleur[65]. En l'espèce, la travailleuse avait reçu des courriers non sollicités faisant la promotion de médicaments pour l'amélioration des performances sexuelles. La cour constatant qu'il n'était pas démontré que, s'agissant typiquement de *spam*, la réception de ces courriels s'expliquait par la consultation de sites dont le contenu serait contraire aux bonnes mœurs, a considéré que l'employeur ne pouvait se prévaloir de cette finalité pour justifier le contrôle opéré.

Dans un cas d'espèce soumis à la cour du travail de Mons[66], l'employeur avait, à la suite de la découverte fortuite d'un courriel suspect, procédé à un contrôle systématique des courriels qui avaient été échangés par le travailleur sur une période de plusieurs mois. L'employeur avait pris connaissance de manière fortuite d'un courriel auquel était annexé un cahier des charges relevant de la sphère d'activités de l'entreprise. Il avait alors nourri des soupçons quant à un manque de loyauté de son travailleur et à l'exercice d'une activité concurrente ou parallèle. La question était de savoir si l'employeur pouvait, comme il l'avait fait, poursuivre sa recherche afin d'assurer la protection des intérêts économiques, commerciaux et financiers de l'entreprise. Dans un arrêt du 8 décembre 2010, la cour répond par l'affirmative en indiquant que, en ce qui concerne le contrôle du contenu des courriels subséquents, tenant compte des suspicions légitimes d'activités concurrentes ou parallèles, le principe général de finalité contenu notamment dans la loi du 8 décembre 1992 est respecté[67].

Dans un même ordre d'idées, la cour du travail de Liège a considéré que « lorsque l'employeur a connaissance, de quelque façon que ce soit, d'une possible attaque de son système par un virus, un ver, un cheval de Troie ou autre, ou d'une menace d'une telle attaque, il se trouve incontestablement dans une situation visée à l'article 4, 3°, précité qui l'autorise à procéder à un contrôle des données de communication ». En l'occurrence, l'employeur avait découvert un échange de messages entre deux travailleurs ayant accès à son système qui évoquaient la possibilité d'introduire un virus dans ledit système[68].

La cour du travail d'Anvers a quant à elle été amenée à se prononcer sur la régularité d'un contrôle poursuivant plusieurs finalités[69]. Un responsable du service informatique d'une entreprise avait repéré une utilisation suspecte des ressources informatiques de l'entreprise de par l'utilisation d'une connexion et un pare-feu nouvellement installé dans le chef de plusieurs travailleurs. Il s'agissait donc de vérifier le bon fonctionnement du réseau ce qui correspond à une finalité de contrôle expressément autorisée par l'article 5, § 1er, 3°, de la C.C.T. Il est apparu à ce responsable informatique, dans un second temps, que le trafic internet était particulièrement élevé pour un seul des travailleurs concernés, en l'occurrence l'employé licencié par la suite. La cour relève qu'un contrôle visant à vérifier le respect du règlement informatique de l'entreprise — qui ne permettait qu'un usage exceptionnel de l'internet à des fins privées en dehors des périodes de pause — était également possible au regard de l'article 5, § 1er, 4°, de la C.C.T. et était prévu dans le règlement informatique. Dans le présent cas de figure, l'employeur n'avait pas respecté la phase d'alerte préalable exigée par la C.C.T. n° 81 uniquement lorsque le but du contrôle porte sur la vérification de respect des règles d'utilisation des outils de communications électroniques au sein de l'entreprise. La cour a estimé que, lorsque le contrôle poursuit à la fois une finalité de contrôle du respect d'un règlement interne sur l'usage de l'internet au sein de l'entreprise et une finalité de protection de la sécurité et du bon fonctionnement du système informatique de l'entreprise, il n'est pas nécessaire que l'employeur passe par une phase d'alerte avant d'individualiser les données.

15. Principe de proportionnalité. — La proportionnalité des contrôles a également retenu l'attention dans la jurisprudence recensée. Ce n'est en effet pas parce que la finalité poursuivie est considérée comme légitime que tout contrôle sera régulier. Encore faut-il que les opérations de traitement mises en œuvre soient proportionnées par rapport à la finalité poursuivie. Ainsi dans deux arrêts évoqués *supra* qui avaient conclu au respect du principe de finalité, la juridiction saisie a considéré que le contrôle n'avait pas été suffisamment ciblé par rapport à l'objectif poursuivi. Dans un arrêt du 8 décembre 2010[70], la cour du travail de Mons jugera le contrôle disproportionné, dans la mesure où il n'avait pas ciblé uniquement les courriels susceptibles de révéler des faits de concurrence déloyale qui correspondait à la finalité de contrôle. Pour la cour du travail d'Anvers (section de Hasselt) c'est le fait que la prise de connaissance du contenu des courriels adressés par une travailleuse incluait les courriers échangés en soirée pendant une période où cette dernière était en congé, alors que l'employeur devait raisonnablement s'attendre à ce que ces courriels aient un caractère privé qui l'a amenée à considérer le traitement disproportionné[71]. Dans un jugement du 3 février 2003, le tribunal du travail d'Audenarde relève quant à lui également le caractère disproportionné d'un contrôle en raison du fait qu'il était réalisé de manière systématique sur les PC des travailleurs, dans l'optique d'un suivi de rentabilité[72].

2. Contrôle par la géolocalisation du travailleur

16. Utilisation du GPS comme instrument de contrôle. — Nous ne relevons que peu de jurisprudence portant sur les conditions dans lesquelles l'employeur peut établir la régularité d'un licenciement en se fondant sur des données obtenues par la géolocalisation du travailleur.

La cour du travail de Bruxelles a eu à connaître, dans un arrêt du 18 novembre 2004[73], de l'utilisation du GPS qui équipait un taxi pour établir l'existence d'excès de vitesse constants et importants d'un travailleur. La cour estime qu'en vertu des articles 16 et 17 de la loi du 3 juillet 1978 et de l'existence du lien de subordination sous lequel le travailleur effectue son travail, l'entreprise doit être à même d'exercer un contrôle sur le travailleur et que l'utilisation d'un GPS pour localiser les taxis ne constituerait pas une atteinte à la vie privée du chauffeur puisqu'il ne s'agit pas de l'espionner... Dans le même sens, le tribunal du travail de Liège avait estimé que, dès lors que le travailleur savait que l'enregistrement de données GPS le concernant était possible et que cet enregistrement a été réalisé pour contrôler l'emploi du temps du travailleur pendant son travail, le recours à cet enregistrement répond aux conditions de finalité et de proportionnalité et ne constitue pas une violation de la vie privée du travailleur[74].

En revanche, dans un arrêt plus récent qui date du 14 octobre 2011, la cour du travail de Gand analyse plus en détail la problématique au regard du cadre légal applicable et parvient à une appréciation différente

(62) C.T. Mons, 8e ch., 25 novembre 2009, *R.D.T.I.*, 2010, p. 81, note K. Rosier.
(63) Signalons que l'absence de déclaration est passible de sanctions pénales en vertu de l'article 39, 7°, de la loi du 8 décembre 1992.
(64) 1. la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui; 2. la protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires; 3. la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise; 4. le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.
(65) C.T. Anvers, sect. Hasselt, 2e ch., 15 novembre 2005, R.G. n° 2004-0348, www.juridat.be.
(66) C.T. Mons, 8e ch., 8 décembre 2010, *J.L.M.B.*, 2011, p. 715; *Chr. D.S.*, 2011, p. 399, note O. Rijckaert.
(67) À propos d'un contrôle relatif à l'exercice d'une activité concurrente durant les heures de travail, voy. T.T. Gand, 1er septembre 2008, R.G. n° 175054/06, www.juridat.be.
(68) C.T. Liège, 5e ch., 20 mars 2006, R.G. n° 33.137/05, www.juridat.be.
(69) C.T. Anvers, sect. Hasselt, 2 septembre 2008, R.G. n° 2070230, inédit.
(70) C.T. Mons, 8e ch., 8 décembre 2010, *J.L.M.B.*, 2011, p. 715; *Chr. D.S.*, 2011, p. 399, note O. Rijckaert.
(71) C.T. Anvers, sect. Hasselt, 2e ch., 15 novembre 2005, R.G. n° 2004-0348, www.juridat.be.
(72) T.T. Audenarde, 1re ch., 3 février 2009, *Chr. D.S.*, 2010, p. 396.
(73) C.T. Bruxelles, 2e ch., 18 novembre 2004, *J.T.*, 2005, p. 145.
(74) T.T. Liège, 5e ch., 16 mai 2007, R.G. n° 358.538, www.cass.be.

J.T. n° 6571 - 27/2014 - Larcier Groupe Larcier F.U.N.D.P. /

et plus correcte, à notre sens, de la problématique[75]. Se prononçant dans un cas impliquant l'utilisation d'un système de traçage GPS installé dans le véhicule d'un représentant de commerce, la cour estime qu'un tel contrôle doit être conforme à l'article 8 de la C.E.D.H., à l'article 22 de la Constitution et aux dispositions de la loi du 8 décembre 1992.

La cour constate que, du point de vue de la légitimité du contrôle, la localisation d'un véhicule volé ou la surveillance d'un travailleur peuvent, le cas échéant, constituer des finalités légitimes de traitement des données de localisation du véhicule utilisé par le travailleur. Toutefois, en l'espèce, il n'avait pas été satisfait à l'obligation d'information préalable. La cour souligne en particulier à cet égard qu'une seule disposition du règlement de travail signalant la présence d'un système de géolocalisation dans le véhicule ne suffit pas à satisfaire à l'obligation d'information qui doit mentionner les finalités d'utilisation du système. Par ailleurs, la cour estime que les modalités de contrôle étaient disproportionnées en ce que la surveillance portait également sur les déplacements effectués en dehors des heures de travail.

C. Vidéosurveillance

17. Applicabilité de la loi du 8 décembre 1992. — La surveillance par caméra sur le lieu du travail a été réglée par convention collective de travail n° 68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail[76]. La loi du 8 décembre 1992 reste également applicable à la vidéosurveillance des travailleurs comme l'a rappelé le tribunal du travail de Liège dans un jugement du 10 mars 2005[77]. Il nous semble dès lors que c'est à tort que, dans l'arrêt *Manon* du 2 mars 2005, la Cour de cassation a considéré que « la vidéosurveillance d'une caisse enregistreuse ne comporte, lorsqu'elle se limite à celle-ci, aucun élément d'identification directe ou indirecte, au sens défini [à l'article 1er de la loi du 8 décembre 1992], de la personne qui l'emploie »[78]. Dans le cas d'espèce, cet enregistrement était produit pour établir qu'une employée avait détourné une partie de l'argent de la caisse. Cette employée faisait valoir que la vidéosurveillance avait été mise en place sans qu'elle en soit informée. Même si c'était vers la caisse enregistreuse qu'avait été dirigée la caméra, il nous paraît contradictoire que les images filmées puissent être produites pour prouver des actes imputés à une employée et, dans le même temps, qu'elles ne soient pas considérées comme des données à caractère personnel au motif qu'elles ne permettraient pas d'identifier l'auteur du comportement incriminé. On constatera d'ailleurs que dans un litige portant également sur la légalité de l'utilisation d'une caméra fixe installée dans un magasin et dirigée sur la caisse enregistreuse, le tribunal du travail de Liège a considéré que la C.C.T. n° 68 était pleinement applicable[79].

Les deux aspects de la vidéosurveillance qui sont davantage mis en exergue dans les décisions rendues en la matière ont trait à la transparence. Il s'agit de l'obligation d'information préalable et la déclaration à la Commission de la protection de la vie privée.

18. Information. — Concernant la portée des obligations d'information préalable prescrites à l'article 9, §§ 1er et 4, de la C.C.T, la cour du travail de Bruxelles relève qu'il ne suffit pas d'informer le conseil d'entreprise quant à la finalité des caméras utilisées par l'employeur; encore faut-il que l'employeur puisse démontrer qu'il avait informé le conseil d'entreprise du principe du placement des caméras *dès avant leur installation*[80]. Dans un jugement du 6 mars 2007, le tribunal du travail de Liège considérera que le simple fait que la présence d'une caméra soit visible pour les travailleurs ne suffit pas à pallier le défaut d'information préalable concernant les finalités et modalités de vidéosurveillance[81].

19. Déclaration de traitement. — Dans une décision concernant l'utilisation d'images de caméra installée dans une salle de jeu de casino, la cour du travail de Liège (section de Namur) constate que le personnel du casino était dûment informé de l'installation des caméras et considère que les images ainsi obtenues peuvent être utilisées comme mode de preuve, même si, en l'espèce, la déclaration de traitement concernant l'installation de ces caméras faite à la Commission de la protection de la vie privée n'avait pas été rectifiée pour signaler un changement de propriétaire du casino[82]. Elle ne sanctionne donc pas l'irrégularité liée à la déclaration de traitement, contrairement au tribunal du travail de Liège, qui dans un jugement du 10 mars 2005 a conclu à l'irrégularité de la preuve d'un vol rapportée par la production d'un enregistrement vidéo alors que le traitement n'avait pas été déclaré à la Commission de la protection de la vie privée, comme pourtant requis par l'article 17 de la loi du 8 décembre 1992[83].

D. Contrôle du disque dur

20. Information préalable. — Dans un arrêt du 8 décembre 2010, la cour du travail de Mons a considéré que la loi du 8 décembre 1992 s'applique bel et bien au contrôle du disque dur d'un ordinateur et exige l'intervention d'une information préalable conformément à l'article 9 de la loi du 8 décembre 1992[84].

E. Sanctions en cas de non-respect de la loi du 8 décembre 1992

20*bis*. — Dans le cadre des décisions analysées, on constate que le non-respect de la loi du 8 décembre 1992 ou des C.C.T. qui en concrétisent les principes est sanctionné au niveau de la recevabilité de la preuve ou par l'octroi de dommage et intérêts destinés à réparer le préjudice lié au non-respect du droit au respect de la vie privée du travailleur.

21. Incidence sur la recevabilité des preuves. — Si, de longue date, la jurisprudence considérait que la preuve obtenue en violation des règles de droit, en ce inclus le droit au respect de la vie privée, devait être écartée des débats, tout comme les aveux obtenus à la suite de moyens de preuves illégaux, cette solution est remise en cause par la jurisprudence *Antigone* de la Cour de cassation. Aux termes de cette jurisprudence[85], sauf si la loi prévoit expressément le contraire, le juge doit examiner l'admissibilité d'une preuve illicitement recueillie à la lumière des articles 6 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et 14 du Pacte international relatif aux droits civils et politiques en tenant compte de tous les éléments de la cause, y compris de la manière suivant laquelle la preuve a été recueillie et des circonstances dans lesquelles l'irrégularité a été commise. Dans ces conditions, le juge ne peut écarter la preuve que si l'irrégularité entache la fiabilité de la preuve ou si elle conduit à une méconnaissance des principes relatifs au procès équitable, sauf lorsque la preuve a été obtenue en violation d'une règle de forme prescrite à peine de nullité. Dans un arrêt du 23 mars 2010, la Cour indique que les preuves ne peuvent être écartées que si elles répondent aux « critères *Antigone* » qui permettent d'exclure ces éléments de preuve[86].

(75) C.T. Gand, 14 octobre 2011, *J.T.T.*, 2012, p. 190; *Ors.*, 2012, reflet I. Plets, livr.r 2, p. 32; *Or.*, 2012, reflet I. Plets, livr. 2, p. 6.
(76) Convention collective de travail n° 68 conclue le 16 juin 1998 au sein du Conseil national du travail, relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail rendue obligatoire par arrêté royal du 20 septembre 1998.
(77) T.T. Liège, 10e ch., 10 mars 2005, R.G. n° 330.744, inédit. Pour une autre application de la loi du 8 décembre 1992 dans un cas de vidéosurveillance, voy. C.T. Anvers, sect. Hasselt, 6 janvier 2003, *R.W.*, 2003-2004, p. 300; *Chr. D.S.*, 2003, p. 19.
(78) Cass., 2 mars 2005, *J.T.*, 2005, p. 211, conclusions de l'avocat général D.Vandeermeersch; *J.L.M.B.*, 2005, p. 1086, note M.-A. Beernaert.
(79) T.T. Liège, 3e ch., 6 mars 2007, *R.R.D.*, 2007, p. 498, note K. Rosier et S. Gilson; *J.L.M.B.*, 2008, p. 389.
(80) C.T. Bruxelles, 2e ch., 15 juin 2006, *J.T.T.*, 2006, p. 392, note.
(81) T.T. Liège, 3e ch., 6 mars 2007, *R.R.D.*, 2007, p. 498, note K. Rosier et S. Gilson; *J.L.M.B.*, 2008, p. 389.
(82) C.T. Liège, sect. Namur, 13e ch., 8 mars 2011, *Chr. D.S.*, 08/2011, p. 404, note. Pour un commentaire, voy. K. Rosier, « Preuves illicites et écartement de la preuve : qui doit prouver quoi? », *in Bulletin social et juridique*, 2011, n° 454, p. 6.
(83) T.T. Liège, 10e ch., 10 mars 2005, R.G. n° 330.744, inédit. Pour une autre application de la loi du 8 décembre 1992 dans un cas de vidéosurveillance, voy. : C.T. Anvers, sect. Hasselt, 6 janvier 2003, *R.W.*, 2003-2004, p. 300; *Chr. D.S.*, 2003, p. 19.
(84) C.T. Mons, 8e ch., 8 décembre 2010, *J.L.M.B.*, 2011, p. 715; *Chr. D.S.*, 2011, p. 399, note O. Rijckaert. Pour d'autres décisions à propos du contrôle du PC ou d'un CD-ROM procédant à une analyse sur pied de l'article 87 de la C.E.D.H. voy. : C.T. Liège, 9e ch., 20 septembre 2010, R.G. n° 2007/AL/34.907, www.cass.be; *Ors.*, n° 9, 2010, note B. Paternostre, p. 27; *J.L.M.B.*, 40/2010, p. 1899; C.T. Bruxelles, 4e ch., 3 mai 2006, *J.T.T.*, 2006, p. 262.
(85) En référence à l'arrêt suivant : Cass., 2e ch., 14 octobre 2003, R.G. n° P.03.0762.N, www.cass.be, concl. av. gén. De Swaef.
(86) Cass., 2e ch., 23 mars 2010, R.G. n° P.10.0474.N/5, www.cass.be.

Dans un premier temps, les juridictions sociales se sont majoritairement abstenues d'appliquer cette jurisprudence rendue en matière pénale[87]. À la suite de l'arrêt du 10 mars 2008 de la Cour de cassation[88] rendu dans un litige opposant l'O.N.Em. à un chômeur et qui fait application de la jurisprudence dite *Antigone*, on constate une application de plus en plus répandue cette jurisprudence dans les litiges sociaux[89]. Nous avons toutefois relevé quelques décisions qui n'ont pas fait application de cette jurisprudence[90]. La conséquence de l'application plus systématique de la jurisprudence *Antigone* se traduit par une prise en compte de preuves obtenues illicitement, même si certaines décisions écartent la preuve en raison de l'absence de fiabilité de celle-ci[91] ou du non-respect du droit à un procès équitable après application d'une balance des intérêts entre les droits et intérêts en jeu[92]. Ces conséquences de la jurisprudence *Antigone* sont transposables en cas de preuve obtenues en violation de la loi du 8 décembre 1992.

22. Sanction indépendante de la recevabilité de la preuve. — Indépendamment de la sanction de l'écartement des débats de la preuve illicitement recueillie, certaines décisions condamnent l'employeur au paiement de dommages et intérêts pour le préjudice résultant de la violation du droit au respect de sa vie privée.

Dans un jugement du 6 mars 2007[93], le tribunal du travail de Liège a considéré que l'employeur, en obtenant des images de façon irrégulière, a manqué au principe de la loyauté dans le cadre de l'exécution de contrat de travail. Il condamne l'employeur à des dommages et intérêts en se fondant sur un manquement à l'article 16 de la loi sur le contrat de travail ainsi sur l'existence d'une faute au sens de l'article 1382 du Code civil. Ce faisant, le tribunal épingle le recueil de la preuve par caméra de manière irrégulière comme constituant un comportement fautif réalisé au cours du processus ayant abouti au licenciement. Il qualifie ce comportement de « faute dans l'exercice du droit de licencier au sens large ». Le tribunal juge également que la travailleuse démontre avoir subi un dommage du fait de ce comportement fautif, dommage consistant en une atteinte à sa vie privée.

La cour du travail de Liège avait également octroyé des dommages et intérêts en raison de la production de courriers électroniques dont l'employeur avait irrégulièrement pris connaissance[94]. La cour considéra que la prise de connaissance irrégulière de courriers électroniques ainsi que le fait de les imprimer et de les produire en justice relèvent d'une défense en justice abusive et estime que l'écartement de cette pièce ne suffit pas à réparer le dommage et octroie à la travailleuse des dommages et intérêts.

Dans un arrêt du 8 décembre 2010, la cour du travail de Mons constate une violation des règles applicables en matière de contrôles des courriels du travailleur, n'écarte pas la preuve en s'appuyant à cet égard sur la jurisprudence *Antigone,* mais condamne l'employeur au paiement d'un montant de 1.500 EUR pour avoir consulté tous les courriels échangés par le travailleur sur une période de six mois, et ce sur la base des articles 1382 du Code civil et 16 de la loi du 3 juillet 1978 imposant un devoir de loyauté et de respect mutuel[95].

On relèvera encore une décision qui condamne l'employeur au paiement d'un montant de 500 EUR pour avoir opéré une surveillance irrégulière du travailleur par le biais d'un système GPS[96].

3 La vie privée, les technologies et le domaine de la santé[97]

23. Catégorie de données sensibles. — La loi du 8 décembre 1992 distingue plusieurs catégories de données dont le traitement a des bases de légitimation différentes.

Les données reprises dans la première catégorie sont celles que nous qualifierons de « classiques » dès lors qu'elles ne sont pas susceptibles *in se* de porter atteinte aux libertés fondamentales ou à la vie privée. Il s'agit d'une catégorie « par défaut », car on y retrouve toutes les données qui ne sont pas visées par l'autre. On a coutume de considérer que les nom, prénom, adresse... font partie de cette première catégorie.

Nous devons relever que le principe de traitement concernant cette première catégorie est celui d'autorisation via l'article 5, f, de la loi qui prescrit que le traitement de données à caractère personnel peut être effectué « lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi ». Cela revient à dire que le traitement est autorisé au terme d'une mise en balance effectuée par le responsable de traitement entre ses intérêts à traiter les données et l'intérêt ou les droits et libertés fondamentaux de la personne concernée. En cas de litige porté devant lui par une personne concernée qui estimerait avoir été victime d'un traitement basé sur cet article, le juge devra procéder lui-même à cette analyse de balance. Il s'agira alors d'un contrôle *a posteriori*.

C'est à cette analyse *a posteriori* que la cour d'appel de Liège a procédé, dans le cadre d'un dossier de promotion et de prospection commerciale, pour considérer que « s'il peut être admis que les finalités de promotion et de prospection commerciale sont légitimes, elles sont néanmoins primées par les droits fondamentaux de la personne concernée, dont le droit à la protection de sa vie privée »[98]. Si cette analyse *a posteriori* n'est pas confortable pour le responsable de traitement, le législateur — tant européen que belge — a considéré qu'il s'agissait du seul moyen permettant de protéger les intérêts et droits fondamentaux de la personne concernée tout en permettant au responsable de traitement d'exercer son activité.

Le deuxième type de catégories concerne les données que l'on qualifiera de sensibles et dont le traitement est prévu aux articles 6, 7 et 8 de la loi du 8 décembre 1992 Ces articles mettent en place un régime d'interdiction de traitement compte tenu du fait que les données visées

(87) T.T. Liège, 3e ch., 6 mars 2007, *R.R.D.*, 2007, p. 498, note K. Rosier et S. Gilson; *J.L.M.B.*, 2008, p. 389; C.T. Bruxelles, 2e ch., 15 juin 2006, *J.T.*, 2006, p. 492; C.T. Bruxelles, 3 mai 2006, *J.T.T.*, 2006, p. 262; T.T. Bruxelles, 3e ch., 16 mars 2006, inédit cité par F. Gillet, « Une preuve obtenue en violation des dispositions de la C.C.T. no 68 est illicite, de même que l'aveu obtenu sur cette base », www.hrttoday.be; C.T. Bruxelles, 14 décembre 2004, *Computerr.*, 2005, p. 313; T.T. Nivelles, 1re ch., 8 février 2002, *J.T.T.*, 2002, p.181; T.T. Liège, 3e ch., 19 mars 2008, R.G. no 360.454, www.cass.be.

(88) Cass., 10 mars 2008, *J.L.M.B.*, 2009, p. 580, note R. De Baerdemaeker.

(89) C.T. Mons, 2e ch., 14 septembre 2009, *R.R.D.*, 2008, p. 555; C.T. Gand, sect. Bruges, 2e ch., 28 juin 2010, *J.T.T.*, 2011, p. 366; C.T. Liège, 9e ch., 20 septembre 2010, R.G. no 2007/AL/34.907, www.cass.be; *Orientations*, no 9, 2010, note B. Paternostre, p. 27; *J.L.M.B.*, 40/2010, p. 1899; C.T. Liège, sect. Namur, 13e ch., 8 mars 2011, *Chr. D.S.*, 08/2011, p. 404, note C.T. Bruxelles, 6e ch., 2 mai 2011, R.G. no 2009/AB/52260, inédit; Dans un arrêt du 8 décembre 2010, la cour du travail de Mons mentionne expressément que « les enseignements issus de cet arrêt du 10 mars 2008 trouvent à s'appliquer dans le cadre d'un litige relatif à la rupture de relations contractuelles entre un travailleur et son employeur. Il n'y a en effet pas lieu de considérer que ces enseignements seraient limités au contentieux de la sécurité sociale » (C.T. Mons, 8e ch., 8 décembre 2010, *J.L.M.B.*, 2011, p. 715; *Chr. D.S.*, 2011, p. 399, note O. Rijckaert.

(90) C.T. Mons, 15 décembre 2008, *R.R.D.*, 2008, p. 237, note D. Mougenot; C.T. Bruxelles, 2e ch., 5 novembre 2009, R.G. no 2009/AB/52381, www.cass.be C.T. Bruxelles, 2e ch., 7 février 2013, *J.T.*, 2013, p. 262, note D. Mougenot. Pour une non-application de la jurisprudence dans un litige de concurrence déloyale relevant du droit commercial : Gand, 22 mars 2010, R.G. no 2008/AR/476, www.cass.be.

(91) T.T. Audenarde, 1re ch., 3 février 2009, *Chr. D.S.*, 2010, p. 396. Voy. également pour des arrêts concluant à l'absence de fiabilité de la preuve : Mons, 14e ch., 2 mars 2010, *J.T.*, no 6393, 2010, p. 296, note D. Mougenot (dans un litige mettant en cause la recevabilité d'un rapport établi par un détective) et C.T. Bruxelles, 6e ch., 2 mai 2011, R.G. no 2009/AB/52260, inédit (à propos de la preuve issue de la fouille d'une armoire vestiaire).

(92) C.T. Liège, sect. Namur, 14 décembre 2010, R.G. no 2009/AN/8.833, www.cass.be; C.T. Bruxelles, 28 mars 2012, R.G. no 2010/AB/1.176, inédit, commenté sur www.terralaboris.be.

(93) T.T. Liège, 3e ch., 6 mars 2007, *R.R.D.*, 2007, p. 498, note K. Rosier et S. Gilson; *J.L.M.B.*, 2008, p. 389.

(94) C.T. Liège, sect. Namur, 11 janvier 2007, *R.R.D.*, 2006, p. 488, note K. Rosier et S. Gilson.

(95) C.T. Mons, 8e ch., 8 décembre 2010, *J.L.M.B.*, 2011, p. 715; *Chr. D.S.*, 2011, p. 399, note O. Rijckaert.

(96) C.T. Gand, 14 octobre 2011, *J.T.T.*, 2012, p. 190; *Ors.*, 2012 (reflet I. Plets), livr. 2, p. 32; *Or.*, 2012 (reflet I. Plets), livr. 2, p. 6.

(97) Cette partie est rédigée par Jean-Marc Van Gyseghem.

(98) Liège, 7e ch., 19 novembre 2009, *D.A. O.R.*, p. 455.

J.T. n° 6521 - 27/2014
Larcier 2014 Groupe Larcier
F.U.N.D.P. /

sont susceptibles *in se* de porter atteinte aux libertés fondamentales ou à la vie privée.

Le législateur européen a ainsi considéré que « les données qui sont susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée ne devraient pas faire l'objet d'un traitement, sauf consentement explicite de la personne concernée; que, cependant, des dérogations à cette interdiction doivent être expressément prévues pour répondre à des besoins spécifiques, en particulier lorsque le traitement de ces données est mis en œuvre à certaines fins relatives à la santé par des personnes soumises à une obligation de secret professionnel ou pour la réalisation d'activités légitimes par certaines associations ou fondations dont l'objet est de permettre l'exercice de libertés fondamentales »[99].

Dans le cadre de la présente chronique, nous nous attacherons uniquement à développer les questions liées aux données relatives à la santé, soit les traitements visés par l'article 7 de la loi du 8 décembre 1992 et le régime de l'interdiction confirmé par le tribunal du travail de Bruxelles qui a considéré que « la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel *interdit le traitement de données relatives à la santé*, sauf s'il est nécessaire pour exécuter les obligations et droits spécifiques du responsable du traitement en matière de droit du travail, et uniquement sous la responsabilité d'un professionnel des soins de santé »[100].

La Commission de la protection de la vie privée belge[101] a confirmé, dans un avis du 18 mars 2009, que « les données à caractère personnel relatives à la santé, au sens de l'article 7 de la loi du 8 décembre 1992, qui sont soumises à un niveau de protection plus élevé en raison de leur caractère sensible »[102]. Par ailleurs, elle a également rappelé, à maintes reprises que la loi du 8 décembre 1992 « prévoit une protection particulière pour les données à caractère personnel relatives à la santé. Le traitement de telles données est en principe interdit (article 7 de la loi du 8 décembre 1992). L'article 7, § 2, de la loi du 8 décembre 1992 énumère les cas où un tel traitement est quand même permis »[103].

24. Nécessité d'une autorisation de traitement. — Le législateur belge a poursuivi la logique du régime d'interdiction de traitement de ces données en soumettant ces traitements à autorisation alors qu'une simple notification est habituellement de mise.

Ainsi, toute communication de données relatives à la santé doit faire l'objet d'une autorisation par le comité sectoriel de la sécurité sociale et de la santé, section santé, à l'exception :

— de communications entre professionnels des soins de santé dans le cadre d'un traitement;

— de communications par ou en vertu de la loi, après avis de la Commission de protection de la vie privée;

— de communications relevant de la compétence de la section sécurité sociale du comité sectoriel de la sécurité sociale et de la santé;

— de communications dispensées d'autorisation par le Roi, après avis de la Commission de protection de la vie privée[104].

Pour chaque demande d'autorisation, le comité sectoriel effectue une analyse sous l'angle de la licéité du traitement, de sa finalité, de la proportionnalité, de la transparence et des mesures de sécurité.

Dans le cadre de sa compétence d'autorisation, il a eu l'occasion de rappeler et de préciser que « les données à caractère personnel relatives à la santé peuvent uniquement être traitées sous la surveillance et la responsabilité d'un professionnel des soins de santé. Même si cela n'est pas strictement requis dans la loi relative à la vie privée, le comité sectoriel estime qu'il est préférable que de telles données soient traitées sous la responsabilité d'un médecin »[105]. La jurisprudence du comité est donc plus stricte que la loi qu'elle est censée appliquer et l'on est en droit de se poser la question de la légitimité d'une telle exigence. En effet, la loi du 8 décembre 1992 parle de professionnel des soins de santé[106] qui est une notion plus large que celle de médecin. En vertu de quelle compétence, le comité sectoriel réduit cette notion de professionnel de soins de santé aux seuls médecins?

Le comité sectoriel a également une compétence d'avis par rapport à la désignation des conseillers en sécurité au sein des hôpitaux belges[107] [108].

25. Notion de données à caractère personnel relatives à la santé. — Au niveau de la notion de données à caractère personnel relatives à la santé, la Cour de justice de l'Union européenne — et ce sera la seule référence à une juridiction internationale dans le cadre de cette chronique consacrée à la jurisprudence belge[109] — a considéré, au sujet de données à caractère personnel relatives à la santé, qu'« il convient de donner à l'expression "données relatives à la santé" employée à son article 8, § 1er [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], une interprétation large de sorte qu'elle comprenne des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne » et que « l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, § 1er, de la directive 95/46 »[110].

Cette interprétation large a été reprise par le Conseil d'État dans un arrêt du 27 octobre 2005 qui a précisé qu'« un test d'haleine, *impliquant le traitement de données de santé*, ne peut être exécuté que moyennant le consentement écrit de l'agent qui y est soumis et ne peut être réalisé que par un professionnel des soins de santé qui est tenu au secret y compris vis-à-vis de l'autorité, laquelle est seulement autorisée à savoir si l'agent est apte ou non à exercer ses fonctions. La sanction disciplinaire fondée sur un test d'haleine qui ne respecte pas ces principes est irrégulière. Il est utile d'attirer l'attention du lecteur sur le fait que le consentement de la personne concernée est un reflet du principe d'autodétermination de l'individu, mais n'est pas la seule base de légitimation prévue par la loi.

26. Proportionnalité. — La notion de proportionnalité doit s'analyser à divers niveaux, y compris celui de la communication. En effet, et quand bien même il y aurait une obligation de transmettre des données à caractère personnel — et encore plus en ce qui concerne celles relatives à la santé — cette communication doit se limiter à ce qui est nécessaire. La justice de paix de Bruges a ainsi eu l'occasion de préciser que « la communication d'un jugement de mise en observation à la Commission des jeux de hasard est contraire aux articles 2 et 5 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. Une communication partielle peut être accordée »[111].

La C.P.V.P. attire également l'attention sur ce principe de proportionnalité. À titre d'exemple, nous pouvons citer son avis concernant un avant-projet de décret flamand en matière de prévention et de la lutte contre le dopage dans le sport dans lequel elle a relevé et précisé que « l'avant-projet contient également une disposition selon laquelle l'O.N.A.D. peut contraindre tout sportif qui n'est pas un sportif d'élite "dont les prestations présentent une amélioration soudaine et importante ou qui présente de sérieux indices de dopage" [traduction libre effectuée par le secrétariat de la Commission en l'absence de traduction officielle] à fournir ses données de localisation. Bien que l'on puisse comprendre que l'O.N.A.D. doive également disposer d'instru-

(99) Directive 95/46, considérant 33.
(100) T.T. Bruxelles, réf., 30 novembre 2006, *Chr. D.S.*, 2008, liv. 1, p. 24; nous soulignons.
(101) Ci-après, « C.P.V.P. ».
(102) C.P.V.P., avis n° F-20090318-3 (8/2009) du 18.03.2009.
(103) C.P.V.P., avis n° F-20130904-10 (38/2013), 4.09.2013, n° 35.
(104) Pour plus d'information, voir www.privacycommission.be/fr/node/7109.
(105) Délibération n° 14/024 du 18 mars 2014 relative à la communication de données à caractère personnel codées relatives à la santé par Kind en Gezin à l'université de Gand pour la réalisation d'une étude relative à l'influence de facteurs sociaux sur le développement du jeune enfant, www.ehealth.fgov.be/sites/default/files/assets/fr/pdf/sector_committee/2014/sector_committee_14-024-f049.pdf.
(106) Article 7, §4, de la loi du 8 décembre 1992.
(107) Les hôpitaux belges doivent désigner un conseiller en sécurité sur pied de l'arrêté royal du 23.10.1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre.
(108) Pour des exemples d'avis à ce sujet, voir www.privacycommission.be/fr/search/site/conseill%C3%A9%20en%20s%C3%A9curit%C3%A9?f[0]=im_field_source%3A49
(109) Pour plus de détails sur la jurisprudence européenne, voy. J.-M. Van Gyseghem, C. de Terwangne, J. Herveg et C. Gayrel, « Vie privée et protection des données à caractère personnel », *Journal européen des droits de l'homme*, 2014, pp. 54-87.
(110) C.J.U.E., 6 novembre 2003, *Lindqvist*, C-101/01, points 50 et s.
(111) J.P. Bruges, 31 décembre 2005, *T.G.R. - T.W.V.R.*, 2007, livr. 3, p. 169.

J.T. n° 6571 - 27/2014
Larcier - © Groupe Larcier
F.U.N.D.P. /

ments adaptés vis-à-vis de sportifs qui ne sont pas des sportifs d'élite afin de lutter contre le dopage, il est recommandé d'interpréter cette règle de façon stricte (l'exposé pourrait mettre l'accent sur ce point) afin d'éviter qu'elle soit appliquée de manière disproportionnée »[112].

Dans ce même avis, elle a rappelé que « la communication doit en effet s'organiser de la façon la plus restrictive possible. Dans sa formulation actuelle, l'avant-projet semble plutôt se rapprocher d'une publication de sanctions sur internet, réprouvée par le Groupe 29 et par la Commission »[113].

27. Information. — En matière de données à caractère personnel relatives à la santé, l'information délivrée à la personne concernée ne se limite pas à ce qui est prévu à l'article 9 de la loi du 8 décembre 1992 dès lors qu'elle doit être complétée par les éléments prescrits par 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[114]. La C.P.V.P. a déjà eu l'occasion de le préciser en attirant l'attention sur le fait que « l'information, [en cas de traitement de données à caractère personnel relative à la santé], ne doit pas uniquement mentionner les éléments repris à l'article 9, § 1er, de la loi du 8 décembre 1992, mais qu'il faut également tenir compte des articles 25, 4°, et 26 de l'arrêté royal du 13 février 2001, étant donné que le traitement concerne des données de santé »[115].

28. Droit d'accès. — En matière de droit d'accès, l'article 10, alinéas 2 et 3, de la loi du 8 décembre 1992 prévoit un régime particulier dès lors que toute « personne a le droit, soit directement, soit avec l'aide d'un patricien professionnel en soins de santé, de prendre connaissance des données à caractère personnel traitées en ce qui concerne sa santé »[116] et 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* »[117] sans préjudice de l'article 9, § 2, de la loi du 22 août 2002 relative aux droits du patient. Le tribunal du travail de Louvain a considéré dans le cas d'un indépendant qui souhaitait avoir accès à son dossier médical auprès de sa mutuelle en se fondant sur l'article 10 de la loi que « dans cet article, le législateur stipule en effet expressément que toute personne a le droit, soit directement, soit 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 »[118] et que « le tribunal souscrit au point de vue que la loi précitée est d'application à la médecine de contrôle et d'expertise. Par conséquent, le tribunal estime en l'espèce que cette loi est d'application et attribue donc au demandeur le droit de consultation demandé »[119]. À noter qu'en appel, la cour du travail de Bruxelles a confirmé ce jugement en précisant que le plaignant avait un droit d'accès tant sur la base de la loi du 8 décembre 1992 que sur celle de la loi du 22 août 2002 relative aux droits du patient[120 121].

Par ailleurs, la loi du 8 décembre 1992 permet également de suppléer la loi du 22 août 2002 relative aux droits du patient. En effet, et dans certaines hypothèses, cette loi peut se révéler inefficace pour permettre à une personne d'accéder à ses données médicales, tandis que l'article 10 de la loi du 8 décembre 1992 lui donnera la base légale à un tel accès. Ainsi en a jugé la cour d'appel d'Anvers dans un arrêt du 17 mars 2010[122].

À noter que le contraire vaut également, comme le précise le tribunal de première instance de Bruxelles, dans son jugement du 25 mars 2005. Celui-ci se prononce en ces termes :

« Jusqu'à l'entrée en vigueur de la loi du 22 août 2002 relative aux droits du patient, il n'existait aucune disposition légale autorisant les héritiers d'un défunt à obtenir la levée du secret médical après le décès afin de consulter, même par la voie d'un médecin-conseil de leur choix, le dossier médical de la personne décédée.

» Les héritiers devaient être considérés comme des tiers, au sens de l'article 7 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, de sorte qu'ils ne pouvaient se voir communiquer des données à caractère personnel du défunt. L'article 10 de la même loi n'autorise que la personne concernée à demander, de son vivant, l'accès à son dossier médical.

» En vertu de l'article 9, paragraphe 4, de la nouvelle loi du 22 août 2002, un droit de consultation du dossier médical du patient décédé n'est accordé aux proches que pour autant que leur demande soit suffisamment motivée et spécifiée et que le patient ne s'y soit opposé expressément »[123].

29. Sécurité/confidentialité. — La qualification d'une donnée à donnée à caractère personnel relative à la santé a également un impact au niveau de la sécurité et de la confidentialité qui en est exigée. En effet, la loi vie privée prescrit, en son article 16, § 4, alinéa 2, que les mesures de sécurité « 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, d'autre part, de la nature des données à protéger et des risques potentiels ». Les données à caractère personnel relatives à la santé étant de nature sensible, les mesures de sécurité/confidentialité devront être au diapason.

Appliquant ce principe, le président du tribunal de commerce de Bruxelles a considéré, dans un arrêt du 16 juin 2003, que « la pratique d'une compagnie d'assurances qui consiste à joindre le questionnaire médical à la proposition d'assurance sans mettre en œuvre aucune technique de protection de la confidentialité des données, enfreint l'article 16, § 4, de la loi du 8 décembre 1992 relative à la protection de la vie privée et est contraire à l'article 94 L.P.C.C. »[124]. Il a de plus précisé que le fait pour le preneur de consentir au traitement de ses données à caractère personnel ne permet pas à la compagnie d'assurances de procéder à ce traitement « sans contrôle et sans responsabilité d'un médecin »[125] et que le preneur d'assurance « n'a pas pour autant renoncé à son droit au respect de la confidentialité de ces données médicales »[126].

La confidentialité telle qu'imposée par la loi privée ne peut cependant pas constituer un moyen pour un hôpital, ou toute personne pouvant s'en prévaloir, d'empêcher la bonne marche de la justice par rapport à un accident survenu en son sein. Le tribunal de première instance de Liège a ainsi précisé que « rien ne s'oppose à ce qu'il soit ordonné à l'hôpital, en application de l'article 877 du Code judiciaire, de déposer au dossier de la procédure la liste des personnes ayant été reçues en consultation à la polyclinique de cardiologie l'avant-midi [au cours duquel s'est produit l'accident]. Pareille liste ne porte pas atteinte au

(112) C.P.V.P., avis n° F-20110706-2 (13/2011), 6 juillet 2011, n° 7.
(113) C.P.V.P., avis n° F-20110706-2 (13/2011), 6 juillet 2011, n° 33.
(114) Lors du traitement de données à caractère personnel visées aux articles 6 à 8 de la loi, le responsable du traitement doit prendre les mesures supplémentaires suivantes :
1° les catégories de personnes, ayant accès aux données à caractère personnel, doivent être désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées;
2° la liste des catégories des personnes ainsi désignées doit être tenue à la disposition de la Commission par le responsable du traitement ou, le cas échéant, par le sous-traitant;
3° il doit veiller à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées;
4° lorsque l'information, due en vertu de l'article 9 de la loi, est communiquée à la personne concernée ou lors de la déclaration visée à l'article 17, § 1er, de la loi, le responsable du traitement doit mentionner la base légale ou réglementaire autorisant le traitement de données à caractère personnel visées aux articles 6 à 8 de la loi.
(115) C.P.V.P., avis n° F-20080227-14 (09/2008), 27.02.2008, n° 41.
(116) Article 10, § 2, alinéa 1er, de la loi du 8 décembre 1992.
(117) Article 10, § 2, alinéa 2, de la loi du 8 décembre 1992; c'est nous qui soulignons.
(118) T.T. Louvain, 22 janvier 2008, *Rev. dr. santé*, 2010-11, livr. 4, p. 333.
(119) T.T. Louvain, 22 janvier 2008, *Rev. dr. santé*, 2010-11, livr. 4, p. 333.
(120) C.T. Bruxelles, 5 mars 2009, *Rev. dr. santé*, 2010-11, livr. 4, p. 336.
(121) Au sujet de la notion de dossier médical au sens de la loi du 22 août 2002 relative aux droits du patient, voy. R. Saelens et P. De Hert, « La loi relative aux droits du patient et le traitement des données relatives à la santé », *Vie privée et données à caractère personnel*, Politea, note infrapaginale 498 de J.-M. Van Gyseghem.
(122) Anvers, 17 mars 2010, *Rev. dr. santé*, 2011-12, livr. 1, p. 18,
(123) Civ. Bruxelles, 25 mars 2005, *J.L.M.B.*, 2006, livr. 27, p. 1197; voy. *contra* : Civ. Bruxelles, 23 avril 1999, *Rev. dr. santé*, 1999-2000, p. 353 qui a considéré que « les héritiers et ayants droit ne sont d'ailleurs pas des tiers au sens de l'article 7 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 dans la mesure où ils poursuivent la personnalité du défunt. Ces personnes doivent au contraire être assimilées à l'intéressé au sens de l'article 10, § 3, de cette loi ».
(124) Prés. Comm. Bruxelles, 16 juin 2003, *D.C.T.R.*, 2004, livr. 63, p. 88.
(125) *Idem*.
(126) *Idem*.

J.T. n° 6571 - 12/7/2014
Larcier © Groupe Larcier
F.U.N.D.P. /

secret médical et n'est pas contraire à la réglementation du traitement des données à caractère personnel, dès lors qu'il s'agit uniquement pour l'hôpital de communiquer la liste des personnes ayant rendez-vous, sans divulgation relative à leur état de santé, leur éventuel témoignage ultérieur étant uniquement relatif aux circonstances de la chute de la victime »[127]. Si la décision respecte les principes de limitation de l'ingérence et donc la proportionnalité que nous avons vue ci-dessus, il nous paraît cependant discutable, au regard de la jurisprudence européenne mentionnée précédemment, l'affirmation du tribunal selon laquelle le fait de savoir que telle personne se trouvait en rendez-vous à la polyclinique ne constitue pas une donnée relative à l'état de santé.

C Conclusions

Comme le laisse apparaître cette étude, le régime juridique de la protection de la vie privée et des données à caractère personnel est organisé par des lois multiples et éparses, entre lesquelles il peut s'avérer ardu de dégager une cohérence. De plus, ces règles sont jonchées de concepts souvent flous et peu connus, d'autant plus difficiles à comprendre que les technologies requièrent bien souvent, en amont, une bonne connaissance technique des outils utilisés.

Compte tenu de ces éléments, la compréhension et l'application du régime juridique de la protection de la vie privée et des données à caractère personnel sont complexes. Dans ce contexte, on ne saurait qu'insister sur l'importance du travail des avocats et des magistrats qui, par leurs actions et leurs décisions, mettent en lumière l'existence et l'importance de ces règles encore trop souvent méconnues, et des sanctions qu'entraîne le non-respect de ces normes. La jurisprudence ainsi créée constitue un précieux matériel pour aider le citoyen à comprendre la portée et l'intérêt des règles qui balisent le développement fulgurant des technologies dans notre société interconnectée.

Elise DEGRAVE[128]
Karen ROSIER[129]
et Jean-Marc VAN GYSEGHEM[130] [131]

(127) Civ. Liège, 13 mars 2012, *J.L.M.B.*, 2012 (sommaire), livr. 23, p. 1114.

(128) Elise Degrave est chargée de cours à la Faculté de droit de l'Université de Namur et chercheuse post-doctorante à la chaire E-gouvernement et au C.R.I.D.S.
(129) Karen Rosier est maître de conférences à la Faculté de droit de l'Université de Namur et chercheuse au C.R.I.D.S. ainsi qu'avocate.
(130) Jean-Marc Van Gyseghem est directeur de l'Unité de recherche « Libertés et société de l'information » du C.R.I.D.S. (www.crids.eu) et avocat au barreau de Bruxelles (www.rawlingsgiles.be).

(131) Le présent article ne reflète que les opinions personnelles des auteurs.

Jurisprudence

PRESCRIPTION LIBÉRATOIRE
- Actes interruptifs
- Citation (article 2244 C. civ.) Portée de l'effet interruptif
- Demande(s) virtuellement comprise(s)
- Fin de l'effet interruptif
- Rejet de la demande (article 2247, C. civ.)
- Application à la demande virtuellement comprise dans la citation
- Condition

Cass. (1re ch.), 11 avril 2014

Siég. : Ch. Storck (prés.), M. Regout, M. Lemal (rapp.), M.-Cl. Ernotte et S. Geubel.

Min. publ. : Th. Werquin (av. gén.).

Plaid. : MMes P.A. Foriers, P. Van Ommeslaghe et J. Verbist.

(P. e.a. c. BNP Paribas e.a.).

En cas de demande incidente dont l'objet est virtuellement compris dans la citation introductive de la demande principale, l'interruption de la prescription dont profite la demande incidente n'est regardée comme non avenue que si elle est elle-même définitivement rejetée, indépendamment du rejet de la demande princi-

(Extraits)

I. La procédure devant la Cour.

Le pourvoi en cassation est dirigé contre l'arrêt rendu le 5 janvier 2012 par la cour d'appel de Liège.

Le conseiller Michel Lemal a fait rapport.

L'avocat général Thierry Werquin a conclu.

II. Les moyens de cassation.

Les demandeurs présentent deux moyens libellés dans les termes suivants :

[...]

Second moyen.

Dispositions légales violées.

— articles 2244, 2247 et 2262*bis* du Code civil;

— articles 807, 808 et 1042 du Code judiciaire.

Décisions et motifs critiqués.

Après avoir rappelé, en substance, que « la demande nouvelle est la demande incidente par laquelle le demandeur étend ou modifie sa demande originaire »; qu'« alors que la demande additionnelle est celle qui, comme le définit l'article 808 du Code judiciaire, s'étend aux accessoires, la demande nouvelle s'en prend à l'objet ou à la cause de la demande principale pour l'étendre ou la modifier »; que, « comme toute demande, les demandes reconventionnelle et nouvelle doivent répondre aux conditions d'intérêt et de qualité prescrites aux articles 17 et 18 du Code judiciaire, qui doivent être réunies dans le chef du demandeur »; que « l'article 807 du Code judiciaire [...] comporte deux conditions de recevabilité : la première est celle des conclusions contradictoirement prises pour assurer le respect des droits de la défense; la seconde de ces conditions — dériver d'un fait ou d'un acte invoqué dans l'acte introductif — veut éviter toute surprise au défendeur en exigeant un lien précis avec la demande originaire »; que, « pour autant qu'il n'y ait pas lieu d'annuler l'acte introductif d'instance et que la demande originaire relevât de la compétence du juge saisi, le juge appelé à apprécier la demande modifiée ou étendue est tenu de statuer sur cette demande, sans devoir examiner la recevabilité et le fondement de la demande originaire (Cass., 21 juin 2010, R.G. no C.09.0067.N.) »,

et après avoir décidé qu'« en l'espèce, [les demandeurs] ont, par voie de conclusions déposées au greffe le 12 février 2010, demandé la condamnation [des défenderesses] à les indemniser de la perte des plus-values potentielles attendues des investissements effectués », qu'« il s'agit d'une demande nouvelle qui repose sur des faits invoqués en termes de citation; que [les demandeurs] fondent leur demande sur les comportements fautifs [des défenderesses] qui auraient provoqué la faillite de Neuroplanet et entraîné un préjudice important dans leur chef; que cette demande nouvelle a été introduite à un moment où la faillite de Neuroplanet était clôturée, celle-ci étant intervenue le 10 février 2004 »,

J.T. n° 6571 - 27/2014
Larcier - Groupe Larcier
F.U.N.D.P. /
page