Vie privée

Poullet, Yves

Published in:
Droit de l'informatique et des technologies de l'information : chroniques de jurisprudence 1995-2001

Publication date:
2003

Document Version
le PDF de l'éditeur

Chapitre 7

Vie privée[463]

Yves POULLET*

I. Introduction

143. – L'adoption de la loi du 8 décembre 1992 et sa mise en vigueur avaient justifié, dans la période couverte par la précédente chronique, quelques premières décisions venues compléter une jurisprudence hardie fondée tantôt sur le principe de non-discrimination ou directement sur l'article 8 de la Convention européenne des droits de l'homme.

La précédente chronique consacre l'essor d'une jurisprudence en la matière et illustre les difficultés d'interprétation d'une loi aux contours flous et à la lecture ingrate. La fin de la période est marquée d'un point de vue législatif par la modification de la loi de 1992 par la loi du 11 décembre 1998[464] transposant la directive européenne 95/46 du 24 octobre 1995[465]. Cette modification en vigueur depuis le 1er septembre 2001[466] est trop récente pour avoir déjà permis à la jurisprudence de s'y référer même si, comme nous le noterons[467], en particulier à propos des conditions de légitimité des traitements qui fixent le droit à l'information des responsables de traitement, la jurisprudence n'a pas hésité à anticiper.

144. – Le plan de ce chapitre suit celui déjà adopté dans notre précédente chronique :

---

* Doyen et professeur ordinaire à la Faculté de Droit de Namur, directeur du CRID (F.U.N.D.P.).

463 L'écriture du présent chapitre a été achevée le 1er mars 2002. Elle n'a pu tenir compte de la jurisprudence au delà du 1er janv. 2002.

464 *M.B.*, 3 févr. 1998. Cons. notamment Th. LÉONARD et Y. POULLET, «La protection des données à caractère personnel en pleine (r)évolution», *J.T.*, 1999, pp. 37 et s.; D. de BOT, *Verwerking van persoonsgegevens*, coll. Recht en Praktijk, n° 30, Antwerpen, Kluwer, 2001, n° 30.

465 Il s'agit de la Dir. 95/46/CE du 24 oct. 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données. Sur cette directive, lire M-H. BOULANGER, C. de TERWANGNE, Th. LÉONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, «La protection des données en droit communautaire», *J.T.D.E.*, 1997, pp. 121-127, pp. 145-155 et pp. 173-179.

466 Soit 6 mois après la publication de l'A.R. du 13 févr. 2001 (*M.B.*, 13 mars 2001, p. 7839). Sur cet A.R., voy. C. de TERWANGNE et S. LOUVEAUX, «Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal», *J.T.*, 2001, pp. 457-469.

467 *Infra*, nos 150 et s.

la première partie (A) concerne la réflexion jurisprudentielle relative au champ d'application de la directive. Plus particulièrement, les notions de base de «*données à caractère personnel*» et de «*traitement*» ont fait l'objet de décisions intéressantes;

la deuxième partie (B) envisage les conditions de légitimité des traitements de données à caractère personnel. Ce qui permet de préciser les limites du droit des entreprises, associations et administrations à traiter des données en général, des données sensibles en particulier;

enfin, la troisième partie (C) est consacrée aux obligations de transparence des traitements vis-à-vis des personnes concernées et aux divers droits de la personne concernée vis-à-vis de leurs données.

II. – Les notions de base de la loi

A. – La notion de «données à caractère personnel»

145. – La notion de données à caractère personnel n'est point évidente lorsque l'on s'interroge sur les critères qui permettront de considérer qu'une donnée permet d'identifier ou non la personne concernée. Le cas des «*données codées*»[468] en particulier a été au centre de la décision du Conseil d'Etat du 26 janvier 2000[469] relative au Résumé Psychiatrique Minimum.

L'affaire portée devant le Conseil par la Fédération belge des chambres syndicales des médecins concernait une demande d'annulation de l'arrêté royal du 25 février 1996 fixant les règles suivant lesquelles certaines données minimales psychiatriques doivent être communiquées au ministre qui a la Santé publique dans ses attributions[470]. En l'occurrence, l'arrêté visé obligeait les établissements psychiatriques à communiquer un certain nombre de données après avoir «*anonymisé*» celles-ci, conformément à ce qu'impose l'article 86 de la loi sur les hôpitaux du 7 août 1987.

Les requérants soutenaient que la seule absence de toute référence personnelle ou l'absence de mention du numéro d'identification ne pouvaient suffire pour que l'on puisse parler de données anonymes, comme requis par la loi sur les hôpitaux : «*La seule possibilité théorique d'identification est suffisante pour entacher la légalité de l'acte attaqué, sans qu'il soit besoin d'une démonstration s'appuyant sur des cas concrets ...*». A ce premier argument, fondé sur une possibilité *in abstracto* de réidentification par l'entremise de l'établissement psychiatrique qui a codé les données, les requérants ajoutent que «*le risque de réidentification est encore plus grand dans le cas du résumé psychiatrique minimum que dans le cas du résumé clinique minimum dans la mesure où il apparaît clairement des circulaires que l'on désire suivre le parcours complet des patients psychiatriques, que ceux-ci sont des unités beaucoup plus petites, qu'ils sont moins nombreux et par là même par définition plus facilement identifiables*».

Le Conseil d'Etat a suivi cette seconde interprétation de la notion de donnée personnelle en constatant que «*le 'résumé psychiatrique minimum' est de nature à porter atteinte à l'anonymat des personnes concernées imposé par l'article 86 de la loi sur les hôpitaux, par le nombre considérable et la nature des données à communiquer et en particulier par le recoupement possible des indications ...*».

146. – Il est intéressant de noter que la décision du Conseil d'Etat et les débats qui s'y sont tenus opposent implicitement deux conceptions de la donnée à caractère personnel. Ces conceptions sont toutes les deux présentes dans la nouvelle définition de la notion de donnée à caractère personnel telle qu'exprimée par la loi du 18 décembre 1998 transposant mot à mot celle de la directive 95/46 CE[471], à savoir : «*Toute information qui peut être identifiée directement ou indirectement, notamment par référence à un numéro d'identification ou un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, économique, culturelle ou sociale*».

La première conception étend la notion de donnée identifiable à toute donnée pour laquelle il existe un moyen raisonnable d'identifier les

[468] Par donnée codée, il faut entendre selon l'art. 1er, b, de l'A.R. du 13 mars 2001 (*M.B.*, 13 mars 2001). «*une donnée qui ne peut être mise en relation avec une personne identifiée ou identifiable que par l'intermédiaire d'un code*».

[469] C.E., 26 janv. 2000, arrêt n° 84880. *Rev. dr. santé*, 2000-2001, p. 285, avec note S. CALLENS.

[470] *Ibidem*. Cette décision devait obliger le gouvernement à proposer une modification de la loi sur les hôpitaux et à réintroduire, à partir de là, une version quelque peu modifiée de l'arrêté royal. La loi nouvelle et le projet d'arrêté royal ont fait depuis l'objet d'avis de la Commission de protection de la vie privée.

[471] Sur ce débat, voy. Th. LÉONARD et Y. POULLET, *op. cit.*, p. 38, n° 3, avec les réf. aux discussions lors de l'adoption de la loi belge.

personnes concernées, soit dans le chef du responsable du traitement, soit par un tiers[472].

Cette première conception défendue par les requérants semble devoir prévaloir.

On notera en effet que l'exposé des motifs[473] de la loi du 11 décembre 1998[474] aujourd'hui en vigueur, dispose que : «*dès lors qu'il existe un moyen raisonnable d'identifier les personnes concernées, soit dans le chef du responsable du traitement, soit même par un tiers, il s'agit de données à caractère personnel dont le traitement est susceptible d'être réglementé par la loi*».

Cet élargissement a permis à la Commission de protection des données de considérer dans un avis d'initiative récent[475] que les adresses IP sont des données à caractère personnel. En effet, il est toujours possible par l'intermédiaire des fournisseurs d'accès qui délivrent ces adresses IP, de retrouver l'identité des internautes. En l'occurrence, une société d'auteurs collectait sur Internet les adresses IP des internautes piratant des fichiers musicaux en format MP3. Elle contactait par ailleurs les fournisseurs d'accès pour que ces derniers, sans leur dévoiler les identités des abonnés titulaires des adresses IP, adressent de sévères mises en demeure aux internautes[476]. La Commission a estimé que les adresses IP constituaient des données personnelles dans le chef de la société d'auteur même si celle-ci, à aucun moment, ne disposait du nom de l'abonné se cachant derrière l'adresse IP.

La seconde conception retenue par le Conseil d'Etat, certes sous l'empire de l'ancienne loi, est plus restrictive. Elle analyse la notion de donnée à caractère personnel comme le résultat de l'addition d'un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale dans la mesure où cette addition permet, moyennant un effort raisonnable, au responsable d'identifier facilement la personne concernée par ses éléments même si les données ont été codées.

472 Sur le rôle joué par cette jurisprudence dans l'adoption de la loi organique du 30 nov. 1998 des services de renseignements et de sécurité (*M.B.*, 18 déc. 1998), voy. B. HAVELANGE et Y. POULLET, «Secret d'Etat et vie privée ou comment concilier l'inconciliable», in *Droit des Technologies de l'information : regards prospectifs* (E. MONTERO éd.), Cahier du CRID, n° 16, Bruxelles, Bruylant, 1999, pp. 236 et s.

473 Exposé des motifs, *Doc. parl.*, Chambre, sess. ord. 1997-1998, n° 1566/1, p. 15.

474 A ce propos, voy. les commentaires de Th. LÉONARD et Y. POULLET, *op. cit.*, p. 38, n° 3.

475 Avis n° 44/2001 du 12 nov. 2001, sur le site de la Commission (<http://www.privacy.fgov.be>) et publié dans la *Rev. Ubiquité*, 2002, à paraître.

476 Par contre, une interprétation raisonnable du texte de la loi conduirait à reconnaître que ne peuvent être considérées comme «*à caractère personnel*» des données collectées pour lesquelles soit le responsable s'interdit publiquement toute recherche d'identification, soit ne dispose pas des moyens techniques pour opérer cette identification. Dans le même sens, E. WÉRY, «La Commission vie privée n'aime pas les manières de l'IFPI de traquer les pirates sur l'Internet», disponible sur le site <http://www.droit-technologie.org>, 17 déc. 2001.

B. *La notion de traitement*

147. – Plusieurs décisions cherchent à dessiner les contours de la notion de traitement. Notamment, la distinction entre le dossier non soumis à la loi de 1992 et le fichier, support d'un traitement, a fait l'objet d'une décision de la Cour de cassation du 16 mai 1997[477]. Un candidat magistrat évincé du poste auquel il postulait, réclamait le droit d'accès à l'ensemble de son dossier, sur base de la loi du 8 décembre 1992. La Cour d'appel, confirmée en cela par la Cour de cassation, écarte la demande au motif que le dossier ne peut être constitutif d'un fichier au sens de la loi de 1992 : «*Qu'il ne peut être question d'un fichier au sens de la loi précitée que lorsque la structure logique suivant laquelle l'ensemble des données à caractère personnel est constitué et conservé, rend possible une consultation systématique de celles-ci*». Comme le note J. DUMORTIER[478], la simple structuration logique du contenu d'un dossier ne suffit pas; il faut en outre que la consultation du contenu soit facilitée. En d'autres termes, le traitement de l'information contenue dans le dossier doit être tel que le destinataire ou l'utilisateur du dossier puissent se dispenser d'une lecture complète du dossier pour retrouver l'information pertinente recherchée[479].

Le tribunal de première instance d'Hasselt, siégeant en référé le 2 octobre 1997[480], a de même eu à se prononcer sur l'applicabilité de la loi du 8 décembre 1992 à l'occasion d'une demande d'accès au dossier médical d'un défunt. Le président du tribunal a rejetté *in casu* l'application de la loi en précisant la plus-value que doit apporter un fichier soumis à la loi

477 Cass., 16 mai 1997, *Computerr.*, 1997/4, p. 161, note J. DUMORTIER; *J.T.*, 1997, p. 161. Cet arrêt fait suite à la décision de la Cour d'appel d'Anvers du 27 sept. 1995, *R.W.*, 1995-1996, p. 750; *A.J.T.*, 1995-1996, note J. DUMORTIER. Pour une critique de cet arrêt, voy. Th. LÉONARD, «La protection des données à caractère personnel et l'entreprise», in *Guide juridique de l'entreprise*, 2e éd., Diegem, Kluwer, 1996, titre XI, livre 112, p. 15, n° 130.

478 J. DUMORTIER, note précitée, *Computerr.*, 1997/4, p. 163.

479 Sans doute, le demandeur eût-il été bien inspiré de fonder sa demande d'accès non sur la loi du 8 déc. 1992, mais sur l'art. 3 de la loi du 11 avril 1994 relative à la publicité de l'administration (*M.B.*, 30 juin 1994) qui permet un droit de consultation des documents administratifs.

480 Civ. Hasselt (réf.), 2 oct. 1997, *Rev. dr. santé*, 1997-1998, p. 333.

par rapport à un simple dossier : « *Un dossier médical est en soi un fichier si les données y sont structurées de façon ordonnée, de telle façon que l'on peut y trouver les données intermédiaires immédiatement, sans que l'on doive consulter l'entièreté du dossier* ».

148. – On s'étonnera, au vu de cette jurisprudence, du raisonnement tenu par le tribunal de première instance de Bruxelles dans l'affaire dite *Gaia*[481] qui, pour rejeter la projection d'un film vidéo présenté par les plaignants à l'appui de leurs dires, s'appuie notamment sur le non-respect des prescrits de la loi de 1992 et, plus particulièrement, sur le fait que le montage vidéo, en tant que traitement automatisé[482], doit satisfaire aux obligations d'information des personnes concernées et de déclaration du traitement. A notre avis, il ne peut être question de traitement lorsque la collection d'images, même si elle fait l'objet de montage, n'est point structurée de telle sorte que l'accessibilité aux données personnelles relatives à un individu soit facilitée[483] [484]. En d'autres termes, la finalité de l'auteur des images n'était pas d'appliquer un traitement aux données nominatives collectées. Il est à noter que cette opinion s'écarte de celle de la Commission de protection de la vie privée à propos de la vidéosurveillance[485].

149. – Dans l'affaire *Gaia*, on notera, par ailleurs, que le juge ajoute que le fait que les images aient été prises dans un lieu public n'enlève rien au caractère personnel des données enregistrées. On rapprochera de cette affirmation celle contenue dans la décision de la Commission européenne des droits de l'homme du 14 janvier 1998[486]. L'affaire à l'origine

[481] Corr. Bruxelles, 11 janv. 2002. *Journ. proc.*, 8 févr. 2002, p. 29.

[482] « *De opname, montage en reproductie van de videobeelden is overeenkomstig artikel 1 § 3 van genoemde wet te beschouwen als een vorm van 'geautomatiseerde verwerking' zodat de wet wel degelijk toepassing is* ».

[483] Que le moyen de preuve devait être rejeté par le juge sur d'autres bases, n'est pas discuté ici. Sans doute, les possibilités de manipulation de l'image dans le cadre d'un enregistrement vidéo sont telles que l'on peut mettre en doute l'authenticité et le caractère complet des faits ainsi rapportés, comme l'a justement décidé le tribunal correctionnel de Bruxelles mais l'argument supplémentaire invoqué par le tribunal, argument tiré de l'application de la loi vie privée convainc peu. Par ailleurs, il eût été intéressant de s'interroger sur la légitimité pour des associations privées de collecter des informations établissant l'existence d'infractions à des fins de poursuite devant une juridiction pénale. Ne faut-il pas réserver de telles prérogatives aux autorités policières et judiciaires ? Question intéressante quand on songe à la volonté de certains ayants droit de rechercher sur Internet les auteurs d'infractions aux droits d'auteur ?

[484] ... sans quoi, à la limite, toute prise de vue pourrait être considérée comme un traitement.

[485] « *La notion de traitement d'images, s'étend, (...) à tout système de prises de vues, analogique ou numérique, continue ou discontinue, avec ou sans conservation de ces vues, sur quelque support que ce soit. Elle s'applique en particulier à l'utilisation des caméras* » (avis n° 34/99 d'initiative relatif aux traitements d'images effectués en particulier par le biais de systèmes de vidéosurveillance).

[486] C.E.D.H., 14 janv. 1998, *A.J.T.*, 1997-1998, p. 501, note P. DE HERT et O. DE SCHUTTER.

de la décision strasbourgeoise concernait l'application de la loi belge du 8 décembre 1992 à des opérations de « *vidéosurveillance* » de lieux publics, réalisées par des autorités tant privées que publiques. La Commission a estimé qu'« *en l'absence de tout enregistrement, on voit mal comment les données visuelles recueillies pourraient être portées à la connaissance du public ou utilisées à d'autres fins que des fins de surveillance des lieux* ». La Commission relève encore que « *les données qui pourraient être recueillies par une personne se trouvant derrière des écrans de contrôle sont identiques à celles qu'elle aurait pu obtenir par sa présence sur les lieux* ». Elle conclut dès lors que « *les faits susceptibles d'être observés ne peuvent donc essentiellement être que des comportements publics (...). Il n'y a, en l'espèce, aucune apparence d'ingérence dans la vie privée du premier requérant* ».

On ne peut que s'étonner de ce raisonnement qui tend à exclure de toute protection les données recueillies à propos d'événements ayant eu lieu sur la voie publique.

Il va de soi que les limites au contrôle permis par les techniques de vidéosurveillance, qui sont imposées par la nécessité de respecter la vie privée, ne s'appliquent pas qu'aux seuls lieux privés[487]. Il va également de soi que la nature de ce contrôle est radicalement différente de celui opéré par la présence physique d'un policier ou de tout autre contrôleur[488].

La question se pose néanmoins de savoir si ces limites doivent être déduites des législations relatives à la protection des données personnelles ? Nous n'en sommes pas convaincus. La simple visualisation de faits, à distance et en direct, combinée avec la possibilité de repérage des personnes figurant sur les images, soit grâce à un logiciel opérant ce repérage automatique[489], soit vu le contexte par la connaissance *a priori* des personnes filmées[490], ne nous apparaît pas donner lieu à un traitement vu l'absence de toute structure des données permettant une accessibilité plus facile aux données relatives aux personnes concernées, c'est-à-dire de tout « *fichier* ».

[487] Sur ce point, parmi de nombreux auteurs, voy. P. LEMMENS, « Het recht op eerbieding van de persoonlijke levensfeer, in het algemeen en ten opzicht van de verwerking van persoonsgegevens », in *Om deze redenen – Liber Amicorum Armand Vandenplas*, Gand, Mys & Breesch, 1994, 3/3 et s.

[488] Voy. la note de P. DE HERT et O. DE SCHUTTER sous la décision commentée.

[489] Ainsi, dans certains lieux comme les aéroports où le système de vidéosurveillance est relié à une banque de données « *image* ».

[490] Ainsi, dans le contexte de relations de travail (voy. à cet égard, la CCT n° 68 du 16 juin 1998 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail, qui applique les principes de la loi de 1992).

III. – Le droit à l'information des entreprises, associations et administrations

150. – L'exigence de finalités légitimes, déterminées et non incompatibles des traitements de données à caractère personnel est un principe clé des législations de protection des données (§ 1). La stricte proportionnalité du contenu des traitements aux finalités ainsi poursuivies (principe de conformité du contenu) et l'exactitude des données traitées constituent le corollaire de ce premier principe (§ 2).

Sur ces principes fondamentaux, nous consacrerons des développements séparés à deux types de traitements qui, plus particulièrement, ont fait l'objet de l'attention des juges : les publications par la presse et le contrôle par l'employeur de l'utilisation des systèmes d'information par leurs employés (§ 3).

Si la loi du 18 décembre 1998 consacre les principes exposés ci-dessus plus clairement encore que le texte originaire de la loi de 1992, la jurisprudence n'a pas attendu l'application de la loi pour les affirmer et leur donner une portée concrète.

A. – De la légitimité de l'existence des traitements

§ 1. Légitimité des traitements et secteur privé

151. – On notera tout d'abord que la Cour d'appel d'Anvers, le 3 mai 1999[491], a confirmé la décision du président du tribunal de commerce du 7 juillet 1994[492] prise dans le cadre d'une action en cessation, qui condamnait une banque pour avoir utilisé à des fins publicitaires pour des produits d'assurance des données relatives à sa clientèle communiqués dans le cadre d'ordres de paiement. On rappellera qu'en première instance, la légitimité du traitement marketing n'avait pas en soi été contestée. Le tribunal avait souligné le défaut de proportionnalité du contenu des données utilisées et l'absence d'informations suffisantes des clients de la banque sur le fait que les données étaient utilisées pour des services non bancaires. La décision de la Cour est plus sévère encore. Elle met en cause la légitimité du traitement opéré par la banque. Elle s'appuie sur le fait

[491] Anvers, 3 mai 1999, *A.J.T.*, 1999-2000, p. 437, note C. De Vos; *Ann. prat. comm.*, 1999-2000, p. 524.

[492] Largement commenté dans la précédente chronique, *J.T.*, 1996, pp. 233 et s., n[os] 63 et s.

que la finalité d'un virement est la transmission d'informations au bénéficiaire et que dès lors l'utilisation par le banquier de telles informations à des finalités autres, excède les «*prévisions raisonnables*» du client de la banque[493]. En d'autres termes, l'utilisation par la banque de données relatives aux raisons du virement apparaît donc illégitime («*parce que disporportionnée* (want overmatig)[494]»). Le banquier contrevient à son devoir de discrétion par une utilisation claire et non sollicitée de sa fonction de banquier pour une finalité d'assurance. Nonobstant la pratique de plus en plus répandue de la bancassurance, la Cour rappelle ainsi la nécessité d'une séparation claire des fonctions bancaires, d'une part, et d'assurance, d'autre part, en vue d'un exercice de ces activités conforme à la déontologie de ces professions. Seul, le consentement de la personne concernée semble dès lors pouvoir être une cause légitime d'une utilisation marketing par le banquier des données relatives à la raison d'un virement[495].

152. – On rapprochera la dernière décision analysée de la décision du tribunal d'Hasselt du 23 avril 1997[496]. En l'occurrence, une société avait conclu un contrat par lequel elle s'engageait à envoyer à des potentiels futurs mariés, chaque mois, un livre avec des bons d'achat sur lequel

[493] «*dat nergens uit blijkt dat appellante aan haar klanten heeft gemeld dat zij informatie zou opslaan en gebruiken omtrent de inhoudelijke redenen waarom betalingensopdracht de reden van betaling is vermeld (in casu de betaling van een bepaalde verzekeringpremie) dit enkel gebeurt met de bedoeling dat de bankier deze vermelding zou doorgeven opdat de bestemmeling de betaling zou kunnen thuis brengen; dat het met andere woorden gaat om informatie die niet voor de bankier maar voor de begunstigsde van de betaling bestemd is; dat indien de klanten van appellante kennis hebben van of zelfs toestemming hebben verleend tot opslag, verwerking en gebruik van inlichtingen, dit uiteraard slechts kan betrekking hebben op de inlichtingen die voor appellante als bankier bedoeld zijn; dat hiertoe de redenen van betaling niet behoren; (...)*».

[494] «*Dat de vertrouwelijkheid die geacht wordt te gelden in bankzaken ook ten dele geldt tussen bankier en klant; dat uit de wijze (hiervoor aangehaald) waarom hij benaderd werd de rekeninghouder slechts kan afleiden dat de bank zich ongevraagd bezig houdt met de inhoud van de gegeven betalingsopdracht en niet schijnt te aarzelen om van de bekomen informatie gebruik te maken; dat door de inhoudelijke redenen van betalingen te detecteren en uit te spelen appellante op ongeoorloofde (want overmatige) wijze binnendringt in de persoonsgegevens van haar klanten*».

[495] On notera de même la décision du président du tribunal de commerce de Bruxelles du 13 oct. 1995 (*Ann. prat. comm.*, 1995-1996, p. 423) qui condamne l'utilisation du fichier «crédit» d'un client par un préposé de la division voyage, une telle utilisation étant incompatible avec celle de la collecte. A noter qu'en l'occurrence «l'utilisation» consistait en un simple coup de téléphone du préposé à la division «voyages» : «*Lorsque le préposé de la division voyages d'une banque demande des informations concernant le crédit d'un client à la banque, et que cette dernière consulte ses fichiers qui contiennent des informations personnelles, il s'agit d'un usage au sens de l'article 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. Le fait que ce préposé reçoit ces informations par téléphone et ne consulte pas personnellement les fichiers, est sans importance en la matière*».

[496] Comm. Gand, 23 avril 1997, *T.G.R.*, 1997, p. 174.

figurait le magasin de photos tenu par sa cliente. Avec la même périodicité, elle adressait à sa cliente la liste des personnes ainsi contactées. Pour cesser le paiement des mensualités dues, la cliente invoquait le caractère illicite du contrat pour contrariété à la loi de 1992 (cession de données à caractère personnel sans consentement des personnes concernées). Le tribunal rejette l'argument au motif que le plaignant n'est pas la personne concernée[497]. En outre, la collecte des données auprès de *«huwelijksbeurzen»* ou de journaux d'annonces publicitaires est légitime et le traitement poursuit des finalités légitimes, à savoir la communication d'opportunités de réduction auprès d'un magasin de photos.

153. – C'est également dans le cadre d'une action en cessation que le président du tribunal de commerce de Bruxelles devait intervenir dans une affaire opposant la Fédération des importateurs d'automobiles indépendants à la FEBIAC et à l'Etat belge[498]. Les importateurs indépendants se plaignaient de diverses campagnes publicitaires auprès de leurs clients, menées sur base d'adresses obtenues par divers concessionnaires officiels auprès de la FEBIAC. Cette dernière avait en effet conclu une convention avec l'Administration des transports (plus particulièrement le Répertoire d'immatriculation des véhicules (en néerlandais la DIV)) l'autorisant à diffuser les données ainsi collectées à ses membres signataires d'un *«code de conduite»* qui limite l'utilisation des données transmises aux communications avec les propriétaires d'un véhicule de leur marque dans le cadre d'une maintenance *«sécurité»* à entendre au sens le plus large.

La présidente du tribunal condamne sévèrement cette pratique dénuée de tout fondement légal : *«dat de DIV-gegevens onder de 'persoonsgegevens' vallen, zodat de mededeling ervan aan de finaliteit van het repertorium onderwerpen is, en alleen toegelaten is in zovere het openbaar belang zulks vereist (...) dat dit betekent dat de finaliteit van de mededeling exclusief ligt in de contrôle van risico's die volgen uit het wegverken (...) dat het begrip 'verkeersveiligheid' strikt uitgelegd moet worden (....) dat hetgeen voorafgaat toelaat te besluiten dat de mededeling van D.I.V.-gegevens aan FEBIAC voor wat anders dan het terugroepen van voertuigen, met een constructiegebrek in strijd is met de wet van*

[497] «Niet verweerder maar de individuen zelve kunnen daaromtrent indien nodig reageren. Op geen enkele manier is de privacy van verweerder geschaad door het optreden van eiseres».

[498] Comm. Bruxelles (prés.), 12 juillet 1996, *DA/OR*, 1996, liv. 39, p. 73, note G. BALLON; *D.C.C.R.*, 1996, p. 351, note F. DUMONT-NAERT; *R.W.*, 1996-1997, p. 855, note J. MEEUSEN. On rapprochera cette affaire de celles jugées par le président du tribunal de commerce de Bruxelles le 20 mars 1995 (*SA Expo c/ SA Mercedes-Benz e.a.*, AC/6062/94, inédit, analysé dans la précédente chronique, *J.T.*, 1996, p. 233, n° 62) et par le tribunal de commerce d'Anvers (*Moretus Motor c/ British Auto Center*) le 12 oct. 1995.

8 december 1992; dat het KB van 31 december 1953 niets zegt in verband met 'terugroepacties'; dat de praktijk inbreuk maakt op het finaliteitscriterium; dat het zelfde geldt wat betreft het evenredigheidscriterium nu de overdracht van DIV-gegevens niet proportioneel is aan de vooropgestelde finaliteit, doch alle gegevens überhaupt betref».

On notera en outre que l'ordonnance rejette l'argument de la FEBIAC fondé sur la loi d'accès aux documents administratifs du 11 avril 1994 au motif que l'article 10 de cette loi ne permet pas l'utilisation des données obtenues dans le cadre de celle-ci à des fins commerciales[499].

A propos de la distribution gratuite d'un annuaire papier reprenant, par rue et par maisons, les habitants et les commerçants d'une ville, le tribunal correctionnel de Gand[500] se montre également sévère, suivant en cela un avis de la Commission de protection de la vie privée[501], en estimant, sur base du texte ancien de l'article 5, que *«er slechts geen sprake kan zijn van een evenwicht tussen de belangen van de houder van het bestand en de betrokkene personen, vermits een aantal waarborgen worden voorzien, waaronder de uitdrukkelijke toestemming van de betrokkene».* Ainsi, le tribunal opère la balance d'intérêts entre l'intérêt légitime poursuivi par l'éditeur et le public destinataire de la brochure, d'une part, et l'intérêt des personnes concernées, d'autre part. Eu égard aux risques évidents de démarchage commercial et de reconstitution de la composition des ménages, il estime que seul le consentement des personnes concernées et non un simple droit d'opposition pourrait légitimer un tel traitement[502].

154. – La décision du 19 décembre 2000 prononcée par le président du tribunal de première instance de Bruxelles siégeant *«comme en référé»*, selon l'expression de l'article 14 de la loi de 1992[503], se penche sur la légitimité de la centrale DATASSUR, créée par les entreprises d'assu-

[499] Sur les questions difficiles nées de la coexistence de ces lois, voy. C. de TERWANGNE, *Droit à la transparence et droit à l'information : vers une société de la connaissance*, Cahier du CRID, n° 23, Bruxelles, Bruylant, à paraître; P. DE HERT, «De grondrechten en wetten m.d.t. openbaarheid van bestuursdocumenten en bescherming van de persoonlijke levenssfeer», *C.D.T.K.*, 2001, pp. 374 et s.

[500] Corr. Gand, 22 janv. 2000, *Computerr.*, 2001, p. 263.

[501] Recommandation n° 1/95 du 18 juillet 1995 à propos de l'utilisation des listes d'adresse par des firmes de publicité (rapporteurs VOET et GOLVERS), publiée in *Computerr.*, 1996, pp. 82 et s.

[502] L'avis de la Commission déjà mentionné distinguait la question de la légitimité de la finalité du traitement de la conformité des données à cette finalité. Ainsi, même légitime, la Commission relevait que le traitement ne devrait pas reprendre les données par rue et par numéro de maison, ni contenir les prénoms des occupants.

[503] Civ. Bruxelles, 19 déc. 2000, *Bull. ass.*, 2001, p. 266, note C. van OLDENEEL.

rance pour permettre une centralisation des mauvais risques. Cette décision est doublement intéressante, à la fois par le raisonnement tenu et par le fait que cette décision s'écarte du raisonnement proposé par l'avis d'initiative de la Commission de protection de la vie privée[504]. En l'occurrence, au sein de l'UPEA, a été conclue une convention relative au fichier RSR (Risques spéciaux) suivant laquelle chaque contractant signale «*mutuellement les risques spéciaux en IARD, ce qui à terme a pour conséquence de maintenir les primes à un niveau équitable pour tous*». Sans entrer dans les détails ni de la convention, ni de la situation particulière de la personne plaignante, relevons que cette dernière signalée comme risque «*Résiliation plusieurs sinistres*» se plaignait de divers manquements à la loi de 1992. Le tribunal dispose à cet égard :

«*Attendu que Mme van de G. fait valoir, à l'appui de sa demande que*

- *les finalités du traitement litigieux seraient illégitimes,- les données litigieuses seraient inadéquates, non pertinentes et excessives par rapport aux finalités déclarées,*
- *les données litigieuses seraient interdites dès lors qu'elles constitueraient des données judiciaires,*
- *Datassur n'aurait pas respecté son devoir d'information,*
- *le traitement litigieux serait contraire à la directive européenne 95/46/CE qui interdit la prise de décision sur la base exclusive de traitements automatisés*».

Seule la question de la légitimité du traitement sera évoquée à ce stade. Les autres points seront analysés plus loin[505].

La question de la légitimité du traitement suppose que soient vérifiées trois conditions : l'intérêt légitime poursuivi par le responsable du traitement et le tiers, destinataire de la communication; leur supériorité sur les intérêts et droits de la personne concernée; la démonstration du caractère nécessaire du traitement pour la réalisation des intérêts légitimes ci-dessus évoqués.

Le juge considère que cette triple condition est remplie par Datassur. La Commission de protection de la vie privée avait cependant estimé : «*Si les principes contenus dans la loi du 8 décembre 1992 n'interdisent pas nécessairement la constitution d'une mutuelle d'information sur le risque à assurer, les intérêts légitimes poursuivis par ces enregistrements*

[504] Avis d'initiative relatif au fichier RSR géré par le groupement d'intérêt économique «Datassur» (avis n° 21/2000 du 28 juin 2000).

[505] *Infra*, n° 158.

doivent donc être mis en balance avec le droit à la protection de la vie privée de la personne concernée[506]. *Il semble que le fléau de la balance doive pencher in casu en faveur du respect de la vie privée, compte tenu :*

- *du caractère essentiel de la fourniture des produits d'assurance en rapport notamment avec certaines dispositions légales qui obligent les personnes concernées à contracter une assurance (par exemple, l'obligation légale d'assurer sa responsabilité automobile);*
- *du fait qu'une écrasante majorité de compagnies proposant des produits d'assurance IARD communiquent leurs données à Datassur et ont accès aux données du fichier RSR;*
- *du fait que chaque belge peut potentiellement être enregistré dans le fichier avec cette conséquence que la tenue d'un tel fichier ne peut être laissée à la seule initiative privée sans garantie pour le citoyen;*
- *des possibilités qu'offrent, pour l'information de l'assureur sur le risque à assurer et la personnalisation des primes, les systèmes du bonus-malus et de la segmentation.*

Même avec le consentement de l'intéressé, le fichage n'est licite que s'il rencontrait des prévisions raisonnables de l'intéressé. Ceci signifie qu'un consentement non suffisamment éclairé ne suffit pas à rendre le fichage licite. En effet, les données doivent être collectées pour des fins légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé (art. 4 de la loi)».

Le tribunal considère au contraire, premièrement, que : «*L'intérêt de Datassur à traiter ces données – justice actuarielle et lutte contre la fraude – est en effet légitime*», deuxièmement, que les informations relatives à la résiliation des risques sont bien nécessaires à l'appréciation du risque minimum[507] dans la mesure où ni les déclarations bonus-malus, ni

[506] La formulation de l'article 2 nouveau de la loi dispose que «*Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée*». La Constitution mentionne, par ailleurs, le droit à la vie privée ainsi que le droit au travail.

[507] Voy., à cet égard, la référence aux raisonnements de J. DIIONT («Le traitement des données à caractère personnel dans le secteur des assurances – La légalité des banques de données», *Rev. dr. ULB*, 2000, p. 290) : «Que le système d'assurance basé sur la solidarité organisée entre les assurés, ainsi que la concurrence nécessitent que les assureurs puissent évaluer le risque économique qu'ils encourent» et de B. DUBUISSON («Secrets, mensonges et confidences – Conclusions», *Rev. dr. ULB*, 2000, p. 364) : «On peut dès lors souscrire assez aisément à la légitimité d'un traitement qui tend à écarter les fraudeurs et à maintenir la justice actuarielle».

les techniques de segmentation du marché ne suffisent et enfin, troisièmement, que les informations fournies par le système Datassur sont minimales par rapport à celles que l'assuré est tenu de fournir à son assureur en vertu de la loi du 25 juin 1992.

On notera que le raisonnement tenu par le président du tribunal ne répond pas entièrement aux arguments de la Commission sur deux points. Le premier point est l'ampleur du fichage qui concerne la quasi-totalité des entreprises d'assurances et dès lors potentiellement une très large majorité de la population belge[508]. La Commission avait estimé que cette caractéristique du fichier rendait nécessaire une intervention législative.

Le second point est l'interprétation que la Commission donne de l'article 4, § 1, qui exige que le traitement soit compatible avec les finalités de la collecte. Même avec le consentement de l'intéressée, note la Commission, le fichage n'est licite que s'il rencontre les prévisions raisonnables[509] de l'intéressé. Cela signifie qu'un consentement non suffisamment éclairé ne suffit pas à rendre le fichage licite dans la mesure où l'incompatibilité d'un traitement rend celui-ci illégitime sauf «*consentement*» de la personne concernée par ce traitement.

§ 2. Légitimité des traitements et secteur public

155. – C'est surtout à propos des traitements mis en place par la Sûreté de l'Etat et les services de renseignements généraux que la jurisprudence a eu l'occasion de fixer les principes mêmes de la légitimité d'un traitement opéré par la puissance publique à l'égard de ses citoyens[510].

[508] Voy. dans le même sens, J. DHONT (*op. cit.*, p. 290), qui s'interroge dès lors sur la nécessité d'une loi. A cet égard, on pourrait également évoquer l'article 20 de la directive européenne 95/46 qui suggère des garanties spécifiques lorsque le traitement présente de par sa dimension des risques particuliers pour une large fraction de la population. Ce raisonnement pourrait justifier l'obligation de recourir à une loi chaque fois qu'une centrale négative de renseignements, vu son caractère quasi monopolistique dans un pays, crée pour la personne qui s'y trouve fichée le risque d'être exclue du bénéfice de services pourtant essentiels pour la vie en société.

[509] Ainsi, il ne s'agit pas de remettre en cause la balance d'intérêts telle qu'opérée par le juge mais de souligner le défaut d'information de la personne concernée lors de la signature du contrat d'assurance à propos de l'existence du fichier DATASSUR, des conditions du fichage et des risques encourus dans ce cas.

[510] Sur le rôle joué par cette jurisprudence dans l'adoption de la loi organique du 30 nov. 1998 des services de renseignements et de sécurité (*M.B.*, 18 déc. 1998), voy. B. HAVELANGE et Y. POULLET, «Secret d'Etat et vie privée ou comment concilier l'inconciliable ?», in *Droit des technologies de l'information – Regards prospectifs* (E. MONTERO éd.), Cahier du CRID, n° 16, Bruxelles, Bruylant, 1996.

Deux arrêts du Conseil d'Etat rendus le même jour, le premier dans l'affaire dite *Cudell*[511] et le second dans l'affaire *Wicart*[512] à propos d'une sanction prise à l'encontre d'un fonctionnaire de la sécurité, et une décision du tribunal de première instance de Bruxelles[513] rappellent avec énergie la jurisprudence constante de la Cour européenne des droits de l'homme pour dénier tout droit des services de renseignement à la collecte et aux traitements d'informations vis-à-vis de citoyens ou de manière plus large d'individus : «*Considérant que l'article 8 § 2 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales permet l'ingérence de l'autorité publique dans l'exercice du droit de toute personne au respect de la vie privée, pour autant que cette ingérence est conforme à la loi, qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire notamment à la sécurité nationale et à la sûreté publique, et que les textes qui la prévoient soient accessibles à l'intéressé et rédigés en termes assez clairs pour lui indiquer de manière adéquate quelles circonstances et sous quelles conditions, ils habilitent la puissance publique à s'y livrer, spécialement si l'ingérence présente un caractère secret*»[514].

La décision du tribunal de première instance de Bruxelles précise encore le propos en déniant au droit non écrit, voire à de simples instructions ou directives, la qualité de «*loi*» au sens de l'article 8 de la Convention européenne des droits de l'homme.

«*En Belgique, le droit non-écrit ne peut être considéré comme une loi répondant aux critères de l'article 8 précité puisque la Constitution attribue au législateur national ou décrétal compétence exclusive pour adapter les droits fondamentaux qu'elle garantit.*

Pour qu'il y ait loi, au sens de l'article 8, il faut donc, en droit interne, un acte écrit à valeur obligatoire et normative qui ne peut être confondu avec de simples instructions ou directives.

La loi doit être accessible, précise et prévisible, en sorte qu'elle permette à chacun de se rendre compte dans quelle mesure elle permet l'ingérence de l'autorité publique, qu'elle fournisse suffisamment de renseignements concernant les normes qui sont d'application et que le

[511] C.E., 30 juin 1995, arrêt n° 54-138.

[512] C.E., 30 juin 1995, arrêt n° 54-139.

[513] Civ. Bruxelles (24e ch), R.G. 95/14503, décision dite *Vlaams Block* (collecte d'informations prises au sujet des membres d'un parti politique).

[514] Cet attendu est repris de l'arrêt *Wicart*. Une formulation quasi semblable de l'attendu est présente dans les deux autres décisions citées.

justiciable puisse adapter sa conduite à ces normes et être en mesure, éventuellement après avis éclairé, de prévoir avec une suffisante certitude, les conséquences de ses agissements.

Les articles 3 et 5 de la loi du 8 décembre 1992 relative à la protection de la vie privée[515] *ne permettent à la Sûreté de l'Etat que le traitement informatique des données clairement déterminées dans un but licite. L'Etat ne peut se baser sur d'autres critères pour réunir des renseignements ou établir des fichiers à l'égard des personnes privées, par exemple parce qu'elles sont membres d'un parti déterminé. Il y a lieu d'interdire de telles pratiques et d'en ordonner la cessation».*

156. – Dans le domaine des administrations de la santé et de la sécurité sociale, un arrêt de la Cour de cassation en date du 1er octobre 1997 à propos de la vaccination obligatoire des enfants[516] rappelle le même principe : «*L'article 8 de la Convention européenne des droits de l'homme autorise l'ingérence des autorités publiques dans la vie privée qu'à la double condition qu'elle soit légale et qu'elle constitue une mesure nécessaire à la protection de la santé*». Cette décision vérifie ainsi le caractère nécessaire et proportionné de la mesure obligatoire par rapport aux risques d'épidémie toujours présents et l'habilitation par arrêté royal de la prise de cette mesure.

Elle fait écho à la décision de la Cour européenne des droits de l'homme dans l'affaire *M.S. c/ Suède* du 27 août 1997[517]. En l'occurrence, la plaignante se plaignait qu'à l'occasion du remboursement de soins auprès de la caisse de sécurité sociale, un certain nombre d'éléments du dossier médical devait être transmis. La Cour ne conteste pas l'atteinte à la vie privée[518] mais estime cependant que cette atteinte était légitime au

[515] On rappellera que sous l'empire de l'ancienne version de la loi de 1992, les traitements de la Sûreté de l'Etat et des services de renseignements étaient totalement exemptés de l'application de la loi de protection de la vie privée. Désormais, depuis l'entrée en vigueur des modifications introduites par la loi de 1998, tel n'est plus le cas, même si certaines exceptions à des dispositions spécifiques de la loi sont maintenues.

[516] Sans doute, la contestation à la base de l'arrêt visait non le traitement de données à caractère personnel (les personnes à vacciner) mais la vaccination prise sur base de ce traitement.

[517] C.E.D.H., 27 août 1997, *M.S. c/ Suède*, *Rec. Arrêt et décisions*, 1997-IV, pp. 1437 et s.

[518] *La Cour relève que «le dossier médical en question comportait des données de nature hautement personnelle et sensible concernant Mme M.S. et notamment des informations relatives à un avortement. Tout en demeurant confidentiel, il est passé d'une autorité publique à une autre, et un nombre accru d'agents publics ont donc pu en prendre connaissance (§§ 12-13 ci-dessus). De plus, si les informations avaient été collectées et conservées au service de gynécologie en rapport avec un traitement médical, leur communication ultérieure servait un but différent : celui de permettre à la Caisse d'examiner la demande d'indemnisation présentée par la requérante. Il ne résultait pas du fait que celle-ci s'était fait soigner*

regard des trois exigences posées par l'article 8, § 2, de la Convention européenne des droits de l'homme : «*prévue par la loi*», «*poursuite d'un but légitime*» et «*nécessaire dans une société démocratique*».

La Cour rappelle que la protection des données à caractère personnel et spécialement des données médicales revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention. «*Le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les Parties contractantes à la Convention. Il est capital non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé en général*»[519].

La Cour note à propos des données en jeu : «*L'intérêt qu'il y a à protéger de telles informations pèsera donc lourdement dans la balance lorsqu'il s'agira de déterminer si l'ingérence était proportionnée au but légitime poursuivi, sachant qu'une telle ingérence ne peut se concilier avec l'article 8 de la Convention que si elle vise à défendre un aspect primordial de l'intérêt public*».

157. – Enfin, à propos de la recevabilité devant une juridiction pénale d'une preuve par profil génétique, la Cour de cassation[520] analyse la portée du consentement donné par un prévenu à un prélèvement corporel aux fins d'expertise génétique effectuée dans le cadre d'une information ou d'une instruction pénale. La Cour dispose à cet égard 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 s'applique, note la Cour, sans doute au traitement de données génétiques permettant d'identifier une personne physique*»[521]. Elle estime dès lors que les informations collectées

au service de gynécologie qu'elle consentirait à la communication des données à la Caisse. Eu égard à ces considérations, la Cour estime que la communication des renseignements à la Caisse par le service de gynécologie a porté atteinte au droit au respect de la vie privée garanti à l'intéressée par le paragraphe 1 de l'article 8» (décision citée, p. 1147).

[519] Dans le même sens, C.E.D.H., 25 févr. 1997, *Rev. dr. santé*, 1997-1998, p. 314, note S. CALLENS, à propos de la décision d'un tribunal suivant laquelle les renseignements médicaux collectés dans le cadre d'un procès et concernant la séropositivité de la personne concernée tomberaient dans le domaine public 10 ans après la décision.

[520] Cass., 31 janv. 2001, publié sur le site de la Cour de cassation (<http://www.cass.be/cgi-juris>).

[521] En particulier, à l'époque, «*l'arrêté royal n° 8 du 7 février 1995 déterminant les fins, les critères et les conditions des traitements autorisés de données visées à l'article 8 de la loi de 1992 qui dispose que les autorités publiques et les services de police qui gèrent un traitement en vue de l'exercice de leurs missions de police judiciaire peuvent traiter les données visées à l'article 8, c'est-à-dire entre autres, celles ayant pour objet les infractions dont une personne est soupçonnée ou dans lesquelles elle est impliquée*».

par l'expert dans le cadre de la mission qui lui est confiée par le juge d'instruction pouvaient légitimement, sur base du consentement donné «*de manière suffisamment éclairée (1°) pour les besoins de l'instruction (2°) aux fins d'expertise génétique*», être conservées «*aux fins de comparaison ultérieures, dans le contexte d'une information ou d'une instruction pénale relative à d'autres faits*»[522].

B. – De la proportionnalité des données traitées et de leur exactitude

158. – L'article 4 de la loi du 8 décembre 1992 modifiée exige que les données soient adéquates, pertinentes et non excessives eu égard à la finalité légitime poursuivie. Au-delà, elle requiert leur exactitude, dans toute la mesure du possible, leur mise à jour et, enfin, leur effacement.

La décision *DATASSUR* déjà citée[523] se prononce sur le premier type d'exigences légales[524]. La non-conformité des données aux finalités du traitement était en effet invoquée par l'assuré. Si effectivement la finalité du traitement de la centrale des risques que constitue DATASSUR est de permettre l'appréciation du risque par le destinataire des données enregistrées par DATASSUR, l'assuré enregistré soutenait que les données enregistrées ne devaient point comprendre certaines données, comme les sinistres dans lesquels la responsabilité de l'assuré n'est pas engagée et par contre devrait inclure le nombre total de sinistres afin de permettre «*le calcul de statistiques de survenance de risque permettant la personnalisation de la prime*». La réponse du juge ne nie pas la validité de l'argument si telle avait été la finalité du fichier mais estime qu'au regard de l'exacte finalité poursuivie par le traitement, à savoir le contrôle de la conformité des informations transmises par l'assuré avec la réalité et au vu du droit des compagnies d'assurances de résilier un contrat suite à une déclaration de sinistre indépendamment de toute responsabilité de l'assuré, les données collectées et transmises par DATASSUR sont bien pertinentes et non excessives par rapport à la finalité légitime déclarée.

[522] A noter depuis la loi du 22 mars 1999 sur les expertises introduisant un art. 44*ter* dans le Code d'instruction criminelle ADN. Sur cette loi, voy. C. MEUNIER, «L'analyse génétique à des fins de preuve», in *Les nouveautés en procédure pénale*, Formation permanente CUP, mars 2000, pp. 260 et s.

[523] *Supra*, n° 154.

[524] Voy. égal. les décisions prises en matière de contrôle par l'employeur de l'utilisation par leur employé des systèmes d'information mis à leur disposition (*infra*, n°s 163 et s.).

159. – La question de l'exactitude des données traitées fait l'objet de deux décisions intéressantes : la première[525] concerne l'émission par l'éditeur d'un annuaire téléphonique des coordonnées d'un médecin généraliste. Il est intéressant de noter que la simple circonstance de l'absence de mention ne suffit pas à entraîner la responsabilité de l'éditeur mais que le juge estime sur base des circonstances concrètes de l'espèce que l'omission constitue une faute. La seconde, inédite[526], concerne l'enregistrement de défauts de paiement d'échéances de mensualités alors même qu'il apparaissait que le crédité n'avait pas reçu les rappels en raison d'une erreur d'adresse. Le tribunal considère que l'inexactitude de la donnée résulte de «*l'inadéquation d'une information donnée par le crédité*», soit d'une absence de vérification des mentions manuscrites du document intitulé «contrat d'achat». En d'autres termes, conclut le tribunal, «*[le crédité] n'établit pas à suffisance de droit que [le responsable du traitement] a commis une faute*».

Cette jurisprudence, fondée sur l'ancien libellé de l'article 16, § 3, de la loi de 1992 qui clairement considérait que l'obligation d'exactitude était une obligation de moyens[527], risque d'être remise en cause. En effet, les textes nouveaux, celui de l'article 4, § 1, 4°, relatif à l'obligation d'exactitude et celui de l'article 15*bis* relatif à la responsabilité, mettront dorénavant à la charge du «*responsable du traitement*» la preuve de l'inexistence de sa faute, la faute de la victime ou d'un tiers et faciliteront dès lors la démarche des personnes concernées.

160. – L'obligation d'effacement des données lorsque celles-ci ne sont plus nécessaires au regard de la finalité du traitement a fait l'objet d'une décision intéressante du président du tribunal de première instance de Bruxelles, le 13 septembre 1995[528], dans le cadre des compétences que lui accorde l'article 14 de la loi de 1992. Les demandeurs, dont les noms avaient été enregistrés dans la centrale d'incidents de remboursement, réclamaient la radiation de leur nom en invoquant la disproportion entre la sanction qui les frappe du fait du maintien de cet enregistrement et leur légère défaillance. Le président du tribunal accueille leur demande[529] no-

[525] Civ. Liège (réf.), 6 juin 1995, *D.I.T.*, 1996/1, p. 47.

[526] Bruxelles (4e ch.), 11 juin 2001, en cause *L. c/ SCRL Record*, R.G. 1998/AR/2002, inédit.

[527] Voy. sur ce point la jurisprudence relative aux centrales d'incidents de paiement reprise et commentée dans la chronique précédente, *J.T.*, 1996, p. 233, n°s 64 et s., en particulier Civ. Bruxelles (prés.), 22 mars 1994, *J.T.*, 1994, p. 82.

[528] Civ. Bruxelles (prés.), 13 sept. 1995, *D.C.C.R.*, 1996, p. 57, note Th. LÉONARD.

[529] A noter que le même raisonnement avait déjà, selon les demandeurs, été tenu par la même présidence dans un jugement rendu le 12 avril 1995 (R.G. 95/53, inédit), malheureusement non en notre possession.

nobstant le fait que les arrêtés royaux du 20 novembre 1992 pris en application de la loi du 12 juin 1992 relative au crédit à la consommation mentionnent un délai de conservation, en l'occurrence non encore atteint. Il estime en effet que les principes de la loi de 1992 priment les dispositions des arrêtés royaux susmentionnés, dans la mesure où «*la limitation [que poseraient ces dispositions], à la supposer impérative et intangible serait contraire aux principes tant de la loi du 8 décembre 1992 que de la convention n° 108 voire même à l'article 8 de la Convention de sauvegarde des droits de l'Homme*». La demande ainsi accueillie n'est cependant pas fondée *in casu* selon le président :

«*Attendu qu'il est bien évident que la finalité desdits fichiers ne justifie pas que les données soient supprimées, dès que le prêt à la consommation au cours duquel les défaillances ont été enregistrées a été entièrement remboursé;*

Que les traitements visent à établir une liste de consommateurs 'à risques' à qui l'octroi de crédit doit être évité en raison de leur fragilité financière; qu'il ne peut être conclu du paiement effectué que cette fragilité financière a immédiatement disparu;

Qu'un délai de deux ans avant de procéder à la suppression de ces données ne paraît pas excessif eu égard aux circonstances de la cause; (...)».

C. *Cas particuliers*

§ 1. Publication par la presse et vie privée

161. – Trois décisions cherchent à établir le difficile équilibre entre le droit de la presse à la libre expression et le droit des personnes concernées à voir respecter leur vie privée à l'occasion de publications dans la presse.

La première, jugée par le tribunal de première instance de Namur le 17 novembre 1997[530], concernait la publication par un journal de presse écrite outre d'un fait divers d'actualité, de l'antécédent judiciaire concernant une des personnes impliquées dans ce fait divers. Cette dernière avait en effet été condamnée un mois auparavant avec sursis. Le juge rappelle que «*La liberté de la presse et les droits qui en découlent, du point de vue*

[530] Civ. Namur, 17 nov. 1997, *J.T.*, 1998, p. 187.

des journalistes, doivent nécessairement se concilier, de manière équilibrée, avec d'autres droits également reconnus par la Constitution et par les instruments internationaux qui ont une valeur supérieure à celle de la Constitution : ainsi, en va-t-il du droit au respect de la vie privée». Sur cette base, il estime que les personnes condamnées judiciairement disposent d'un «*réel droit à l'oubli*»[531] :

«*Ce droit comprend, pour une personne condamnée judiciairement un réel droit à l'oubli, qui découle tant de l'article 22 de la Constitution que de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ainsi que l'article 19 du Pacte international relatif aux droits civils et politiques.*

Ce droit à l'oubli doit être considéré comme étant celui qui permet à l'individu dont la vie n'est pas consacrée à une activité publique, d'exiger le secret et la tranquillité sans lesquels le libre développement de sa personnalité serait entravé».

«*Le respect de ce droit, conclut le tribunal, en ce compris par les journalistes se prévalant de l'exercice de la liberté de la presse, doit être considéré comme un principe; il peut toutefois y être dérogé s'il s'agit, d'une part, de rediffuser des éléments déjà divulgués à l'époque des faits ayant valu condamnation judiciaire et, d'autre part, s'il y a un intérêt contemporain à cette seconde divulgation*».

162. – La seconde affaire, jugée le 4 novembre 1999 par la Cour d'appel d'Anvers[532], concernait la publication d'un ouvrage dont certains passages avaient été jugés par la personne visée comme une atteinte à sa réputation. En l'occurrence, la Cour anversoise considère également que le principe de la liberté d'expression doit souffrir quelques exceptions : «*Het recht op vrije meningsuiting, gewaarborgd in art. 25 Grondwet en in art. 10, eerste lid, E.V.R.M., is niet absoluut en kan onderworpen zijn aan bepaalde voorwaarden en beperkingen die in een democratische samenleving nodig zijn, o.m. ter bescherming van de goede naam of de rechten van anderen*».

[531] Ce «droit à l'oubli» devrait avoir pour première conséquence que les publications des décisions de justice devraient être anonymes. Sur ce point, l'avis n° 7/96 de la Commission de protection de la vie privée (rapporteur Y. POULLET), *M.B.*, 13 mai 1997 (cet avis a été émis à propos de l'A.R. du 7 juillet 1997 à propos de la publication des arrêts du Conseil d'Etat (*M.B.*, 8 août 1997). A propos de l'atteinte à la vie privée que constitue la divulgation sur décision de la Cour de l'identité et de l'état de santé d'une personne par un arrêt, rendu public dix ans après la décision, voy. C.E.D.H., 25 févr. 1997, *Rev. dr. santé*, 1997-1998, p. 314, note S. CALLENS (aff. *Z. c/ X.*).

[532] Anvers, 4 nov. 1999, *R.W.*, 2000-2001, p. 1457.

La Cour estime qu'une «*ongebreedelde bededinging van mensen in hun privé leven*» représente un abus du droit à la liberté d'expression affirmé par l'article 25 de la Constitution et ne peut être toléré[533].

Enfin, le tribunal civil de Bruxelles le 5 décembre 2000[534] précise les hypothèses de faute en la matière : « *Un journaliste peut commettre une faute soit en publiant des informations fausses sans avoir vérifié avec tous les moyens mis à sa disposition, l'exactitude de celles-ci, soit en livrant au public des renseignements exacts, mais portant atteinte à la vie privée sans que ceci n'ait été nécessaire à la manifestation de la vérité* » (les art. 10 de la Conv. eur. D.H., 19 et 25 de la Const. étant en ce cas en balance avec les art. 8 de la Conv. eur. D.H. et l'art. 18 de la Const.)[535].

§ 2. Légitimité du contrôle par les employeurs de leurs employés lors de l'utilisation du système informatique sur le lieu de travail

163. – C'est sans doute à propos de cette question que le droit de la protection des données et de la vie privée a été le plus invoqué devant les tribunaux. La vidéosurveillance et surtout la collecte par l'employeur des données d'utilisation de l'internet par ses employés, qu'il s'agisse de services de courrier électronique, de services Web, ou autres, peuvent représenter un moyen aisé de preuve de la faute d'un employé et justifier une rupture de contrat. La doctrine[536] s'est largement emparée de la question et deux avis de la Commission de protection de la vie privée, l'un sur les systèmes de vidéosurveillance[537], l'autre sur l'utilisation des systèmes d'information[538], tentent de fixer les principes applicables à la matière. Le Conseil national du travail vient

533 A noter que la Cour se défend d'opérer par là une censure, les mesures prises constituant une «preventieve maatregel meer efficiënte maatregel tegen verdere verspreiding».

534 Civ. Bruxelles, 5 déc. 2000, *A. & M.*, 2001, p. 409.

535 En l'occurrence, nonobstant l'affirmation de ces principes, le juge devait considérer l'action du plaignant non fondée dans la mesure où ce dernier n'était pas clairement reconnaissable pour le public.

536 Parmi de nombreux articles, voy. T. CLAEYS et D. DEJONGHE, «Gebruik van e-mail en Internet op de werkplaats en contrôle dan de werkgever», *J.T.T.*, 2001, pp. 121 et s.; P. DE HERT, «Schending van het (tele)communicatiegeheim in het beroepsleven», *T.S.R.*, 1995, pp. 213-293; J. DUMORTIER, «Internet op het werk : controlerechten van de werkgever», *Oriëntatie*, 2000, pp. 35-42; J. DUMORTIER, «Little brother is watching you – Mag de werkgever het Internetgebruik van zijn werknemers controleren ?», in *Liber amicorum Prof. Dr. Roger Blanpain*, Brugge, Die Keure, 1998, pp. 243-259; F. HENDRICKX, *Privacy en arbeidsrecht*, Brugge, Die Keure, 1999, 358 p.; F. LAGASSE, «La vie privée et le droit du travail», *Soc. Kron.*, 1997, pp. 417-435.

537 L'avis n° 34/99 déjà cité (note 482) relatif à la vidéosurveillance abordait explicitement cette question.

538 Avis n° 10/2000 du 3 avril 2000, consultable sur le site de la Commission (<http://www.privacy.fgov.be>).

de les entériner par l'adoption, le 26 avril 2002, de la convention collective de travail n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électroniques en réseau[539].

Les principes qui guident le dernier avis de la Commission de protection de la vie privée nous serviront de fil conducteur dans l'analyse de la jurisprudence.

Le premier est celui de la légitimité de ce type de contrôle. La Commission semble considérer comme légitime le contrôle par l'employeur de l'activité des employés et ce nonobstant les prescrits tant de l'article 109*ter* D de la loi du 21 mars 1991[540] que de l'article 314*bis*, § 1, du Code pénal[541]. En particulier, le premier prescrit interdit à quiconque, sauf autorisation de toutes les personnes directement ou indirectement concernées par l'information», «*de prendre frauduleusement connaissance de l'existence de signes, de signaux, d'écrits, d'images, de sons ou de données de toutes natures transmis par voie de télécommunications, en provenance d'autres personnes et destinées à celles-ci ou de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne* (...)».

Certaines décisions s'attardent à démontrer que ces prescrits ne sont point d'application. Ainsi, dans une décision du 22 juin 2000[542], le tribunal du travail rejette l'application de l'article 314*bis* au motif que l'envoi de photographies pornographiques par un employé à une de ses collègues ne peut être considéré comme une communication privée dans la mesure où ni l'émetteur ni le destinataire ne faisaient mystère de l'envoi[543].

En outre, tant l'application de l'article 314*bis* que celle de l'article 109*ter* D se voient repoussées par les juges aux motifs, premièrement, que l'enregistrement des données repose sur un motif légitime, à savoir l'exécution de l'article 16 de la loi sur le contrat de travail[544] et, secondement,

539 Il s'agit de la convention collective n° 81. Celle-ci reprend les points principaux de l'avis de la Commission de protection de la vie privée.

540 Le texte initial a été modifié par la loi du 30 juin 1994 (art. 13, § 2, 1°).

541 L. 30 juin 1994 concernant la protection de la vie privée contre l'écoute, la prise de connaissance et l'enregistrement de communications ou télécommunications privées (*M.B.*, 24 janv. 1995). La Commission note dans son avis déjà cité l'existence de cet article mais n'ose aborder le problème délicat de la légalité des interceptions des communications à l'intérieur de l'entreprise au regard de ce texte.

542 Trib. trav. Bruxelles, 22 juin 2000, *Computerr.*, 2001/6, p. 310 : «Het ging eerder om een 'publiek geheim' dan een vertrouwelijke privé-communicatie».

543 ... En ce sens égal., même si le moyen nouveau n'avait pu être reçu par la Cour de cassation, le raisonnement tenu par la Cour de cassation le 27 févr. 2002, à propos de la vidéosurveillance secrète d'une employée.

544 Qui prescrit le devoir des travailleurs et employeurs, d'une part, au respect et aux égards mutuels et, d'autre part, au respect des convenances et des bonnes mœurs.

que l'interception présente un caractère d'urgence et l'unique moyen pour protéger des intérêts[545] supérieurs.

Le tribunal correctionnel de Louvain[546] estime pour sa part que le travailleur, par l'existence même de son contrat de travail, autorise implicitement l'employeur à contrôler l'utilisation par celui-là des moyens électroniques mis à sa disposition.

Le fait que ce contrôle et cette ingérence ne constituent pas des infractions pénales ne suffisent pas à les légitimer. Comme le note le juge bruxellois dans sa décision déjà citée du 22 juin 2000 et, par ailleurs, dans celle du 2 mai 2000[547], il s'agit de concilier le droit du travailleur au respect de sa vie privée fondé sur l'article 8 de la Convention européenne des droits de l'homme[548] et le droit de l'employeur au contrôle des prestations de travail fondé sur les articles 16 et 17 de la loi du 3 juillet 1998 sur le contrat de travail.

Ainsi, même fondés sur une loi, les moyens de contrôle doivent, selon la Commission de protection de la vie privée, répondre à des conditions supplémentaires pour être légitimes. La première est celle de la transparence[549]. «*Le dialogue entre employeur et employés devra permettre d'établir de façon suffisamment détaillée, (...) les différentes caractéristiques de la politique de contrôle de l'employeur (...)*».

545 Sur tous ces arguments, le tribunal renvoie amplement à l'argumentation développée dans l'ouvrage de F. HENDRIKX (*op. cit.*, pp. 199 et 200).

546 Corr. Louvain, 22 juin 1998, *A.J.T.*, 1999-2000, p. 233.

547 Trib. trav. Bruxelles, 2 mai 2000, *Juristenkrant*, 2000, liv. 20, p. 1, note R. de CORTE; *Computerr.*, 2001, p. 26, note D. CASAER.

548 «Dat ook werknemers bij het uitoefenen van hun taak hebben op respect voor hun persoonlijke levenssfeer evident is en overigens bevestigd door het Europees Hof voor de rechten van de mesn (arrest Niemietz, E.H.R.M., 16.12.1992, Serie A, vol. 251 – B); toch geldt het recht op privacy niet absoluut» (Cass. 7.10.81, Arr. Cass. 81-82, 1983)» (trib. trav. Bruxelles, 22 juin 2000, précité). Voy. égal. la citation par la décision du 2 mai 2000 de l'attendu de l'arrêt *Niemietz* du 16 déc. 1992, *J.T.*, 1994, p. 65, note E. JAKUBAN et P. LAMBERT, jurisprudence confirmée par les arrêts *Funcke*, *Cremieux* et *Miailhe* du 25 févr. 1993, ce dernier publié dans *Rev. trim. D. H.*, 1994, p. 117, note YERNAULT) : «... le respect de la vie privée doit aussi englober dans une certaine mesure le droit pour l'individu de nouer et de développer des relations avec ses semblables. Il n'y a aucune raison de principe de considérer cette manière de comprendre la notion 'vie privée' comme excluant les activités professionnelles ou commerciales : c'est dans leur travail que la majorité des gens ont beaucoup voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur».

549 L'art. 4, § 1, 1°, prescrit que le traitement doit être loyal. Voy. égal. l'art. 9 qui prescrit un devoir d'information de la personne concernée. A noter que la Commission prône un devoir d'information, voire de consultation collective, conformément à la convention collective n° 39 du 13 déc. 1983 relative à la consultation sur les impacts sociaux de l'introduction des nouvelles technologies, convention déclarée obligatoire par l'A.R. du 25 juin 1984 (*M.B.*, 8 févr. 1984). Il n'est pas sûr que ni la jurisprudence ni la Commission n'admettent que le consentement donné au traitement des données d'utilisation à des fins de surveillance lors de la signature du contrat de travail puisse être considéré comme un consentement libre, fondement légitime d'un tel traitement. En toute hypothèse, si le consentement permettait de fonder la légitimité d'un traitement, resterait le problème de la validité de celui-ci (sur ce point, voy. *infra*, n° 154 *in fine*).

La seconde tient au respect du principe de la finalité. Le contrôle doit ainsi viser exclusivement la prévention d'infractions pénales, la protection des bonnes mœurs[550], voire l'utilisation abusive des moyens de travail[551], mais ce moyen de contrôle, comme le note le tribunal bruxellois le 2 mai 2000, doit être nécessaire et indispensable : «*il faut d'une part que le but ne puisse être réalisé sans le moyen, et d'autre part, qu'aucun autre moyen ne permette d'atteindre ce but*». On note à ce propos que dans la décision précitée, le tribunal, après avoir rappelé la gravité des faits reprochés à l'employé compte tenu de l'intensité des échanges et de leur persistance, considère que «*l'employeur s'est abstenu de tout contrôle sur le travail fourni avant de demander le rapport sur l'utilisation des systèmes d'information par son employé. Cette négligence est d'autant plus inacceptable que l'employeur avait confié une tâche qu'il qualifiait d'importante à l'employé et qu'il disposait de moyens de contrôle et que l'employeur était donc normalement en mesure de comprendre le travail du salarié, d'en mesurer l'approvisionnement, et le cas échéant, d'identifier les causes de retard. Le contrôle par l'employé de l'utilisation par les salariés des systèmes d'information mis à leur disposition ne peut donc qu'être subsidiaire*[552] *ou se justifier par des situations d'urgence. En outre, il doit, comme l'affirme la Commission de protection de la vie privée, être ponctuel et justifié par des indices laissant suspecter une utilisation abusive des outils de travail*». C'est ce que la Cour de cassation rappelle implicitement dans son arrêt du 27 février 2001[553] lorsqu'elle approuve l'installation par l'employeur d'un système caché de vidéosurveillance pour surprendre une employée, caissière, déjà soupçonnée de divers vols. «*Dat deze verdragsregels (art. 8, lid 1. EVRM) met ervan in de weg staat, dat een werkgever, op grond van een gewettigd vermoeden van betrokkenheid van zijne werknemer bij te zijnen nadele gepleegde misdrijven, maatregelen neemt om door middel van camerabewaking, in een door hem uitgebate, en voor de publiek toegankelijke winkelruim-*

550 Comme c'était le cas dans la décision bruxelloise du 22 juin 2000.

551 «La Commission rappelle que, de même que pour tout autre collecte de données, les données de télécommunications visées ne peuvent être collectées que pour la finalité de contrôle précisée, et ne peuvent être utilisées à des fins différentes» (avis de la Commission de protection de la vie privée précité, p. 3).

552 La Commission ajoute, à juste titre, qu'un contrôle permanent serait contraire à la dignité humaine, voire contreproductif.

553 Cass., 27 févr. 2001, *Computerr.*, 2001, p. 202, note J. DUMORTIER; *AP2T*, oct. 2001, p. 31, note P. DE HERT, «La Cour de cassation ne s'écarte pas du raisonnement tenu par la Cour d'appel de Gent du 2 février 1999» (jugement publié in *AP2T*, 2001, p. 33, note P. DE HERT).

te[554]*, nieuwe strafware feiten te voorkomen of vast te stellen. Dat dergelijke maatregel, voor zover zij de aangifte van de feiten bij de overheid tot doel heeft en, uitgaande van dit doel, toereikend, ter zake dienend en niet overmatig is en geen inmenging inhoudt op de uitoefening van dit recht in de zin van artikel 8 lid 2 EVRM»*[555].

La proportionnalité du contenu des traitements constitue une troisième condition. Même légitimé, le contrôle doit être aussi restreint que possible: le moyen de contrôle n'est plus admissible si des moyens moins nuisibles peuvent réaliser l'objectif[556]. C'est à ce titre que le tribunal bruxellois, dans la décision déjà citée, écarte comme élément de preuve de la faute de l'employé, le dépôt auprès du tribunal des messages proprement dits. «*Le tribunal estime qu'il dispose d'éléments suffisants pour apprécier le motif grave : il connaît le nombre de messages, le moment précis auquel chacun a été expédié ou reçu, leur caractère privé, leur durée approximative et leur objet (...). Le contenu précis de chaque message ne serait pas de nature à mieux informer le tribunal, il n'est donc ni nécessaire, ni indispensable, ni proportionné*».

Il s'agit ici d'une application du principe classique de la proportionnalité du contenu des traitements. La Commission de protection de la vie privée propose, sur cette base, le type de données susceptibles d'être traitées en matière d'utilisation du courrier électronique[557] et celles en matière de consultation de sites web. C'est en effet, comme le note J. DUMORTIER, que l'attente légitime raisonnable («de redelijke privacyverwachtingen») de vie privée n'est pas la même dans ces différents contrats.

[554] Le raisonnement de la Cour eût-il été différent si la caméra avait été placée dans un lieu non ouvert au public comme un lieu de stockage où l'attente légitime de l'employé à ne pas subir de contrôle eût dû être respectée ? On note que la Cour ne fait pas mention de la convention collective de travail n° 68 en matière d'usage de caméras sur les lieux du travail.

[555] La Cour estime qu'aucun devoir d'information préalable n'existait en l'occurrence dans le chef de l'employeur. L'art. 8 de la convention collective n'en impose point. Une telle obligation existerait sur base de l'art. 9 de la loi du 8 déc. 1992. Faut-il en conclure que la Cour, à l'inverse de la Commission belge de protection de la vie privée, estime que le système de vidéosurveillance mis en place ne constituerait pas un traitement au sens de la loi de 1992 (voy. sur ce point, *supra*, n° 148)?

[556] Trib. trav. Bruxelles, 2 mai 2000, précité. Comp. «En ce qui concerne plus précisément la nature des données sujettes à contrôle, seules les données nécessaires à ce dernier peuvent être collectées. Dans la majeure partie des cas, la prise de connaissance du contenu des informations n'est pas nécessaire à l'exercice du contrôle» (Commission de protection de la vie privée, avis n° 10/2000).

[557] En distinguant les courriers entrants et ceux sortants. Pour les premiers, la Commission estime que le droit du contrôle ne s'étend pas à des messages dont un de ses employés n'est pas l'auteur sauf à des contrôles par des moyens techniques n'impliquant pas la saisie des données de trafic (p. ex., blocage de fichiers entrants de grande taille).

La durée de conservation des données ainsi collectées et les mesures de sécurité qui doivent entourer leur stockage font l'objet d'autres considérations de la Commission. La jurisprudence n'a pas encore eu l'occasion de se pencher sur ces questions.

164. – En conclusion, sur une question qui agite l'ensemble des pays européens, la jurisprudence belge a pris une position réaliste, soucieuse d'un équilibre entre les préoccupations légitimes de l'employeur et de l'employé. Elle[558] reprend certes les attendus de la Cour de cassation de France[559] qui avait considéré que «*le salarié a droit, même au temps et au lieu de travail, au respect 'de l'intimité de sa vie privée'; que celle-ci implique en particulier le secret des correspondances; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation professionnelle de l'ordinateur*» mais n'interdit pas un contrôle motivé, proportionnel à la gravité des faits reprochés et strictement limité à ce qui est nécessaire pour l'établissement de ces faits. Sous peine de quoi, les moyens de preuve sont considérés comme acquis de manière illicite et doivent être écartés des débats[560].

IV. – De diverses obligations de transparence mises à charge du responsable du traitement et des divers droits de la personne concernée – Des actions contre le responsable du traitement

A. Les prescrits

§ 1. Les obligations de transparence du responsable du traitement

165. – Le responsable a notamment pour obligation de déclarer les traitements qu'il entreprend auprès de la Commission de protection de la vie privée[561]. On note que nombre de décisions vérifient incidemment

[558] Voy. à cet égard, Civ. Verviers, 20 mars 2002, en cause *D.V. S.A. Creaspeace*, R.G. 811/2000, inédit.

[559] Cass. fr., 2 oct. 2001, *Rev. gén. dr. civ.*, 2002, p. 109.

[560] Voy. à cet égard, C. trav. Gand, 22 oct. 2001, *J.T.T.*, 2002, p. 40, et Civ. Verviers, 20 mars 2002, précité.

[561] A noter dans l'affaire *Gaia* (commentée *supra*, n° 148) le raisonnement du juge qui, après avoir considéré qu'un enregistrement vidéo sur la voie publique était un traitement, en tire la conséquence que les art. 9

l'accomplissement de cette formalité. Le président du tribunal de commerce de Bruxelles estime ainsi : «*Attendu que la formalité de déclaration des traitements est entrée en vigueur le 1er mars 1994; qu'il résulte d'une copie de lettre (...) de la Commission de protection de la vie privée que la défenderesse a fait déclaration du traitement automatisé litigieux et qu'il lui a été attribué un numéro de fichier*»[562], dans le cadre d'une action en cessation menée par Belgacom contre une société éditant un annuaire électronique sur CD Rom.

Par contre, dans l'affaire gantoise déjà analysée[563] ci-dessus, relative à la publication de brochures d'adresses, le tribunal correctionnel constate l'absence de déclaration du traitement. L'infraction était d'autant plus grave que le responsable du traitement avait été interrogé à ce sujet par la Commission de protection de la vie privée.

Dans les deux cas, celui gantois et celui bruxellois, il était reproché aux éditeurs un manquement à l'obligation d'information. Dans l'affaire jugée par la Cour d'appel de Gand, l'éditeur de la brochure affirmait que les données personnelles publiées venaient de sources telles que les annuaires téléphoniques et les registres d'état civil des communes et, dès lors, pouvaient être considérés comme des données publiques[564]. La Cour rejette l'argument au motif, premièrement, que les données publiées contenaient des données complémentaires à celles reprises dans les annuaires téléphoniques et, secondement, que la publication des adresses contenues dans le registre d'état civil est interdite. Il y avait donc lieu d'informer les personnes concernées du traitement opéré. Dans l'affaire bruxelloise, le président du tribunal retient également le devoir de l'éditeur électronique

(obligation d'information de la personne concernée), 16 (obligation de sécurité) et 17 (obligation de déclaration) sont applicables. On notera cependant que certaines exceptions existent comme le rappelle la Cour d'appel de Bruxelles (8e ch.) le 7 mai 1998 (*BVBA Kapitol Trading c/ F. De Man*, R.G. 1998/4429, inédit) (sur cette affaire, voy. nos réflexions *infra*, n° 167) : «Overeenkomstig artikel 8 van het KB n° 13 van 12 maart 1996 dient geen aangifte te worden gedaan voor de verwerking van voor communicatie noodzakelijke identificatiegegevens die enkel worden vericht met de bedoeling met de betrokkene in contact te treden en voor zover die gegevens met aan derden worden meegedeeld».
Cette exception de déclaration a été maintenue par l'A.R. du 13 févr. 2001 (*M.B.*, 13 mars 2001). Sur cet A.R., voy. C. de TERWANGNE et S. LOUVEAUX, *op. cit.*

562 Comm. Bruxelles (prés.), 19 juillet 1995, *J.T.*, 1995, p. 188. A noter que le tribunal rappelle à Belgacom son devoir de déclaration à propos non du traitement que constitue l'édition de l'annuaire téléphonique papier mais à propos des traitements que représente la communication des listes (sur la distinction à opérer entre les différents traitements que constituent les annuaires téléphoniques ou qui sont constitués à partir de ceux-ci, voy. C. de TERWANGNE et Y. POULLET, «Les annuaires téléphoniques au carrefour de droits – Quelques réflexions à propos de décisions récentes», *J.T.*, 1996, pp. 425 et s.).

563 Corr. Gand, 22 janv. 2001, analysé *supra*, n° 150.

564 Pour rappel, l'ancien art. 3, § 2, 3°, de la loi de 1992 prévoyait que les données faisant l'objet d'une publicité légale ou volontaire n'étaient pas soumises à la plupart des prescrits de la loi.

d'informer les personnes concernées non seulement à propos du traitement de base (l'édition électronique de la liste sous forme de CD) mais surtout à propos du traitement dérivé, c'est-à-dire la transmission à des tiers (les acheteurs des CD des listes d'abonnés). Cette obligation présenterait cependant, selon le juge, un caractère vague dans la mesure où la loi ne précise pas les modalités de cette information.

166. – La transmission par les éditeurs électroniques à des tiers des listes d'abonnés, ou plutôt l'utilisation par ces derniers des fichiers édités, et ce pour des finalités propres, soulève une difficulté qui peut s'avérer embarrassante. Les tiers en question sont en principe tenus, puisque, par hypothèse, ils n'opèrent pas dans le cadre d'une collecte de données directement auprès de la personne concernée, d'avertir cette dernière au plus tard lors de leur première utilisation de la donnée. En d'autres termes, chaque personne qui utilise le fichier électronique devrait avertir les personnes concernées dont l'adresse est utilisée de l'existence du traitement qu'il opère. Que le fiché contacté connaisse alors l'identité du responsable du traitement, son existence, ses finalités, voire la source des données traitées, apparaît comme une exigence non disproportionnée. Le but essentiel de la formalité d'information des personnes concernées ne porte pas tant sur la nécessité pour ces dernières de connaître la nature exacte des données enregistrées que sur leur intérêt à pouvoir soit rectifier la donnée le cas échéant erronée, soit s'opposer en connaissance de cause au traitement de leurs données tant auprès du responsable du traitement secondaire qui les a contactées que de la source même de ce traitement, l'éditeur électronique.

C'est pour avoir interprété la loi dans ce sens que l'éditeur d'une revue d'un parti politique extrémiste s'est vu poursuivre par l'éditeur de l'annuaire électronique dont il affirmait s'être servi[565]. En l'occurrence, cet éditeur avait sélectionné les citoyens supposés néerlandophones[566] de la capitale, leur avait envoyé un exemplaire de la revue en mentionnant l'utilisation du CD Rom commercialisé par une entreprise, le numéro de déclaration de cette entreprise et le droit de rectification et d'opposition en même temps que l'identité de l'éditeur de la revue, responsable du traitement. La réaction de l'entreprise éditrice du CD Rom provenait du fait que son nom était associé à celui du parti politique éditeur de la revue. La Cour

565 Même si certains indices montraient que certaines modifications avaient été apportées.

566 Le président décrit la technique utilisée : Belgacom, fichier primaire, utilisé par l'éditeur de l'annuaire électronique, publie en effet les données personnelles dans la langue dans laquelle a été souscrit l'abonnement, ce qui permet de supposer qu'il s'agit de la langue utilisée par la personne.

d'appel de Bruxelles[567] ne peut cependant que constater le respect de la loi : «*Dat de loutere vermelding, aangevuld met het nummer toegekend door de Commissie tot bescherming van de persoonlijke levensfeer en met de identiteit van de beheerder, niet meer dan de herhaling van dit wettelijk recht*».

§ 2. Les droits d'accès et de rectification de la personne concernée

167. – Quelques décisions rappellent aux responsables de traitement leur devoir de répondre aux demandes d'accès des personnes concernées. Ainsi, la décision *Kapitol Trading* du tribunal de première instance de Bruxelles du 7 mai 1998[568] relève que l'éditeur de la revue politique assigné par l'éditeur de l'annuaire téléphonique qui se plaignait d'avoir vu son nom «associé» à la publicité avait, conformément à la loi de 1992, mentionné le droit d'accès des personnes destinataires de la revue à ses fichiers, et ce contre paiement de la somme prévue réglementairement.

168. – Plus intéressante est la décision du même tribunal du 23 avril 1999[569] qui concerne l'accès d'un héritier au dossier médical de son père décédé. Cette demande se heurtait à une fin de non-recevoir du médecin, fondée sur l'obligation de respecter le secret médical[570]. Le tribunal écarte le moyen ainsi invoqué dans la mesure où l'accès était motivé par la volonté de l'héritier de mettre en cause la responsabilité du médecin, compte tenu du fait que l'application de ce secret aurait pour conséquence de soustraire automatiquement le médecin à sa responsabilité professionnelle. Le tribunal conclut dès lors que «*les héritiers et les ayants droit ne sont pas des tiers et peuvent être assimilés à la personne concernée au sens de la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*»[571].

[567] Bruxelles (8e ch.), 7 mai 1998, *BVBA Kapitol Trading c/ De Man*, R.G. 1998/4429, inédit, en appel de Civ. Bruxelles (prés.), 7 mai 1998, R.G. 1998/497/C.

[568] Civ. Bruxelles (8e ch.), 7 mai 1998, R.G. 1998/497/C, en cause *BVBA Kapitol Trading c/ F.De Man*.

[569] Civ. Bruxelles, 23 avril 1999, *Rev. dr. santé*, 1999-2000, p. 353, note M.-H. BOULANGER.

[570] Sur les complémentarités des concepts de «secret médical» et de protection de la vie privée, voy. Y. POULLET, «Le secret professionnel», in *Le secret professionnel* (éd. D. KIGANAHIÉ et Y. POULLET), colloque organisé à Namur, les 5 et 6 nov. 2001, Brugge, La Charte/Die Keure, 2002, pp. 261 et s.

[571] Cette décision rejoint l'accès d'initiative pris par la Commission de protection de la vie privée relatif au droit d'accès des héritiers au dossier médical du défunt (avis n° 18/2000 du 15 juin 2000, rapporteur B. VANLERBERGHE. Voy. égal. l'avis n° 36/95 du 22 déc. 1995 de la même Commission, *Rev. dr. santé*, 1996-1997, p. 163). Le texte de l'avis nous apparaît cependant plus large que celui proposé par le tribunal. En effet, selon l'avis, «les héritiers devraient disposer d'un droit d'accès s'ils poursuivent un intérêt légitime. La Commission est partisane d'un système qui permet l'évaluation des intérêts».

L'arrêt de la Cour d'arbitrage du 23 février 2000[572] concerne notamment le droit d'accès des jeunes en difficulté, de leurs parents ou de leurs avocats aux informations médico-psychologiques et aux informations générées par le directeur ou les conseillers de l'aide à la jeunesse suite à une décision judiciaire, et aux informations judiciaires lorsque les autorités judiciaires apposent la mention «confidentiel» sur celles-ci lors de leur transmission aux services d'aide à la jeunesse. En l'occurrence, la Cour estime que les restrictions au droit d'accès auprès de ces autorités non judiciaires que constituent les services d'aide à la jeunesse, qui sont prévues par le législateur décrétal, satisfont aux conditions prévues par l'article 8.2. de la Convention européenne des droits de l'homme[573].

B. Actions contre le responsable du traitement

169. – En la matière, l'analyse de la jurisprudence appelle des considérations diverses[574]. Les premières ont trait aux actions en responsabilité et en particulier à l'évaluation des dommages subis par la personne concernée; les deuxièmes concernent la diversité des actions susceptibles d'être entreprises; enfin, les troisièmes évoquent la question controversée des actions collectives.

§ 1. Action en responsabilité civile et données nominatives

170. – L'article 15*bis* de la loi belge du 8 décembre 1992 introduit, à la faveur de la transposition de la directive européenne 95/46, dans notre système juridique belge de la responsabilité quelques confusions. La disposition est en effet ambiguë dans la mesure où elle renvoie à la démonstration qu'un comportement du responsable constitue un acte contraire à

[572] Pour un commentaire de cette decision, voy. P. DE HERT, «Jurisprudence constitutionnelle de la Cour d'arbitrage en matière de vie privée et de publicité de l'Administration – Chronique annuelle 2000», *AP 2-T*, n° 4, p. 11.

[573] A propos de l'application de l'art. 32 de la Constitution et de l'accès aux documents administratifs institué par la loi du 10 juillet 1994 sur la publicité de l'Administration, la Cour se contente de noter (considérant B.8.3.) que le droit d'accès créé par cette loi ne porte pas sur les procès-verbaux et pièces issues d'une information ou d'une instruction judiciaire.

[574] Sur ces points, voy. Y. POULLET et J.-F. LEROUGE, «La responsabilité des acteurs de l'Internet», in *Rapports belges au congrès international de droit comparé*, Brisbane, juillet 2002, Bruylant, pp. 815 et s.

la loi[575]. Or cette démonstration, nous l'avons montré, n'est point aisée et suppose parfois que le juge soit amené à examiner si le comportement du responsable est celui d'un bon responsable.

Peut-être, l'article 15*bis* établit-il à cet égard un renversement de la charge de la preuve mais il apparaît douteux que les juges aillent au-delà et imputent aux responsables de traitement une responsabilité objective. Les décisions prises sous l'empire du texte originaire de la loi de 1992 s'écartent en tout cas d'une telle voie.

171. – L'arrêt déjà examiné de la Cour d'appel de Bruxelles[576] s'interrogeait sur la responsabilité de l'organisme de crédit, ayant dénoncé un défaut de paiement à une centrale de renseignements alors même que les défauts de paiement étaient dus, selon la personne en défaut, à une erreur postale qui l'avait privé de toute information sur les réclamations opérées par l'organisme de crédit. La Cour, dans cette affaire, s'interroge longuement sur les devoirs d'un créditeur prudent et soucieux de vérification des données qu'il détient pour conclure que la personne concernée n'établit pas à suffisance la faute de l'organisme créditeur.

Quant à la faute de la victime, le même arrêt de la Cour d'appel reproche à la personne concernée d'avoir transmis une adresse illisible et de ne s'être point inquiétée du silence prolongé du créditeur[577]. De la même façon, la Cour du travail de Gand, le 16 septembre 1998[578], devait exonérer un organisme de paiement de sécurité sociale de toute responsabilité pour traitement de données inexactes quant au degré d'inaptitude d'un

575 On rapprochera la formulation de l'art. 15*bis* de celle utilisée par les présidents des tribunaux de commerce lorsqu'ils ont à statuer dans le cadre d'actions en cessation pour pratiques de commerce contraires aux usages honnêtes suivant l'art. 93 de la loi du 14 juillet 1991 sur les pratiques de commerce : «La violation 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 et de l'obligation générale de prudence est une pratique contraire aux usages honnêtes en matière commerciale susceptible de porter atteinte aux intérêts d'un vendeur» (Comm. Anvers (prés.), 7 juillet 1994, *D.C.C.R.*, 1994, p. 77, conf. par Anvers, 3 mai 1999, *A.J.T.*, 1999-2000, p. 437).
Ainsi, la condamnation pour «pratique contraire aux usages honnêtes en matière commerciale» comme celle en responsabilité de l'art. 15bis requiert la simple démonstration dans les faits de l'acte contraire à la loi (sur cette jurisprudence des présidents des tribunaux de commerce, voy. la précédente chronique, *J.T.*, 1996, p. 237, n^os^ 78 et s.).

576 *Supra*, n° 159.

577 «Que dans ces conditions, l'absence de réaction dans un premier temps (du responsable) à ce qui pouvait lui apparaître, dans l'état des informations qui lui étaient fournies à ce moment, comme la conséquence d'une négligence originairement commise par la personne concernée, ne présente pas en elle-même un caractère fautif».

578 C. Trav. Gand (7^e^ ch.), 16 sept. 1998, *Chron. dr. soc.*, 1999, p. 277.

handicapé, alors que ce dernier n'avait pas pris les mesures nécessaires à la contestation de telles données inexactes.

172. – La question du dédommagement de la victime à la suite de l'utilisation ou de la communication d'une donnée inexacte, incomplète ou obsolète la concernant, donne lieu à des solutions diverses[579]. Si certains jugements se bornent à noter que le dommage n'est pas prouvé par la victime[580] ou le lien de causalité douteux[581], d'autres évaluent *ex aequo et bono* le dommage moral subi[582].

Certains jugements ajoutent que la publication dans un quotidien, outre le franc symbolique, constitue le mode adéquat de réparation[583]. D'autres préfèrent à une condamnation pécuniaire, une réparation en nature[584].

579 A noter que ce dédommagement ne peut être obtenu dans le cadre d'une action fondée sur l'art. 14 de la loi du 8 déc. 1992, action devant le président du tribunal de 1^ère^ instance siégant comme en référé. C'est du moins l'affirmation du président du tribunal de 1^ère^ instance de Bruxelles dans l'affaire *DATASSUR* (*supra*, n^os^ 153 et s.). Cette affirmation rejoint les réflexions de Th. LÉONARD, obs. sur Civ. Bruxelles (prés.), 22 mars 1994 (aff. *Serwy & Wengler c/ UPC*), *J.T.*, 1994, p. 843.

580 Ainsi, déjà la décision inédite de la Cour d'appel d'Anvers du 26 oct. 1992 (en cause *Van Riel D. c/ De Beroepsvereniging van het Krediet*, R.G. 55.219) citée dans la précédente chronique. Plus récemment, la décision inédite commentée *supra*, n° 28 (Bruxelles (8^e^ ch.), 10 nov. 1998, en cause *BVBA Kapitol Trading c/ F. de Man*) et la décision du tribunal civil de Bruxelles qui estime qu'une publication même fautive dans la mesure où elle concerne une personne non clairement reconnaissable ne peut donner lieu à dédommagement pour cette dernière (Civ. Bruxelles, 5 déc. 2000, *A. & M.*, 2001, p. 409).

581 Ainsi, le seul fait qu'une centrale d'informations sur les mauvais risques dans les secteurs bancaires ou d'assurances renseigne à tort une personne comme fichée, peut-il être considéré comme la cause «évidente et nécessaire» du dommage que constitue le refus de crédit ou de police d'assurance.
La centrale aura tôt fait d'invoquer que l'insuffisance des garanties présentées par le demandeur de crédit ou le candidat souscripteur a pesé plus lourd dans la décision négative que le renseignement inexact transmis par elle.
Ainsi, le tribunal civil de Liège le 11 mars 1987 (*J.T.*, 1987, p. 426) et le président du tribunal civil de Bruxelles le 22 mars 1994 (*J.T.*, 1994, p. 843) évaluent à 50.000 BEF le préjudice. Dans une affaire opposant un employeur et un employé, le tribunal du travail de Bruxelles le 2 mai 2000 (*Computerr.*, 2001, p. 26, note D. CASAER) a, au regard des fautes respectives des deux parties, évalué le dommage en équité à 20.000 BEF.

582 Civ. Namur (1^ère^ ch.), 17 nov. 1997, *J.T.*, 1998, p. 187. *Contra*, la décision de la Cour européenne des droits de l'homme qui estime à propos de la publication par la justice suédoise du nom d'une partie dont l'arrêt révélait qu'elle était atteinte du sida : «Attendu qu'un constat de violation ne saurait constituer une satisfaction équitable et qu'il convient donc de leur accorder une indemnité» (C.E.D.H., 25 févr. 1997, *Rev. dr. santé*, 1997-1998, p. 322).

583 A cet égard, Civ. Liège (prés.), 6 juin 1995, *D.I.T.*, 1996/1, p. 47, note P. WÉRY. En l'occurrence, un éditeur d'annuaires avait omis de mentionner les coordonnées d'un médecin. Le juge a considéré que la mesure la plus adéquate consistait à joindre à chaque facture adressée aux abonnés de la zone concernée un avis reprenant les coordonnées du médecin.

584 Voy., de manière ferme, la décision de la Cour européenne de Strasbourg dans une affaire contre l'Etat belge (C.E.D.H., 14 janv. 1998, *A.J.T.*, 1997-1998, p. 501). En l'occurrence, il s'agissait d'une requête de la L.D.H. contre des mesures de vidéosurveillance jugées contraires à la loi du 8 déc. 1992.

173. – Enfin, on notera la décision en référé inédite du président du tribunal civil de Liège du 30 novembre 1995[585] qui tout en reconnaissant l'utilisation abusive faite par un client de Belgacom des listes d'abonnés au service téléphonique, estime que la résiliation par Belgacom de son contrat avec ce client indélicat constituait une mesure unilatérale constitutive d'un abus de droit. En l'occurrence, Belgacom se targuait pourtant d'une recommandation de la Commission de protection de la vie privée[586] qui établissait clairement la violation par son client des dispositions de la loi de 1992.

§ 2. Diversité d'actions

174. – Nous avons déjà noté dans la précédente chronique l'intérêt qu'ont certains concurrents à utiliser l'action en cessation fondée sur la pratique de la loi de 1992 pour interdire à des entreprises la continuation de pratiques contraires aux dispositions de la loi de 1992.

Un certain nombre d'actions en cessation a ainsi été intenté sur cette base. A leur propos, on note l'étrange attendu du président du tribunal de commerce de Bruxelles[587] appelé à prononcer la cessation d'une pratique d'un concurrent de Belgacom. Ce dernier note que les dispositions de protection des données sont assorties de condamnations pénales et que Belgacom aurait dû dès lors poursuivre le contrevenant devant le juge pénal plutôt que devant le juge des cessations : «*Lorsque le juge compétent s'abstient d'appliquer une disposition légale, le juge des cessations hésite à lui donner effet par le biais d'une action en cessation*».

Cette seconde motivation, même compréhensible, vu le malaise du juge à propos de l'interprétation à donner à l'obligation d'information prescrite par la loi de 1992[588], laisse cependant perplexe. Le raisonnement présidentiel aurait pour effet de diminuer la protection des personnes concernées, puisque le concurrent devrait attendre l'issue de l'action pénale pour faire cesser l'infraction.

[585] En cause *SA CIA Security Alleur Int. c/ SA Belgacom*, R.G. 77/95.

[586] Voy. la recommandation n° 102/93 du 7 sept. 1993.

[587] Comm. Bruxelles (prés.), 19 juillet 1995, *J.T.*, 1995, p. 188.

[588] Voy., à cet égard, notre analyse, *supra*, n°s 165 et s.

§ 3. Action collective

175. – Une décision de la Cour européenne de Strasbourg[589] dans une affaire menée par la Ligue belge des droits de l'homme contre l'Etat belge à propos des mesures de videosurveillance jugées contraires à la loi du 8 décembre 1992, déclare irrecevables les actions intentées par les associations au motif que celles-ci peuvent difficilement se prévaloir d'un préjudice direct suite à la violation subie par un membre de leur association[590]. Sans doute, eût-il été bon de permettre les actions collectives là où souvent les personnes concernées ont quelques hésitations à agir contre le responsable du traitement vis-à-vis duquel elles sont en position de débiteurs, voire de faiblesse.

En ce sens, on notera que la Cour d'arbitrage, dans son arrêt du 23 février 2000[591], semble[592] avoir rejeté le moyen avancé par la Communauté française de déclarer irrecevable le recours de l'ASBL Bureau d'accueil et de défense des jeunes. La Cour estime en effet que cette association est affectée par des dispositions qui limitent l'accès à certaines informations pour des personnes dont elle prétend défendre les intérêts.

V. – Conclusions

176. – La jurisprudence «vie privée» indéniablement s'étoffe. Les décisions se multiplient et les thèmes qu'elles abordent touchent à bien des chapitres de la loi. Les concepts de base sont interprétés; les principes fondamentaux, en particulier celui dit de la légitimité des traitements, le sont de même.

Sans doute les questions, objet de cette jurisprudence, ne sont plus les mêmes : les traitements des banques et des centrales de crédit, objet principal des décisions relatées dans la première chronique, ont cédé la «une» aux questions posées par les traitements des employeurs. Ces dernières ont largement été répercutées par la presse. On notera que ces ques-

[589] C.E.D.H., 14 janv. 1998, *A.J.T.*, 1997-1998, p. 501.

[590] Sur cette question controversée, voy. la note très critique de P. De Hert et O. De Schutter, «Straatsburg. Videosurveillance en het vorderingsrecht van vereiningen», obs. sous C.E.D.H., 14 janv. 1998, *A.J.T.*, 1997-1998, pp. 502 et s.

[591] C. arb., 23 févr. 2000, arrêt n° 21/2000, annoté par P. De Hert, in «Jurisprudence constitutionnelle de la Cour d'arbitrage en matière de vie privée et de publicité de l'Administration – Chronique annuelle», *AP2-T*, n° 4, p. 11.

[592] Les considérants relatifs à cet argument n'ont pas été publiés.

tions naissent des risques nouveaux créés par l'utilisation de l'internet qui hormis le contexte spécifique des relations de travail n'a encore fait l'objet d'aucune autre décision.

177. – La présente chronique couvre *grosso modo* les années 1995 à 2002. La période a été marquée, nous le disions en introduction, par une modification importante de la loi fondamentale en la matière, modification intervenue trop tard pour que la jurisprudence doive déjà faire référence à ce texte nouveau. On notera cependant qu'en particulier sur le principe essentiel de la loi, celui de la finalité légitime, nombre de décisions ont anticipé les solutions nouvelles, voire ont imposé sans attendre le législateur, la solution d'*opt out* voire d'*opt in* en matière de traitement ayant une finalité de marketing commercial.

A ce premier point, on ajoutera l'importance des avis de la Commission de protection de la vie privée. Souvent confirmés par la jurisprudence[593], parfois infirmés[594], ils constituent en tout cas une référence que les plaideurs et les juges prennent volontiers en considération.

La précédente chronique avait insisté sur la diversité des procédures (Cour d'arbitrage, Conseil d'Etat, président du tribunal de première instance siégeant comme en référé, etc.) dans lesquelles le débat relatif à la vie privée intervient. Cette diversité s'est confirmée. En particulier, on avait noté l'utilisation de la violation de la législation vie privée dans des procédures d'action en cessation menées par des concurrents. Cette tendance s'est poursuivie au cours de la période analysée[595]. Cette période ajoute cependant d'autres types de références à la loi de 1992. Ainsi, devant les juridictions du travail, la violation des dispositions de la loi citée a permis dans certains cas le rejet des moyens de preuve apportés par l'employeur pour justifier le renvoi de son employé[596]. Le défaut de légalité du moyen de preuve créé en violation de la loi vie privée a également servi d'argument pour écarter devant une juridiction pénale la prévention d'une infraction[597].

---

593 Sans être exhaustif, voy. à cet égard, la jurisprudence *Gaia*, en matière de vidéosurveillance (*supra*, n° 148), celle relative aux traitements de la sûreté de l'Etat (*supra*, n° 155), aux traitements opérés par les employeurs du fait de l'utilisation des données à caractère personnel (*supra*, n°s 163 et s.), celle *FEBIAC* en matière de répertoire de l'immatriculation des véhicules (*supra*, n° 153), etc.

594 En particulier, la jurisprudence *DATASSUR* (*supra*, n° 11) et l'affaire jugée par le président du tribunal de commerce de Liège le 30 nov. 1995 (*supra*, n° 158).

595 Voy., en particulier, les affaires *FEBIAC* (*supra*, n° 153), *KBC* (*supra*, n° 152) et *Belgacom* (*supra*, n° 165).

596 Voy. *supra*, n°s 163 et s.

597 A cet égard, deux décisions, celle à propos des expertises génétiques (*supra*, n° 157) et celle dans l'affaire *Gaia* (*supra*, n° 148).