Abderraouf Elloumi, "La protection des données à caractère personnel sur l'internet", R.J.L., 2010, n° 2, pp. 9 et s.

LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL SUR L'INTERNET

Abderraouf ELLOUMI
Maître-assistant à la faculté de droit de Sfax

« Un monde gagné pour la technique est perdu pour la liberté »
G. BERNANOS, La France contre les robots, 1944

1. Permettant à l'internaute d'éviter l'encombrement de la circulation, d'économiser le temps, de disposer de possibilités de choix sans limites, d'accéder à n'importe quelle information et surtout d'acheter moins cher, l'internet est devenu un des enjeux politiques et économiques[1], suscitant l'intervention des instances internationales[2] et des législateurs de plusieurs pays dans le monde[3]. Source d'un vacarme jamais connu dans le monde, l'internet présente malgré ses avantages des inconvénients certains. La divulgation à la fois facile et large de l'information a provoqué certains problèmes juridiques relatifs à la protection des données à caractère personnel (D.C.P.)[4]. Une

1 V. L. CADOUX, « Informatique et liberté, en 1997, vers où allons-nous ? éléments de prospective », Gaz. Pal., 1997, 1, doct., p. 645.

2 V. notamment : O.C.D.E., Ligne directrices régissant la protection des consommateurs dans le contexte du commerce électronique, Paris, O.C.D.E., 2000 ; O.C.D.E., Lignes directrices régissant la politique de cryptographie, http://www.oecd.org/dsti/iccp/crypto-f.html ; C.N.U.D.C.I., Loi-type sur le commerce électronique, 21ème session 28 mai – 14 juin 1996, J.D.I., 2, 1997, pp. 394-401 ; O.M.C., Déclaration sur le commerce électronique mondial adopté le 20 mai 1998, http://www.wto.org>.

3 V. par ex. Directive 1999/93/C.E. du Parlement européen et du Conseil du 13 déc. 1999, sur un cadre communautaire pour les signatures électroniques, J.O.C.E., n° L.013 du 19 janv.2000, pp.12-20, disponible aussi sur le site http://www.droit-technologie.org/fr/3_1. asp. legislation-id=11 ; Loi belge du 20 oct. 2000, introduisant l'utilisation des moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, http://www.droit-technologie.org/fr/3_1.asp.legislation_id=54.

4 V. J.-L. SOULIER et S. SLEE, « La protection des données à caractère personnel et de la vie privée dans le secteur des communications électroniques Perspective française », R.I.D.C., 2002, n° 2, p. 663.

statistique précise que plus de 90% des sites web belges collectent des D.C.P.[5] D'après un rapport présenté au congrès américain de la "Federal Trade Commission" (F.T.C.), sur 1400 sites internet américains, seulement 2 % d'entre eux proposent une protection effective des D.C.P.[6] Pour cette raison les politiques adoptées en vue de protéger les D.C.P. ont été qualifiées de « *vaste blague* »[7]. L'atteinte aux D.C.P. a été enregistrée même sur le site du Parlement européen[8]. Ceci montre bien que la toile d'araignée est en train de devenir un vrai cauchemar pour les internautes[9]. La pratique montre que les données collectées pour une finalité bien déterminée sont utilisées dans d'autres fins dont notamment le spamming[10]. Ce genre de comportement a diminué la confiance des internautes et a perturbé le développement des transactions électroniques[11].

2. L'internationalité et l'immatérialité du réseau des réseaux permettent de glaner, stocker et partager les informations[12], ce qui augmente le flux[13] et la mobilité[14] des données. Dans ce contexte, le contrôle du respect des D.C.P. semble être inefficace[15]. Étant donné que toute vie sociale nécessite l'échange

---

5 V. M. WALRAVE, « Protection des données personnelles en ligne : la loi est-elle respectée en Belgique ? », http://www.droit-technologie.org/2_1.asp?dossier_id=92fmotocle, p.1.

6 V. M.-F. TROUSSEAU et G. HAAS, Internet et protection des données personnelles, Paris, Litec, 2000, p.161 ; O. CACHARD, « Le commerce électronique : vers une bipolarité Europe-Etats-Unis ? », D.I.T., 1998, n° 2, p. 66.

7 V. Ph. VALANGENDONCK, « USA : protection de la vie privée en ligne, une vaste blague ? », http:// www.droit-technologie.org/fr/1_2.asp?actu_id=588540009, p. 1.

8 V. E. WERY, « Vie privée sur les sites des autorités européennes peut mieux faire ! », http://www.droit-technologie.org/fr/1_2.asp?actu_id=754822720, p. 1.

9 V. Ph. S. MUNCK, « La distribution sur Internet contrecarrée par la protection du réseau de distribution sélective », note sous C.A. Paris, 14 ch. B, 5 sept. 2003, Com.-Com. Elec., 2004, n° 2, p.37.

10 Le spamming, appelé aussi pollupostage, inondation-réseau et multipostage abusif, « *(...) consiste en l'envoi massif et parfois répété de courriers électroniques non sollicités à caractère commercial à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'Internet (...)* ». V. M. L. CHESTERKINE, « Quelle protection pour l'internaute contre le publipostage informatique ? », P. aff., 2000, n° 38, p. 4.

11 V. B. SALVAS, La protection de la vie privée sur le web avec P3P : L'arrimage incertain du technique et du juridique, Mémoire du Maîtrise en droit (L.L.M.), Université de Montréal, Faculté de droit, 2001, p. 2.

12 Ibid., p. 1 ; J.-L. SOULIER et S. SLEE, article précité, loc. cit. ; A. LUCAS, J. FRAYSSINET, Droit de l'informatique et de l'Internet, Paris, PUF, 2001, p. 8.

13 V. W. JARRAYA, La protection des données personnelles dans le commerce électronique, mémoire pour l'obtention du Master en droit privé, Université de Sfax, Faculté de droit de Sfax, 2004-2005, p. 1.

14 V. A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 13.

15 V.

des D.C.P.[16], la possibilité de collecter ces données et de constituer des bases de données n'est pas une tâche difficile. C'est d'ailleurs pour cette raison que le « *fichage* » a existé même avant l'avènement de l'informatique[17]. Certains supermarchés offrent à leurs clients des cartes de fidélités qui doivent être remplies pour bénéficier d'une réduction importante ou pour obtenir des cadeaux lors de chaque achat. Les données contenues dans ces cartes sont entrées dans une base de données qui déterminera le profil de chaque client. Toutefois, l'internet nécessite plus de protection car en plus des données collectées au su de la personne concernée[18], d'autres sont collectées à son insu. C'est ainsi que lors de chaque accès à l'internet, l'utilisateur laisse des traces[19] qui peuvent être interceptées par les spécialistes. Généralement, lors de chaque connexion les données suivantes sont transmises : l'adresse T.C.P./I.P.[20], la marque et la version du programme de navigation et du système d'exploitation, la langue employée par l'internaute et les sites web consultés[21]. Ces données permettent de faire le lien entre l'internaute et l'ordinateur[22]. En sus de l'adresse I.P. certaines grandes sociétés ont essayé d'implanter « *des identifiants techniques* » dans les microprocesseurs ou les logiciels des ordinateurs et qui

---

كمال العياري، "الحماية القانونية للمعطيات الشخصية"، مجلة القضاء و التشريع، جويلية 2005، ص. 276 و ما بعدها.

16 V. A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 9.

17 V. A. VITALIS, « La protection des renseignements personnels en France et en Europe : approches éthique et juridique », in. Dir., René CÔTÉ, Vie privée sous surveillance : la protection des renseignements personnels en droit québécois et comparé, Québec-Canada, Les éditions Yvon Blais Inc., 1994, p. 177.

18 On peut citer les ex. de données laissées lors de l'accomplissement d'une transaction électronique ou d'un abonnement auprès d'un intermédiaire technique. De même, les D.C.P. peuvent être transmises volontairement en cas d'inscription à un service de liste de diffusion (mailing list) ou en cas d'échanges d'opinions sur les forums de discussion (newsgroups). V.S. LOUVEAUX, « Le commerce électronique et la vie privée », in. CORNELIS Ludo et autres, Le droit des affaires en évolution, Belgique, BRUYLANT, 1999, p. 185 ; A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 15.

19 V. notamment, E. SIMON, « Protection des données sur l'Internet en Hongrie », http://www.droit-ntic.com/pdf/dp_hongrie.pdf, p. 1 ; Th. VERBIEST, « Internet et la difficile protection de la vie privée (chronique " droit et multimédia " de l'Echo) », http://www.droit-technologie.org/1_2.asp?actu_id=254&motcle, p. 3 ; A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 14.

20 Transmission Control Protocol/Internet Protocol, est un nom des protocoles de l'internet qui permet d'identifier l'ordinateur sur le réseau.

21 V. Th. VERBIEST, article précité, pp. 3 et s. ; S. LOUVEAUX, article précité, pp. 185 et s.

22 V. A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 16.

seront par la suite activés sans obtenir le consentement des internautes[23]. Par ces pratiques de traçabilité, l'utilisateur de l'internet devient transparent[24]. L'anonymat qui a été présenté comme l'un des apports de la toile semble être un leurre[25], surtout par l'utilisation des « *cookies* »[26], appelés aussi « *témoins* » ou « *mouchards du réseau* »[27]. Les informations collectées sont utilisées pour dresser le profil du consommateur et ses intérêts[28], c'est-à-dire « *(...) connaître ses centres d'intérêt (...) et ses habitudes de consommation* »[29]. Grâce à ces D.C.P., le professionnel peut « *(...) cibler les consommateurs en fonction des sites visités* »[30]. La collecte de D.C.P., comme les adresses électroniques[31], est devenue une profession très rentable[32]. Servant à la naissance d'une nouvelle activité économique[33], le commerce des D.C.P.[34] a attisé les inquiétudes et a

---

23 Ibid., p. 17.

24 V. Ch. GADDES, « La consécration constitutionnelle de la protection des données à caractère personnel », in. mélanges offerts au doyen Sadok BELAID, Centre de Publication Universitaire, 2004, p. 367 ; A. VITALIS, article précité, p. 117.

25 V. Th. VERBIEST, article précité, p. 1.

26 Le cookie « *(...) est un petit fichier envoyé par le gestionnaire du site sur le disque dur de l'utilisateur. Celui-ci permet d'identifier l'utilisateur lors de sa connexion et de mémoriser celle-ci* », V. M.-P. F. TROUSSEAU et G. HAAS, op. cit., p. 135.

27 V. S. GUINCHARD, M. HARICHAUX et R. de TOURDONNET, Internet pour le droit, Paris, Montchrestien, 2ème éd., 2001, p. 172 ; N. M. POUJOL, La création multimédia et le droit, Paris, Litec, 2000, p. 16 ; Ministère de l'Economie, des Finances et de l'Industrie français, « Le publipostage électronique et les communications commerciales non sollicitées : comment s'en protéger ? », http://www.finances.gouv.fr/cybercommerce, p. 2 ; L. BOCHURBERG, Internet et commerce électronique : Site web. Contrats. Responsabilité. Contentieux, Paris, DELMAS, 2ème éd., 2001, p. 95.

28 V. F. MONEGER et Ph. BISIAUX, « Le commerce électronique sur Internet et protection des données personnelles (Fr.-U.E.) », http://www.juriscom.net/uni/mem/03/index.html, p. 8.

29 M.-F. TROUSSEAU et G. HAAS, op. cit., p. 19.

30 S. LOUVEAUX, articlé précité, p. 188.

31 Une société spécialisée, appelée Alliance Bureautique Service (A.B.S.) a proposé la vente d'un logiciel, "Robotmail", qui permet de collecter les adresses électroniques se trouvant sur les espaces publics du réseau. Ce genre de robot-logiciel aspire d'une manière automatique toute phrase contenant un " a commercial " ou " arobase " (@). Après la collecte, le logiciel permet la prospection des clients. V. sur cette question J. LE CLAINCHE, « Les « pourriels » : le droit dépassé par la technique ? », note sous T.G.I. Paris, 17è ch., 7 déc. 2004, Rev. Lamy droit de l'immatériel, mai 2005, n° 5, p. 28 ; Th VERBIEST, article précité, p. 3.

32 V. M. LAIME, « Allons-nous devoir vendre nos données personnelles », http://www. uzine. net, pp. 1 et s. ; E. WERY, « Faillites des "start-up Internet" : la vie privée est à vendre ! », http://www.droit-technologie.org/fr/1_2.asp?actu_id=962791024, p. 2 ; B. WARUSFEL, « Les entreprise face à la protection des données personnelles : contraintes subies et responsabilités croissantes », R.F.A.P., n° 89, janv.-mars, 1999, p. 114.

33 V. A. VITALIS, article précité, p. 126.

attiré l'attention des gouvernements[35]. Face à « *(...) une machine capable de tout enregistrer et de rien ignorer (...)* »[36], entraînant la perte de l'intimité et des secrets de la personne[37], il est logique d'affirmer que « *(...) la destruction de la vie privée est à l'économie de l'information ce que la destruction de l'environnement est à l'économie industrielle* »[38].

3. L'article 4 de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel[39], définit la notion de D.C.P. comme étant « *(...) toutes les informations quelle que soit leur origine ou leur forme et qui permettent directement ou indirectement d'identifier une personne physique ou la rendent identifiable, à l'exception des informations liées à la vie publique ou considérées comme telles par la loi* ».

L'article 5 de la même loi prévoit que : « *Est réputée identifiable la personne physique susceptible d'être identifiée, directement ou indirectement, à travers plusieurs données ou symboles qui concernent notamment son identité, ses caractéristiques physiques, physiologiques, génétiques, psychologiques, sociales, économiques ou culturelles* ».

La définition des D.C.P. suscite quelques observations :

D'abord, la loi organique emploie la notion de D.C.P., alors que la loi française n° 78-17 du 6 janvier 1978, relative à l'informatique aux fichiers et aux libertés[40] utilise initialement l'expression "*informations nominatives*". La notion choisie par le législateur tunisien semble être meilleure dans la mesure où une information pourrait ne pas être nominative, tout en permettant

---

34 Ce commerce a entraîné le développement des logiciels de croissement (data-mining) et des entrepôts de D.P. (data ware houses) V. A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 18.
35 B. SALVAS, article précité, p. 85.
36 A. VITALIS, article précité, p. 117.
37 V. Ch. GADDES, article précité, p. 367.
38 A. BLLEL, « e-Privacy », Dunod, 2001, cité par M. KORNPROBST, « Internet et les libertés publiques », J.C.P., n° 4, 2002, éd. E., p. 5.
39 J.O.R.T., du 30 juill. 2004, n° 61, pp. 1988 et s.
40 Loi disponible sur le site http://www.lexinter.net/lois/loi_informatique_etlibertes.htm.

l'identification de la personne[41]. La notion de D.C.P. est plus large et donc plus protectrice que celle de donnée nominative. C'est peut-être pour cette raison que la directive du 24 octobre 1995[42] et la loi française du 6 août 2004[43] ont délaissé l'expression "informations nominatives" au profit de celle de D.C.P.

Ensuite, la définition des D.C.P. est large puisqu'elle englobe « *(...) toutes les informations quelle que soit leur origine ou leur forme (...)* ». Les D.C.P. présentées sur support numérique sont donc inclues dans cette définition.

Enfin, la définition donnée par législateur s'applique aux personnes physiques et exclue par conséquent les personnes morales. En Europe, la directive du 12 juillet 2002[44], protège aussi les D.C.P. relatives aux personnes morales.

La doctrine a présenté plusieurs distinctions à la notion de D.C.P. On parle ainsi de D.C.P. directes (état de santé, vie sexuelle…) et de D.C.P. indirectes (adresses, cartes à mémoire…), de D.C.P. ordinaires (nom, prénom…) et de D.C.P. sensibles (origine raciale ou ethnique, idées politiques ou philosophiques…)[45]. Quelles que soient les subdivisions proposées à cette notion[46], il est clair que les D.C.P. sont multiples. Elles englobent ainsi, le nom

---

41 V. L.-X. RANO, La force du droit à l'oubli, mémoire de D.E.A. Informatique et droit, Université de Montpellier 1, Faculté de droit, 2003-2004, p. 9.

42 Directive 95/46/CE 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 de ces données, J.O.C.E., n° L.281 du 23 nov. 1995, p. 31.

43 Loi n° 2004-801, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés, J.O., n° 182 du 7 août 2004, p. 14063.

44 Directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), J.O.C.E., n° L201/37 du 31 juill. 2002.

45 V. A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 10 ;
نادر عمران، "حماية المعطيات الشخصية على ضوء القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004"، مجلة القضاء و التشريع، أكتوبر 2004، ص. 141 و ما بعدها.

46 Notre législateur adopte dans la loi organique n° 2004-63 du 27 juill. 2004, la distinction entre donnée personnelle ordinaire et donnée personnelle sensible. V. débats parlementaires du 21 juill. 2004, n° 34, p. 1282.

et prénom de la personne[47], l'adresse électronique[48], l'image[49], les données bancaires[50], les données passagers (P.N.R.)[51], les données médicales[52]…

4. L'une des questions qui se posent, en ce qui concerne les D.C.P., est celle de savoir s'il existe une différence entre cette notion et celle de vie privée ?

Étant « *changeante* » et difficile à cerner[53], la notion de vie privée a été rarement définie[54]. Même les définitions présentées sont larges[55]. Cette imprécision peut faire croire que les deux notions sont synonymes[56]. S'il est généralement admis que la vie privée[57] englobe le respect de la demeure de l'individu, l'inviolabilité de la personne humaine et la liberté de divulguer ou non les informations la concernant, il est clair que cette notion est plus large que

47 V. C. CREPIN, « Bilan abécédaire 2006 de la protection des données personnelles », http://www.mag-securs.com/article.php3?id:article=6893, pp. 1 et s. ; Ch. GADDES, article précité, p. 366.

48 V. J. LE CLAINCHE, article précité, p. 29.

49 V. arrêt inédit de la Cour de cassation n° 20842/20932 du 22 janv. 2008 ; trib. de première instance de Tunis, jugement n° 56199 du 23 juin 2005 ; trib. de première instance de Sfax, jugement n° 14032 du 20 nov. 2006. V. aussi en France sur la publication des images à partir d'un flux RSS : T.G.I. de Paris ordonnance de référé du 15 décembre 2008, disponible sur le site http://www.legalis.net. V. aussi sur le droit à l'image Ph. BELLOIR, « La protection de l'image publiée sur Internet », http://www.juriscom.net/ pro/visu.php? id=667, pp. 1 et s.

50 V. sur l'affaire SWIFT, DOMAGUIL, « On reparle de SWIFT », http://www.quoideneufeurope.hautetfort. com/archive/, pp. 1 et s.

51 V. E. WERY, « La Cour de Justice va-t-elle interdire le transfert aux autorités US des données des passagers se rendant aux USA ? L'avocat général le suggère », http://www.droit-technologie.org/1_2.asp? actu_id=113&motcle=protection+des+do, pp. 1 et s.

52 V. sur l'affaire Mitterrand

كمال العياري، المقال السابق، ص. 274.

53 V. notamment Ch. GADDES, article précité, p. 368 ; P.-Y. GAUTIER, « Le droit au respect de la "vie privée électronique" est en marche », Com.-Com. Elec., 2002, oct., pp. 3 et s. ;

محمد كمال شرف الدين، "تطور حماية الحياة الخاصة في التشريع التونسي"، المجلة القانونية التونسية، 1997، ص. 27 و ما بعدها ؛ كمال دبش، "الحماية القانونية للحياة الخاصة في القانون التونسي و القانون المقارن"، مجلة القضاء و التشريع، 1998، عدد 10،ص. 122.

54 V. A. COUSIN et C. PICCIO, « Vie privée, liberté d'expression... une presse à la frontière de la légalité ? », Gaz. Pal., 2003, mars-avril, p. 899.

55 V.

كمال دبش، المقال السابق، ص. 122.

56 V. B. MARTINE et P. Ch. MARIE, « Urgent, concepts à clarifier : protection de la vie privée et données personnelles », Droit de l'informatique et des télécommunications, 1998, n° 3, p. 13.

57 V. sur cette notion N. MEZGHANI, La protection civile de la vie privée, thèse, Paris II, 1976, pp. 1 et s. ; F. MECHRI, « L'informatique et la protection de la vie privée », in. Mélanges offerts au Doyen Abdelfattah Amor, Tunis, Centre de publications universitaires, 2005, pp. 781 et s.

celle de D.C.P., qui n'est selon le rapport du Conseil d'Etat français[58] qu'une partie du principe général relatif à la protection de la vie privée[59].

5. La question de la protection de la vie privée en général est ancrée dans l'histoire. Le coran a exigé le respect de la vie privée des personnes à maintes reprises[60]. Cependant, sur le plan juridique, la théorie de la protection de la vie privée est récente puisqu'elle ne date que de la fin du 19ème siècle[61]. Plus récente encore la question de la protection des D.C.P. qui a caractérisé la deuxième moitié du 20ème siècle.

6. Au niveau international, plusieurs textes consacrent la protection de la vie privée ou des D.C.P., comme la déclaration universelle des droits de l'homme de 1948[62], le pacte des Nations Unies relatif aux droits civils et politiques[63], la convention n° 108 qui concerne la protection des personnes à l'égard du traitement automatisé des D.C.P., les lignes directrices de l'O.C.D.E. régissant la protection de la vie privée et les flux transfrontaliers de D.C.P.[64]

Au niveau européen, deux textes doivent être cités, la directive 95/46 du 24 octobre 1995[65], et la directive du 12 juillet 2002 appelée "*directive vie privée*".

---

58 V. Rapport du Conseil d'Etat, Internet et les réseaux numériques, http://lesrapports.ladocumentationfrançaise.fr/BRP/984001519/0000.htm.

59 Même s'il existe une position contraire. V. Rapport Guy BRAIBANT, Données personnelles et société de l'information : Rapport au premier ministre sur la transposition en droit français de la directive 95/46, 3 mars 1998, Documentation française, 1998.

60 يقول الله تعالى في سورة النور الآية 27 :"*يَا أَيُّهَا الَّذِينَ آمَنُوا لاَ تَدخُلُوا بُيُوتًا غَيرَ بُيُوتِكُم حَتَّى تَستَأنِسُوا وَتُسَلِّمُوا عَلَى أَهلِهَا ذَلِكُم خَيرٌ لَّكُم لَعَلَّكُم تَذَكَّرُونَ*"

ويقولُ تعالى في سُورة الحُجُرَات الآية 11:"*يَا أَيُّهَا الَّذِينَ آمَنُوا لاَ يَسخَر قَوْم مِن قَومٍ عَسَى أَنْ يَكُونُوا خَيرا مِنْهُم وَلاَ نِسَاء مِن نِسَاءٍ عَسَى أَنْ يَكُنَّ خَيرا مِنْهُن وَلاَ تَلمزُوا أَنفُسَكُم وَلاَ تَنَابَزُوا بِالأَلقَابِ بِئسَ الاسمُ الفُسُوقُ بَعدَ الإِيمَانِ وَمَن لَّم يَتُبْ فَأُولَئِكَ هُمُ الظَّالِمُون*".

61 V.
محمد كمال شرف الدين، المقال السابق، ص. 27 و ما بعدها.

62 V. l'art. 12.

63 V. l'art. 17.

64 Disponibles sur le site http://www.oecd.org/

65 Directive précitée.

Depuis 1970, les lois relatives à la protection des D.C.P. se sont multipliées partout dans le monde[66].

7. En Tunisie, le code des obligations et des contrats (C.O.C.) ne comporte pas un article général qui consacre la protection des D.C.P. ou de la vie privée. Avant l'avènement des lois spéciales, le recours au régime de la responsabilité civile était une nécessité. Les codes de la presse[67], des télécommunications[68], et pénal[69], la loi n° 98-39 du 2 juin 1998, relative aux ventes avec facilité de paiement[70], la loi n° 2004-5 du 3 février 2004, relative à la sécurité informatique[71] et la loi n° 2005-51 du 27 juin 2005, relative au transfert électronique de fonds[72] ont prévu dans certains articles la protection. Toutefois, la loi du 9 août 2000 relative aux échanges et au commerce électroniques[73] a été la première loi qui a consacré explicitement la protection des D.C.P. Cette protection a été rehaussée au niveau constitutionnel après la modification de la constitution le premier juin 2002[74]. La loi organique en date du 27 juillet 2004 a détaillé cette protection. Depuis la fin des années 90, certains décrets et arrêtés ont été pris et qui concernent le problème de la protection des D.C.P., on doit citer notamment le décret n° 2000-2331 du 10 octobre 2000[75] et les décrets n° 2001-1667 et 2001-1668, du 17 juillet 2001.[76] L'arrêté du ministre des

---

66 V. l'historique de ces lois Ch. GADDES, article précité, p. 370 ; A. LUCAS, J. DEVEZE et J. FRAYSSINET, article précité, p. 41 ; P. BISCHOFF, « L'union européenne et la protection des données. La société de l'information à l'épreuve des droits de l'homme », Rev. du Marché commun et de l'Union européenne, n° 421, 1998, p. 538.

67 V. art. 57.

68 V. arts. 2, 30, 63 et 77.

69 V. spécialement les arts. 199 bis et 199 ter.

70 V. l'art. 14.

71 J.O.R.T. du 3 fév. 2004, n° 10, pp. 242 et s. V. l'art. 9 de cette loi.

72 J.O.R.T. du 11 août 2000, n° 64, pp. 1887-1892.

73 J.O.R.T. du 28 juin 2005, n° 51, pp. 1428 et s. V. l'art. 5 de cette loi.

74 L'art. 9 de la constitution dispose que : « *L'inviolabilité du domicile, le secret de la correspondance et la protection des données personnelles sont garantis, sauf dans les cas exceptionnels prévus par la loi* ».

75 Loi fixant l'organisation administrative et financière et les modalités de fonctionnement de l'agence nationale de certification électronique J.O.R.T. du 24 oct. 2000, n° 85, pp. 2554-2557.

76 Décrets qui concernent respectivement l'approbation du cahier des charges relatif à l'exercice de l'activité de fournisseur de services de certification électronique et la, fixation de procédures d'obtention de

communications du 9 septembre 1997[77] concerne la protection des D.C.P. par l'utilisation du cryptage.

8. Le sujet de la protection des D.C.P. sur l'internet présente un intérêt certain puisqu'il permet de dresser le rapport entre la liberté d'expression et la protection des D.C.P. En pratique, l'une des conditions du développement de l'internet, est la création de la confiance chez l'internaute[78]. Or, cette confiance ne peut être instaurée que si les D.C.P. trouvent une protection adéquate. Par ailleurs, la protection des D.C.P. ne peut être faite par les États seulement, l'initiative des professionnels est une question primordiale et ce à travers plusieurs moyens comme les chartes et les labels[79]. Dans ce contexte, la question qui peut être posée est celle de savoir quelle est la spécificité de la protection des D.C.P. sur l'internet ?

9. L'examen des règles régissant les D.C.P. montre que la protection est assurée à la fois par des principes difficiles à contrôler (**première partie**) et des droits nécessitant la diligence de la personne concernée (**deuxième partie**).

---

l'autorisation d'exercice de l'activité du fournisseur de certification électronique. J.O.R.T. du 27 juill. 2001, n° 60, pp. 1846-1850.

77 Arrêté, fixant les conditions d'utilisation du cryptage dans l'exploitation des services à valeur ajoutée des télécommunications, J.O.R.T. du 23 sept. 1997, n° 76, p. 1799.

78 C. CHASSIGNEUX, « La protection des informations à caractère personnel », in. E. LABBE, D. POULIN, F. JACQUOT et J. F. BOURQUE, Dir., op. cit., p. 183.

79 V. A. SENDRA et G. D. PASANAU, « Quel sort pour les données personnelles dans une faillite de start-up internet ? », http://www.droit-technologie.org/1_2.asp?actu_id=375& motcle, pp. 2 et s.

PREMIÈRE PARTIE

LAPROTECTION PAR DES PRINCIPES DIFFICILES À CONTRÔLER

10. Pour que les D.C.P. soient protégées, le responsable du traitement doit respecter certains principes. Ces principes, qui sont difficiles à contrôler, visent à instaurer la transparence **(A)** et la sécurité dans le traitement des D.C.P. **(B)**.

A- Les principes visant à instaurer la transparence

11. Si la notion de transparence peut être définie comme étant la qualité qui permet de « *(...) laisser apparaître la vérité* »[80], toute opération de traitement des D.C.P. doit être compatible à la vérité déclarée par le responsable.

12. Le traitement des D.C.P. a été défini par le législateur tunisien dans l'article 6 de la loi organique du 27 juillet 2004 comme étant : « *(...) les opérations réalisées d'une façon automatisée ou manuelle par une personne physique ou morale, et qui ont pour but notamment la collecte, l'enregistrement, la conservation, l'organisation, la modification, l'exploitation, l'utilisation, l'expédition, la distribution, la diffusion ou la destruction ou la consultation des données à caractère personnel, ainsi que toutes les opérations relatives à l'exploitation de bases des données, des index, des répertoires, des fichiers, ou l'interconnexion* ».

Cette définition suscite les remarques suivantes :

Premièrement, introduite par l'adverbe notamment, la liste des opérations citées n'est pas exhaustive, ce qui laisse la porte ouverte pour inclure d'autres

[80] N. VIGNAL, La transparence en droit privé des contrats (Approche critique de l'exigence), Thèse, Université de droit d'économie et des sciences d'Aix-Marseille, Institut de droit des affaires, Faculté de Droit de Sciences Politiques d'Aix-Marseille, 1998, p. 17.

opérations, comme l'adaptation, l'extraction, la communication par transmission, la mise à disposition, le rapprochement, le verrouillage et l'effacement[81]. L'élargissement de la définition a été adopté même en jurisprudence[82].

Deuxièmement, le traitement peut concerner *«(...) les opérations réalisées d'une façon automatisée ou manuelle* ». Même si le traitement manuel est concevable, la pratique montre que sur l'internet les opérations sont réalisées d'une manière automatisée, ce qui peut être expliqué par le nombre croissant des D.C.P. collectées. Selon la même définition, le traitement peut être réalisé, soit par une personne physique soit par une personne morale. Si la protection concerne les personnes physiques seulement[83], elle joue contre tout responsable même s'il s'agit d'une personne morale.

Troisièmement, en utilisant les notions d'exploitation et d'utilisation, le législateur semble vouloir protéger les D.C.P. contre le spamming. Cette volonté a été précisée même dans la loi du 9 août 2000[84].

Quatrièmement, la loi organique utilise la notion de collecte sans la définir. Une telle notion a suscité en France un débat à cause de son ambiguïté. Il est permis de se demander si cette opération exige ou non la conservation ou l'enregistrement des D.C.P.[85] ?

---

81 V. l'art. 2-b de la directive du 24 oct. 1995, l'art. 2 de la loi française du 6 janv. 1978, telle que modifiée par la loi du 6 août 2004 et l'art. 2.s de la loi du Luxembourg du 2 août 2002, relative à la protection des personnes à l'égard du traitement des données à caractère personnel, MEMORIAL du Grand-Duché de Luxembourg du 13 août 2002, A- n° 91, pp. 1836 et s.

82 Le trib. de G.I. de Pivas a défini le traitement automatisé comme étant : « *(...) l'extraction, la consultation, l'utilisation, la commercialisation par transmission, la diffusion ou tout autre forme de mise à disposition de D.C.P.* ». V. T.G.I. Pivas, 3 sept. 1997, Expertise, n° 213, mars 1998, p. 79.

83 V. Art. 4 de la loi organique du 27 juill. 2004.

84 V. art. 40 de cette loi.

85 En France, la question a été posée vu l'existence d'un progiciel "Freeprospect" réalisé par une société et qui permet l'envoi des messages dès qu'il trouve une adresse électronique sans que cette adresse soit enregistrée. La question a été donc posée pour savoir si l'ancien article 25 de la loi du 6 janv. 1978 est applicable en l'absence de conservation des D.C.P., V. J. LE CLAINCHE, article précité, pp. 29 et s.

La C.N.I.L. considère que le fait de récupérer une D.C.P., depuis un espace public de l'internet puis l'utiliser est suffisant pour qualifier l'opération de collecte[86]. Cette conception large n'a pas été retenue par le juge qui a adopté une conception stricte, considérant ainsi que la collecte des D.C.P. « *(…) signifie les recueillir et les rassembler, ce qui implique leur enregistrement ou leur conservation dans un fichier* »[87].

En Tunisie, l'absence de définition de la notion de collecte n'empêche pas d'affirmer que même le fait de récupérer une D.C.P. sans la conserver est une sorte de traitement. L'utilisation des notions d'enregistrement et de conservation après celle de collecte prouve ce raisonnement.

13. La transparence[88], facteur indispensable pour la promotion des transactions électroniques, exige que tout traitement des D.C.P. soit loyal. L'article 11 de la loi organique prévoit expressément que : « *Les données à caractère personnel doivent être traitées loyalement (…)* »[89]. La loyauté est un concept « (…) riche de sens mais flou, impliquant une appréciation morale ou éthique autant que juridique, intégrant fortement les faits contextuels »[90]. Selon le vocabulaire juridique[91], la loyauté désigne soit la sincérité contractuelle, soit la bonne foi contractuelle. L'ambiguïté du principe de loyauté montre que le contrôle du respect de ce principe est difficile à effectuer, ce qui a poussé un

---

86 Ibid., loc. cit.

87 V. J. LE CLAINCHE, article précité, loc. cit.

88 L'article premier de la loi organique du 27 juill. 2004 exige expressément la transparence en prévoyant que : « *Toute personne a le droit à la protection des données à caractère personnel relatives à sa vie privée comme étant l'un des droits fondamentaux garantis par la constitution et ne peuvent être traitées que dans le cadre de la transparence, la loyauté et le respect de la dignité humaine et conformément aux dispositions de la présente loi* ».

89 Certains textes juridiques exigent la loyauté et la licéité en même temps. V. art. 6 de la directive du 24 octobre 1995, l'article 2 de la loi française du 6 janv. 1978 et l'article 4-1 de la loi du Luxembourg du 2 août 2002.

90 A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 126.

91 G. CORNU, Dir., Vocabulaire juridique, Paris, P.U.F., 1987, p. 490.

auteur à affirmer que les principes de licéité et de loyauté sont inefficaces[92]. La question reste malgré tout à l'appréciation discrétionnaire du juge.

14. Le principe de loyauté est très connu dans les lois relatives au traitement des D.C.P., qui ont constitué une source d'inspiration à la loi tunisienne[93]. La licéité évoque l'idée de la conformité au droit, c'est-à-dire à l'ordre public et aux bonnes mœurs[94]. Ainsi pour être licite, le traitement doit faire l'objet ou bien d'une déclaration préalable[95], ou bien d'une autorisation[96]. Selon M. Ali KAHLOUN, le principe de licéité signifie que ne peuvent être collectées que les informations nécessaires à la prestation et en cas de collecte elles ne peuvent être utilisées qu'à des fins légitimes ou licites[97]. Cette définition semble confondre entre le principe de licéité et celui de finalité[98].

Malgré son ambiguïté, il est généralement admis que le principe de loyauté exige que toute opération de traitement soit faite avec le consentement de la personne concernée. L'article 27 de la loi organique prévoit que : « *A l'exclusion des cas prévus par la présente loi ou les lois en vigueur, le traitement des données à caractère personnel ne peut être effectué qu'avec le consentement exprès et écrit de la personne concernée ; si celle-ci est une personne incapable ou interdite ou incapable de signer, le consentement est régi par les règles générales de droit (...)* ».

---

92 J. LE CLAINCHE, article précité, p. 30.

93 Selon le ministre de la justice et des droits de l'homme, la Tunisie s'est inspirée dans la rédaction de cette loi organique de 26 expériences des pays développés. V. débats parlementaires sur le projet de loi organique relative à la protection des D.C.P. du 21 juill. 2002, n° 34, p. 1295.

94 G. CORNU, vocabulaire précité, p. 479.

95 V. l'art. 7 de la loi organique et les arts. 3 et s., spécialement les arts. 8 et 9, du décret n° 2007-3004 du 27 nov. 2007, fixant les conditions et les procédures de déclaration et d'autorisation pour le traitement des données à caractère personnel, J.O.R.T. du 30 nov. 2007, n° 96, p. 4039.

96 V. l'art. 8 de la même loi organique et les arts. 3 et s. du décret n° 2007-3004 du 27 nov. 2007, spécialement les arts. 10 à 15.

97 Cet auteur prévoit expressément que :
"*مبدأ الشرعية معنى ذلك أن لا تجمع إلا المعلومات الضرورية للخدمة، و إن جمعت فلا تستخدم إلا في الأغراض المشروعة*" أنظر علي كحلوان، الجوانب القانونية لقنوات الاتصال الحديثة و التجارة الالكترونية، تونس، دار إسهامات في أدبيات المؤسسة، 2002، ص. 355.

98 V. les arts. 10, 11 et 12 de la loi organique.

15. Tout en exigeant le consentement de la personne concernée pour toute opération de traitement des D.C.P., le législateur n'a pas trouvé nécessaire de définir le concept de consentement. L'article 2-h de la directive du 24 octobre 1995 le définit comme étant : « *(...) toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* »[99].

16. Témoignant de l'existence d'un formalisme relatif à la protection des D.C.P., l'article 27 exige le consentement exprès et écrit de la personne concernée[100]. En pratique, l'écrit prévu revêt la forme d'un acte sous seing privé puisque le législateur exige dans le même article la signature de la personne concernée. En cas d'existence d'un enfant le consentement de son tuteur et l'obtention de l'autorisation du juge de la famille sont indispensables[101].

17. Sur l'internet, le responsable du traitement peut rédiger un écrit qui exprime le consentement à ce que les D.C.P. soient traitées et propose aux personnes qui accèdent à son site de donner leur consentement par l'apposition de leurs signatures. L'exigence que le consentement soit fait par écrit n'a pas été prévue expressément par certains textes juridiques étrangers[102]. Si le législateur tunisien se montre attaché à des exigences de forme pour protéger la personne concernée, à travers l'exigence que le consentement soit exprès et écrit, certains textes juridiques exigent des conditions de fond pour que le consentement soit valable. L'article 2-h de la directive du 24 octobre 1995 prévoit que le consentement doit être libre, spécifique et informé. La condition de la liberté est très importante surtout dans le monde de l'internet. La liberté ne se conçoit pas

---

99 L'art. 2-c de la loi du Luxembourg du 2 août 2002 exige en plus que ce consentement soit exprès et non équivoque.

100 Dans ce qui semble être l'un des premiers jugements appliquant la loi organique du 27 juill. 2004 en ce qui concerne la publication des images sur l'internet, le trib. de première instance de Sfax a rappelé cette exigence de l'art. 27 dans sa décision précitée du 20 nov. 2006.

101 Art. 28 de la loi organique.

102 V. l'art. 7 de la directive du 24 oct. 1995 et les arts. 2-c et 5-f de la loi du Luxembourg du 2 août 2002.

avec l'existence d'une pression exercée sur la personne. Ainsi, le consentement ne peut être considéré comme étant libre en cas où l'accès à un site est conditionné à l'acceptation préalable à ce que les D.C.P. soient traitées par le responsable de ce site. Cette pratique est très répandue sur le net. Le problème c'est que le contrôle par le juge du respect de cette condition n'est pas une tâche facile sur le réseau. Le responsable peut alléguer que le consentement n'a pas été obtenu comme condition d'accès aux pages web du site. Étant le propriétaire du site, toute modification ultérieure reste possible pour le responsable du traitement.

18. Le consentement doit aussi être spécifique c'est-à-dire donné à une fin bien déterminée et non pas en termes généraux[103]. Si le traitement avait plusieurs finalités, le consentement peut être sélectif[104], c'est-à-dire que l'internaute consent à livrer ses D.C.P. pour une finalité et non pour les autres[105]. La spécificité du réseau des réseaux c'est qu'il permet que le consentement ne soit pas donné une seule fois pour toute l'opération du traitement. Le responsable du traitement peut demander séparément que l'internaute lui consent à collecter telle ou telle information. Malgré ce processus, le consentement donné reste spécifique puisque l'internaute consent chaque fois à ce qu'une information bien déterminée soit livrée au demandeur.

19. Selon la directive de 1995, il est aussi nécessaire que le consentement soit informé c'est-à-dire donné en connaissance de cause de l'opération de traitement, de ses finalités et des risques qu'elle présente pour les D.C.P. Toutefois, dans une décision du T.G.I. de Paris en date du 7 décembre 2004[106],

---

103 V. S. LOUVEAUX, article précité, p. 195.

104 V. A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 130.

105 L'art. 30 de la loi organique prévoit dans ce sens que : « *Le consentement au traitement des données à caractère personnel sous une forme déterminée ou pour une finalité déterminée ne s'applique pas aux autres formes ou finalités* ».

106 V. commentaire de J. LE CLAINCHE, article précité, loc. cit.

le juge avait précisé que la violation du droit à l'information n'est pas de nature à affecter la loyauté de la collecte[107]. Critiquant cette position, la C.N.I.L. considère que : « *(...) la collecte est déloyale dès lors qu'elle est faite à l'insu de l'intéressé qui n'est alors pas en mesure de faire jouer ses droits et en particulier son droit d'opposition* »[108].

20. Le législateur a insisté sur la condition d'obtention du consentement de la personne concernée dans plusieurs articles[109]. Le non-respect de l'exigence du consentement a été sanctionné par les articles 87 et 88 de la même loi. L'article 29 de la loi organique donne des exceptions à l'exigence de consentement de la personne concernée « *(...) lorsqu'il s'avère manifestement que ce traitement est effectué dans son intérêt et que son contact se révèle impossible, ou lorsque l'obtention de son consentement implique des efforts disproportionnés ou si le traitement des données à caractère personnel est prévu par la loi ou une convention dans laquelle la personne concernée est partie* »[110].

Cet article suscite au moins trois remarques :

D'abord, il ne suffit pas pour exclure l'exigence de l'obtention du consentement que le traitement soit manifestement dans l'intérêt de la personne concernée, encore faut-il que "*son contact se révèle impossible*" ou "*implique des efforts disproportionnés*". Les deux conditions sont cumulatives, ce qui est bénéfique pour la protection des D.C.P.

Ensuite, on peut se demander quand est ce que le traitement est effectué dans l'intérêt de la personne concernée ? Qui va, aussi, juger cette question ?

---

107 Cette position est un peu spéciale puisque la loi du 6 janvier 1978 n'exige pas avant sa modification en août 2004 le consentement de la personne avant le traitement des D.C.P.

108 V. J. LE CLAINCHE, article précité, loc. cit.

109 V. les arts., 44, 47, 49, 62 et 68 de la loi organique.

110 L'art. 7 de la directive du 24 oct. 1995 allonge la liste des exceptions puisqu'il cite, en plus des exceptions prévues par l'article 29 de la loi organique, le cas où le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci, le cas où le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, et le cas où il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement.

Dans le domaine médical le traitement des D.C.P. peut être parfois manifestement dans l'intérêt de la personne concernée[111]. C'est l'exemple du traitement effectué en vue d'identifier les personnes victimes de contaminations virales par transfusions sanguine[112]. Toutefois, dans le commerce électronique il est difficilement concevable que le traitement des D.C.P. soit fait dans l'intérêt de la personne concernée. La question a été posée par les commissions chargées du projet de la loi organique[113], le ministre de la justice et des droits de l'homme avait répondu que c'est le responsable du traitement qui va juger cette question[114] et qu'en cas de litige c'est l'Instance Nationale de Protection des D.C.P. (I.N.P.D.C.P.) qui va le trancher[115].

Enfin, l'expression "*efforts disproportionnés*" suscite aussi quelques interrogations. Une telle expression donne aussi par sa généralité le pouvoir d'appréciation au responsable du traitement, ce qui peut conduire à des abus. Le ministre avait précisé dans une de ses réponses que l'expression signifie, en général, l'existence de grandes difficultés matérielles qui empêchent d'obtenir le consentement de la personne concernée, comme le cas de son existence à l'extérieur du pays ou si son domicile est inconnu ou en cas de situation de santé grave[116]. Tous ces exemples relèvent du monde matériel et ne peuvent être

---

111 Le considérant 31 de la directive du 24 oct. 1995 cite le cas où le traitement « *(...) est effectué en vue de protéger un intérêt essentiel à la vie de la personne concernée* ».

112 V. A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 131.

113 V. débats parlementaires sur le projet de la loi organique, p. 1288.

114 Ceci rend, paradoxalement, le responsable du traitement juge et partie en même temps.

115 La question qui peut être posée dans ce cadre, est celle de savoir la nature juridique de l'I.N.P.D.C.P. S'agit-il d'une autorité administrative ou d'un organe juridictionnel ? La réponse n'est pas facile, puisque d'une part, cette Instance dispose de la personnalité morale et de l'autonomie financière (art. 75 de la loi organique), ce qui la rapproche de l'autorité administrative et d'autre part, l'art. 82 de la même loi organique prévoit que : « *Les décisions de l'Instance sont susceptibles de recours devant la cour d'appel de Tunis*... », ce qui laisse penser qu'il s'agit d'une juridiction spécialisée qui rend des décisions de premier ressort. Les garanties procédurales, données par les arts. 76 et 77 de la même loi organique confirment cette position, même si la composition de l'Instance laisse un peu de doute. V. R. BELGAROUI, L'Instance nationale de protection des données à caractère personnel, Mémoire en vue de l'obtention du diplôme du Mastère en droit public et commerce international, Université de Sfax, Faculté de droit de Sfax, 2008-2009, pp. 18 et s.

116 Ibid., loc. cit.

considérés comme impliquant des efforts disproportionnés, en cas de traitement des D.C.P. sur l'internet. Le risque c'est que dans un monde immatériel l'allégation qu'il y a eu des tentatives pour contacter la personne concernée afin d'obtenir son consentement sans succès est possible. Dans ce cas, la tentative de contacter la personne concernée une ou deux fois sans obtenir sa réponse suffira-t-elle pour caractériser l'existence d'efforts disproportionnés ?

La généralité de l'expression utilisée, avec l'existence d'un monde immatériel dans lequel l'utilisation des astuces est une chose très simple, prouvent la difficulté de contrôler le respect du principe de consentement et donc du principe de loyauté. Ceci peut être confirmé avec l'utilisation de méthodes capables de collecter des D.C.P. à l'insu de l'internaute, comme les cookies. Même si l'utilisation des cookies a été considérée comme étant légitime[117], il est nécessaire que l'internaute soit averti de leur existence[118] et ait le droit de les refuser[119].

21. Le principe de loyauté nécessite pour être instauré l'existence d'un *"maximum de transparence"*[120]. La transparence et la loyauté sont très enchevêtrées, on ne peut avoir un traitement loyal sans la transparence, ni de transparence sans loyauté. La transparence doit régner en ce qui concerne les finalités envisagées au traitement[121]. Le principe de finalité[122] signifie l'obligation à la charge du responsable de traitement d'informer la personne concernée des objectifs du traitement et de s'y conformer. Les finalités du traitement doivent même être précisées à l'I.N.P.D.C.P., si ce traitement

117 V. le considérant 25 de la directive du 12 juill. 2002.
118 V. Th. VERBIEST, article précité, p. 5 ; M. WALRAVE, article précité, p. 5.
119 V. le même considérant 25 de la directive du 12 juill. 2002.
120 L'expression est à S. LOUVEAUX, article précité, p. 193.
121 Ibid., loc. cit. ; A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 126. A. GRUBER, « Le système français de protection des données personnelles », P. aff. , 2007, n° 90, p. 8.
122 Le principe de finalité a été détaillé par le législateur dans plusieurs articles de la loi du 27 juillet 2004. V. les arts. 10, 11, 12, 17, 47, 66 et 94. Le même principe a été prévu dans la loi du 9 août 2000. V. les arts. 16 al. 3 et 39.

nécessite l'obtention d'une autorisation[123]. L'article 10 de la loi organique prévoit que : « *La collecte des données à caractère personnel ne peut être effectuée que pour des finalités licites, déterminées et explicites* »[124].

L'exigence que la finalité soit déterminée et explicite « *(...) renvoi de nouveau à l'idée de transparence (...)* »[125]. La finalité peut être déterminée, mais non explicite. C'est le cas quand le responsable du traitement utilise des termes généraux, vagues ou équivoques.

22. Allant dans une voie plus protectrice, la directive européenne du 24 octobre 1995 exige dans l'article 6-c que les D.C.P. soient « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement* ».

Ces exigences sont de nature à contourner certaines pratiques déloyales qui existent sur la toile d'araignée. Dans le commerce électronique par exemple, certains professionnels exigent pour accomplir la transaction certaines informations qui ne sont pas pertinentes au regard de l'opération envisagée. On peut citer le cas où ils demandent la fourniture d'informations relatives à l'âge de la personne concernée, son statut personnel ou ses revenus[126]. De même, certains professionnels demandent le numéro de carte bancaire, alors que le paiement sera effectué hors ligne[127]. Toutes ces informations sont excessives et non pertinentes. Il semble que le législateur tunisien a voulu protéger la personne concernée contre ces abus en exigeant dans l'article 11 de la loi organique que « *Les données à caractère personnel doivent être traitées*

123 Art. 8 de la loi organique.

124 Presque la même disposition a été prévue dans l'art. 6-b de la directive du 24 oct. 1995. Selon cet article : « *Les États membres prévoient que les données à caractère personnel doivent être : (...)*
b) collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités ».

125 S. LOUVEAUX, article précité, loc. cit. ; Th. VERBIEST, article précité, p. 2.

126 V. S. LOUVEAUX, article précité, p. 197.

127 V.
شراز العطوي، التجارة الالكترونية و حماية المعطيات الشخصية، مذكرة لنيل شهادة الدراسات المعمقة في قانون الأعمال، جامعة تونس للحقوق و الاقتصاد و التصرف، كلية الحقوق و العلوم السياسية بتونس، 2004-2005، ص. 23.

loyalement et dans la limite nécessaire au regard des finalités pour lesquelles elles ont été collectées ».

23. Il est regrettable que la formulation de l'article 11 laisse penser que le critère de nécessité ne joue que lors du traitement effectué après l'opération de collecte. Il était souhaitable qu'un tel critère soit exigé même lors de la collecte des D.C.P. Dans le cadre de la loi du 9 août 2000, l'article 16 alinéa 2 prévoit que : « *Il est interdit au fournisseur de services de certification électronique de collecter les informations non nécessaires à la délivrance du certificat* »[128]. L'exigence de la nécessité dans cette loi ne joue que dans les rapports entre le fournisseur de services de certification électronique et le titulaire du certificat, ce qui a été considéré comme étant lacunaire[129].

24. L'article 12 de la loi organique donne certaines exceptions[130] à l'exigence que le traitement soit effectué dans le cadre des finalités déclarées. Selon un chercheur, l'exigence de l'obtention du consentement de la personne concernée n'est pas une exception puisque : « *Si la personne concernée a donné son consentement c'est qu'il a été déjà informé* »[131]. En réalité, la nécessité d'obtenir le consentement est une exception, car le premier consentement a été donné pour une finalité bien déterminée, l'utilisation des D.C.P. pour une autre finalité est interdite à moins que le responsable du traitement obtienne un nouveau consentement spécifique à la finalité envisagée.

---

128 Presque la même disposition a été réitérée dans l'art. 39 de la même loi.

129 V. A. ELLOUMI, La protection du consommateur dans le commerce électronique, Mémoire pour l'obtention du D.E.A. en droit des affaires, Université de Sfax, Faculté de droit de Sfax, 2001-2002, pp. 92 et s.

130 L'art. 12 prévoit que : « *Le traitement des données à caractère personnel ne peut être effectué pour des finalités autres que celles pour lesquelles elles ont été collectées sauf dans les cas suivant :*
- *si la personne concernée a donné son consentement.*
- *si le traitement est nécessaire à la sauvegarde d'un intérêt vital de la personne concernée ;*
- *si le traitement mis en œuvre est nécessaire à des fins scientifiques certaines* ».

131 W. JARRAYA, mémoire précité, p. 37.

25. Pour contourner le principe de finalité certains professionnels utilisent des termes généraux et déroutants[132]. Ce qui nécessite l'application des sanctions appropriées[133].

26. L'un des grands problèmes que rencontrent les principes déjà étudiés est la difficulté de contrôler leur respect. Comment peut-on, en effet, vérifier le respect des dispositions de la loi, en cas de collecte des données faite à l'insu de la personne concernée ? Dans un tel cas les D.C.P. sont traitées sans que la personne puisse déterminer le responsable. Dans un monde dématérialisé, dans lequel nous sommes tous fichés et tracés, la promotion de la sécurité devient une exigence vitale.

B- Le principe de sécurité des D.C.P.

27. Les D.C.P. collectées doivent être détenues en toute sécurité. L'article 18 de la loi organique prévoit que : « *Toute personne qui effectue, personnellement ou par une tierce personne, le traitement des données à caractère personnel est tenue à l'égard des personnes concernées de prendre toutes les précautions nécessaires pour assurer la sécurité de ces données et empêcher les tiers de procéder à leur modification, à leur altération, ou à leur consultation sans l'autorisation de la personne concernée* »[134].

D'après cet article, même le traitement effectué par le recours à une tierce personne n'exonère pas le responsable de l'engagement de sa responsabilité.

---

132 On peut trouver des exemples comme : « *usage interne* », « *actions commerciales et contractuelles* » et « *vous offrir une meilleure expérience web* ». V. M. WALRAVE, « Protection des données en ligne : amélioration de la protection des données dans les sites Web belge, un an après l'entrée en vigueur de la "nouvelle" Loi Vie Privée ? », http://www.droittechnologie.org/2_1.asp?dossier_id=92&motcle= protection +des+donnees+personnelles&mode=motamot, p. 4.

133 V. art. 94 de la loi organique et 226-21 du Code pénal français. La comparaison des deux textes montre que le législateur français est plus sévère contre la violation des dispositions relatives au respect de la finalité du traitement.

134 Le principe de sécurité a été prévu aussi par les arts. 17 de la directive de 1995, 22 de la loi du Luxembourg du 2 août 2002 et 34 de la loi française de 1978.

L'article 20 alinéa 3 de la loi organique est aussi dans le même sens en prévoyant que : « *Le responsable du traitement et le sous- traitant engagent leur responsabilité civile en cas de violation des dispositions de la présente loi* ».

28. Le responsable du traitement est tenu de prendre "les précautions nécessaires" pour assurer la sécurité des D.C.P. Cette expression, qui montre que le principe de sécurité a un caractère préventif[135], a été détaillée dans l'article 19 de la même loi[136]. Elle vise à empêcher l'intrusion des personnes non autorisées, soit par l'accès aux équipements et installations, soit par la lecture, modification ou déplacement des supports de données, soit même l'introduction ou l'effacement des données. Les D.C.P. doivent être sécurisées contre l'intervention des tiers. La notion de tiers peut poser certains problèmes. C'est pour cette raison que le législateur l'avait défini dans l'article 6 de la même loi. Elle vise « *toute personne physique ou morale ou l'autorité publique ainsi que leurs subordonnés, à l'exception de la personne concernée, le bénéficiaire, le responsable du traitement, le sous-traitant ainsi que leurs subordonnés* »[137].

29. L'un des problèmes d'application des articles 18 et 19 est la difficulté de contrôler le respect du principe de sécurité, surtout en cas de traitement effectué via l'internet. Étant donné que le contrôle par la personne concernée est inconcevable, la seule possibilité reste l'intervention de l'I.N.P.D.C.P. Même si l'article 77 de la loi organique accorde à l'Instance un droit d'investigation, la lourdeur de ses missions[138] et l'aspect technique des mesures de sécurité laissent des doutes sur l'efficacité des contrôles à effectuer. Le doute persiste surtout que le nombre des responsables du traitement augmente d'un jour à l'autre.

---

135 V. A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 163.

136 Cet article reprend presque mutatis mutandis le même contenu de l'art. 23 de la loi du Luxembourg du 2 août 2002.

137 L'art. 2-(r) de la loi du Luxembourg du 2 août 2002 donne des exemples de tiers dans le secteur public comme le ministère, l'administration, l'établissement public et la commune ou un service public.

138 V. l'art. 76 de la loi organique et le décret n° 2007-3003 du 27 nov. 2007, fixant les modalités de fonctionnement de l'instance nationale de protection des données à caractère personnel, J.O.R.T. du 30 nov. 2007, n° 96, p. 4038.

30. Pour faciliter le contrôle du respect du principe de sécurité, l'article 22 de la loi du Luxembourg exige l'établissement d'un rapport annuel sur les mesures techniques prises par le responsable du traitement et qui doit être soumis à la *"Commission nationale"*. La sécurité nécessite non seulement la bonne conservation des D.C.P. mais aussi la destruction de ces données dès l'expiration du délai de la conservation ou la « *(...) réalisation des finalités pour lesquelles elles ont été collectées ou lorsqu'elles deviennent inutiles pour l'activité du responsable du traitement* »[139].

La sécurité exige donc la consécration d'un *"droit à l'oubli"*[140], c'est-à-dire le droit de la personne de voir ses données oubliées après un laps de temps bien déterminé[141]. En réalité c'est l'article 45 de la loi organique qui consacre, sans le dire expressément, ce droit[142].

31. La sécurité des D.C.P. nécessite l'utilisation des mesures techniques[143], ce qui pousse le responsable du traitement à investir et à s'organiser dans un domaine très évolutif. Estimant que l'internet présente plus de risques sur les D.C.P., la C.N.I.L. exige un haut niveau de sécurisation dans le traitement[144] .

32. La sécurité doit être instaurée surtout dans les cas de flux de D.C.P. La loi organique distingue entre le flux interne, appelé communication, et le flux externe, c'est-à-dire vers un pays étranger, appelé transfert de D.C.P. Concernant la communication des données, l'article 47 de la loi organique prévoit un principe et des exceptions. Le principe consiste dans l'interdiction de la communication des D.C.P. « *(...) sans le consentement exprès donné par*

139 Art. 45 de la loi organique.
140 V. L.-X RANO, mémoire précité, pp.1 et s. ; R. LIDON, La création prétorienne en matière de droit de la personnalité et son incidence sur la notion de la famille, Paris, Dalloz, 1974, p. 25.
141 V. le site http://www.parodie.com; W. JARRAYA, mémoire précité, p. 42.
142 Selon W. JARRAYA, ce droit est consacré dans l'art. 24 in. fine et l'art. 26. Or, ces deux articles exigent la destruction des D.C.P. dans des cas extrêmes (Cessation d'activité, décès du responsable ou dissolution de la personne morale). La réglementation de la destruction des D.C.P. dans les cas normaux, et donc la consécration du droit à l'oubli, est faite dans l'art. 45 de la loi organique.
143 V. A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 163.
144 Ibid., p. 166.

n'importe quel moyen laissant une trace écrite ». Consacrant un formalisme protecteur, l'article 47 prévoit deux régimes d'exceptions au principe d'interdiction. Le premier, prévu par le paragraphe premier, ne nécessite pas l'obtention de l'autorisation de l'I.N.P.D.C.P., puisque les données sont communiquées aux autorités publiques. En réalité, cette exception est très large. L'utilisation des expressions "*sécurité publique*", "*défense nationale*" et "*missions dont elles sont investies*" témoigne que le principe a été contourné par ces exceptions.

Le deuxième régime d'exception prévu par le deuxième paragraphe du même article, nécessite l'obtention d'une autorisation de l'I.N.P.D.C.P.[145]

33. Selon l'article 47 paragraphe 2, la communication peut être autorisée par l'I.N.P.D.C.P., lorsqu'une telle communication s'avère nécessaire pour la réalisation des intérêts vitaux de la personne concernée, de ses héritiers ou de son tuteur[146]. Aussi paradoxalement que cela puisse paraître, cette exception consacre un cas où l'I.N.P.D.C.P. connaît plus que la personne concernée ses intérêts ! Le refus de la personne, de ses héritiers ou de son tuteur peut être écarté par une appréciation souveraine de l'Instance. Le pouvoir de celle-ci, est, toutefois, conditionné par "*la réalisation des intérêts vitaux*"[147]. Cette expression est un peu ambiguë. Si les intérêts relatifs à la santé peuvent être considérés comme étant vitaux, il est difficile de concevoir des intérêts vitaux en cas de données collectées lors d'une vente électronique.

---

145 L'exigence de l'autorisation peut être justifiée par le fait que, dans ce deuxième régime, la communication des données n'est pas faite au profit d'une autorité publique.

146 Un autre cas qui permet à l'Instance de donner son autorisation mérite d'être clarifié qui est celui où la communication est nécessaire pour *"l'exécution d'un contrat auquel la personne concernée est partie"*. L'exemple type est celui d'une réservation d'hôtel effectuée par une agence de voyage faite dans un pays tiers au profit d'un client. V. S. LOUVEAUX, article précité, p. 202.

147 Il est légitime de se demander quelle est la différence entre cette expression et celle prévue dans l'art. 29 de la même loi, qui prévoit que le consentement de la personne concernée n'est pas exigé pour le traitement des D.C.P. « *(...) lorsqu'il s'avère manifestement que ce traitement est effectué dans son intérêt (...)* ». La condition prévue dans l'art. 47 al. 2 est plus stricte que celle prévue dans l'art. 29, même si le législateur emploie dans ce dernier article l'adverbe "*manifestement*". Les intérêts de la personne ne sont pas, en effet, tous vitaux.

34. En ce qui concerne le transfert des D.C.P., l'article 51 de la loi organique prévoit que : « *Le transfert vers un autre pays de données personnelles faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement, ne peut avoir lieu que si ce pays assure un niveau de protection adéquat apprécié au regard de tous les éléments relatifs à la nature des données à transférer, aux finalités de leur traitement, à la durée du traitement envisagé, et le pays vers lequel les données vont être transférées ainsi que les précautions nécessaires mises en œuvre pour assurer la sécurité des données. Dans tous les cas, le transfert des données à caractère personnel doit s'effectuer conformément aux conditions prévues par la présente loi* ».

35. La lecture de cet article permet de dégager les remarques suivantes :

Premièrement, le législateur exige, pour le transfert des données, que le pays vers lequel ces données sont transférées assure *"un niveau de protection adéquat"*[148]. La loi n'a pas donné une définition de la notion de protection adéquate, elle a, cependant, précisé les critères de son appréciation, comme la nature des données, les finalités et la durée du traitement, le pays destinataire de ces données et les mesures de sécurité adoptées[149]. Il est clair que le terme "*adéquat*" ne peut être assimilé à celui d'"*équivalent*", qui a été proposé initialement dans le projet de loi française du 6 août 2004, mais a été rejeté [150].

Deuxièmement, la question qui se pose est celle de savoir qui est la partie compétente de juger qu'un pays assure ou non une protection adéquate ?

---

148 L'art. 68 de loi française du 6 août 2004 avait remplacé le terme "*adéquat*" par celui de "*suffisant*".

149 L'art. 25 al. 2 de la directive donne presque les mêmes critères d'appréciation en ajoutant, toutefois, les règles professionnelles. Cet article prévoit ainsi : « *Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données ; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées* ».

150 V. P. LECLERCQ, « Loi du 6 août 2004 Les transferts internationaux de données personnelles », Com.-Com. Elec., 2005, fév., p. 31.

Il découle de l'article 52 que c'est l'I.N.P.D.C.P. qui est compétente en la matière[151]. Toutefois, le dernier alinéa de cet article prévoit que : « *Lorsque les données à caractère personnel à transférer concernent un enfant, la demande est présentée au juge de la famille* ». Le juge de la famille aurait-il le pouvoir de refuser d'accorder une autorisation au motif que tel ou tel pays n'accorde pas une protection adéquate aux D.C.P. ? La question reste posée surtout en cas où l'Instance aurait permis le transfert vers ce même pays.

Troisièmement, l'utilisation de l'expression *"niveau de protection adéquat"* a été critiquée par certains auteurs qui considèrent que le terme "adéquat" n'accorde pas une protection suffisante aux personnes intéressées. Selon eux, c'est la protection équivalente qui est la seule capable de préserver les droits des personnes[152]. À l'inverse, d'autres auteurs précisent que le terme utilisé est de nature à bloquer le flux de D.C.P. et par conséquent le commerce électronique[153].

Quatrièmement, l'article 51 exige que le *"niveau de protection adéquat"* soit assuré par le pays vers lequel les données vont être transférées. Le problème, c'est que, sur le web, la régulation des difficultés ne peut être la tâche de l'État seulement. L'autorégulation par l'intervention des initiatives privées et des règles professionnelles, tels que les codes de bonne conduite, les chartes de sécurité et la labellisation des sites, prouve que l'appréciation de la protection accordée ne peut se baser sur les règles édictées par l'État uniquement[154]. On peut concevoir l'absence de règles protectrices des D.C.P. dans un État bien

---

151 En Europe, c'est la Commission européenne qui est compétente. Elle prend une décision appelée « *décision d'adéquation* ». La commission avait ainsi reconnu que la Suisse, la Hongrie, l'Argentine, le Canada, l'Ile de Man, les États-Unis…présentent un niveau de protection adéquat. V. Ch. TORRES, « Flux transfrontalières de données : convention ou règles internes ? », Gaz. Pal., juill. 2006, p. 2277 ; J.-L. SOULIER et S. SLEE, article précité, p. 671.

152 V. P. BISCHOFF, article précité, p. 541.

153 Ibid., loc. cit.

154 C'est, peut-être, pour cette raison, que l'article 25 al. 2 de la directive européenne de 1995 cite parmi les critères d'appréciation de la protection adéquate "*les règles professionnelles*".

déterminé, alors que les données vont être transférées à une société qui propose par sa propre initiative une protection adéquate de ces données[155]. L'inverse est aussi vrai, l'État peut édicter des règles qui assurent une protection adéquate, alors que la société, vers laquelle les D.C.P. vont être transférées, ne respecte pas ces règles. L'article 51 pose aussi quelques problèmes en cas de transferts multiples. Vu le caractère international du réseau des réseaux, les D.C.P. peuvent se déplacer d'un pays à l'autre jusqu'à ce qu'elles arrivent à un État qui n'assure pas un niveau de protection adéquat. Ceci prouve encore une fois la difficulté de contrôler le respect des principes qui tendent à protéger les D.C.P. sur l'internet.

Cinquièmement, le législateur exige pour le transfert des D.C.P. l'obtention "*dans tous les cas*" d'une autorisation[156] de l'I.N.P.D.C.P.[157] Il est clair que le législateur recourt de plus en plus au formalisme pour assurer la sécurité des données[158].

36. Après les évènements du 11 septembre 2001, les États-Unis avaient adopté une loi appelée l'« *Activation and Transportation Security Act* » du 19 novembre 2001 pour lutter contre le terrorisme. Cette loi oblige les compagnies aériennes qui utilisent le sol américain de transmettre aux autorités américaines les D.C.P. des voyageurs[159]. La question qui s'est posée est de savoir si les États-Unis adoptent ou non une protection adéquate ?

---

155 V.

كمال العياري، المقال السابق، ص. 168.

156 Contrairement à la communication des D.C.P. aux autorités publiques qui n'exige pas l'obtention d'une autorisation. V. art. 47 al. premier.

157 V. art. 52 de la loi organique et l'art. 11 al. 3 du décret n° 2007-3004 du 27 nov. 2007.

158 Ce formalisme peut être facilement constaté à travers l'examen des articles du décret n° 2007-3004 du 27 nov. 2007.

159 V. E. BARBRY et V. LEPERLIER, « Le transfert des données passagers vers les Etats-Unis face à l'impératif de protection des données personnelles », Gaz., Pal., 2004, janv.-fév., p. 88.

S'attachant plus à l'autorégulation, les États-Unis accordent moins d'importance à la réglementation étatique[160]. Pour cette raison, l'Europe avait entretenu des négociations avec les autorités américaines pour parvenir à un accord permettant aux D.C.P. d'être transférées aux États-Unis en toute sécurité. Après de longues discussions, la Commission européenne a rendu une décision reconnaissant que les principes du "*Safe-Harbour*"[161] présentent un niveau de protection adéquat[162]. Constituant un arrimage entre la loi et l'autorégulation[163], le "*Safe-Harbour*" regroupe plus de 200 entreprises qui ont accepté d'adhérer volontairement aux règles protectrices de D.C.P.[164] Toutefois, le respect des règles retenues reste contestable. Le terme "*adéquat*", donné à la protection présentée par les entreprises américaines, a été même critiqué[165]. Ce qui montre que la garantie d'une sécurité absolue des D.C.P. transférées est presque impossible sur l'internet.

37. Le contrôle du respect des sociétés, vers lesquelles les données sont transférées, des principes et des règles prévues est très difficile. Cette difficulté devient une impossibilité en cas de données collectées à l'insu de la personne concernée. Les règles juridiques ne peuvent assurer qu'une protection partielle. Face au phénomène de collecte *"sauvage"*, il est nécessaire de recourir à la technique pour pallier l'insuffisance des règles de droit. Un tel recours est indispensable pour que la personne concernée puisse exercer ses droits.

---

160 V. Th. VERBIEST, article précité, p. 5.

161 Le *"Safe Harbour"*, appelé aussi *"sphère de sécurité"* est un dispositif contenant les conditions d'adhésions volontaires des entreprises américaines aux principes de protection des D.C.P., avec l'intervention de la *"Federal Trade Commission"* pour préserver l'effectivité des règles retenues. Toute entreprise adhérant à ce système serait présumée assurée un niveau de protection adéquat. V. P. LECLERCQ, article précité, p. 32 ; Th. VERBIEST, article précité, p. 6 ; Ch. TORRES, article précité, loc. cit.

162 Décision de la Commission du 26 juill. 2001. V. le site http://www.europa.eu.int/com/ internal_market/en/ dataprot/news/decision_fr.pdf .

163 V. B. SALVAS, mémoire précité, pp. 82 et s.

164 V. P. LECLERCQ, article précité, loc. cit.

165 Ibid., loc. cit. ;

كمال العياري، المقال السابق، ص، 270.

DEUXIEME PARTIE

LA PROTECTION PAR DES DROITS NÉCESSITANT LA DILIGENCE DE LA PERSONNE CONCERNÉE

38. Le caractère international et immatériel de l'internet exige de la personne concernée la diligence pour pouvoir exercer ses droits soit lors de la collecte **(A)** soit lors la conservation des D.C.P. **(B)**.

A- Les droits exercés lors de la collecte des D.C.P.

39. Pour que le traitement des D.C.P. soit licite, loyal et transparent une autre exigence doit être faite, qui est celle de garantir aux personnes concernées un droit à l'information[166]. Ce droit se distingue de l'obligation d'information à la charge du professionnel, lors d'une transaction électronique[167]. Il se distingue aussi de l'obligation d'information de l'I.N.P.D.C.P., que ce soit en cas de la déclaration préalable[168], ou en cas de l'autorisation[169].

40. L'alinéa premier de l'article 31de la loi organique de 2004 prévoit que l'information doit être faite « *(...) par n'importe quel moyen laissant une trace écrite (...)* » [170]. L'exigence de la forme écrite a pour but de protéger la personne

---

166 V. J. LE CLAINCHE, article précité, p. 30 ; S. LOUVEAUX, article précité, p. 203.

167 V. l'art. 25 de la loi du 9 août 2000 ; A. ELLOUMI, mémoire précité, pp. 17 et s.

168 V. l'art. 7 de la loi organique qui consacre, en réalité, une autorisation déguisée puisqu'il permet à l'Instance de s'opposer au traitement des D.C.P.

169 V. l'art. 8 de la même loi organique.

170 L'art. 31 prévoit que : « *Après l'expiration du délai fixé par l'article 7 de la présente loi pour l'opposition de l'Instance, il faut informer au préalable et par n'importe quel moyen laissant une trace écrite les personnes concernées par la collecte des données à caractère personnel de ce qui suit :*
-la nature des données à caractère personnel concernées par le traitement ;
-les finalités du traitement des données à caractère personnel ;
-le caractère obligatoire ou facultatif de leur réponse ;
-le nom de la personne physique ou morale bénéficiaire des données, ou de celui qui dispose du droit d'accès et son domicile ;
-le nom et prénom du responsable du traitement ou sa dénomination sociale et, le cas échéant, son représentant et son domicile ;
-leur droit d'accès aux données les concernant ;

concernée contre toute forme d'abus. Toutefois, il est regrettable que le législateur ne détermine pas la sanction civile applicable en cas de non-respect des dispositions de cet article[171].

Il est curieux de constater que le législateur répète dans le dernier alinéa de l'article 31 la même exigence tout en donnant l'exemple d'une notification effectuée par lettre recommandée avec accusé de réception. Il existe une différence entre la rédaction arabe de l'article 31, qui parle dans le dernier alinéa de l'information et la rédaction française du même article qui utilise la notion de "*notification*". La différence entre les deux versions est patente. Le professionnel peut, en effet, en se basant sur la version arabe informer la personne concernée par l'exposition des données sur son site sans qu'il soit tenu de notifier l'information, opération plus coûteuse et plus complexe.

41. Pratiquement, l'information doit être effectuée dans la première page en utilisant des fenêtres successives. L'existence des pages web contenant l'information est un moyen concevable. L'utilisation des techniques permettant d'enregistrer l'adresse I.P. de l'ordinateur de chaque internaute accédant à l'information, permet de réaliser la condition de "*laisser une trace écrite*".

42. L'information prévue dans l'article 31 doit être effectuée « *(...) dans un délai d'un mois au moins avant la date fixée pour le traitement des données à caractère personnel* ». Le responsable du traitement peut être libéré de l'exigence du délai si les informations sont disponibles d'une façon permanente sur son site. D'ailleurs, peut-être pour cette raison, la loi du Luxembourg

---

-leur droit de revenir, à tout moment, sur l'acceptation du traitement ;
-leur droit de s'opposer au traitement de leurs données à caractère personnel ;
-la durée de conservation des données à caractère personnel ;
-une description sommaire des mesures mises en œuvre pour garantir la sécurité des données à caractère personnel.
La notification s'effectue par lettre recommandée avec accusé de réception ou par n'importe quel moyen laissant une trace écrite dans un délai d'un mois avant la date fixée pour le traitement des données à caractère personnel ».

[171] L'art. 87 de la loi organique prévoit, toutefois, une sanction pénale qui consiste dans l'emprisonnement de deux ans et d'une amende de dix mille dinars.

exonère le responsable du traitement du respect du délai d'information en cas où la personne concernée « *(...) en a déjà été informée* »[172]. La détermination du moment de l'information a pour but de permettre à l'intéressé d'exercer ses droits[173].

L'article 26 de la loi du Luxembourg du 2 août 2002 fait une distinction entre les D.C.P. collectées auprès de la personne concernée (collecte directe)[174] et celles qui n'ont pas été collectées auprès de cette personne (collecte indirecte). Dans le premier cas, l'information doit être faite au plus tard lors de la collecte, alors que dans le deuxième cas l'information doit être fournie « *(...) dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données* ».

Le délai d'un mois prévu par l'article 31 de la loi organique doit être compté avant la date fixée pour le traitement des données. En réalité, il était plus précis de parler de collecte et non de traitement, car comment le responsable pourrait-il faire le traitement s'il n'a pas collecté les D.C.P. auparavant.

43. Contrairement à l'article 31, qui ne donne pas des exceptions aux droits de l'information, l'article 11-2 de la directive de 1995[175] et l'article 27 de la loi du Luxembourg[176] prévoient certaines exceptions. Parmi les exceptions prévues

---

172 Art. 26-1 de la loi du 2 août 2002.

173 V. J. LE CLAINCHE, article précité, p. 30.

174 La loi française du 6 janv. 1978 ne consacre le droit d'information que dans le cas de collecte directe des D.C.P. V. N. M. POUJOL, La création multimédia et le droit, Paris, Litec, 2000, p. 61.

175 L'art. 11-2 de la directive prévoit que : « *Le paragraphe 1 ne s'applique pas lorsque, en particulier pour un traitement à finalité statistique ou de recherche historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément l'enregistrement ou la communication des données. Dans ces cas, les États membres prévoient des garanties appropriées* ».

176 L'art. 27 (1) prévoit que : « *L'article 26, paragraphes (1) et (2), ne s'applique pas lorsque le traitement est nécessaire pour sauvegarder :*
(a) la sûreté de l'État ;
(b) la défense ;
(c) la sécurité publique ;

par ce dernier article, figure le cas où l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés. En pratique, on peut concevoir la collecte par le responsable du traitement des D.C.P. à partir des espaces publics du web sans avoir par la suite la possibilité de contacter les personnes concernées[177].

44. Le lux de détail du contenu de l'information prévu dans l'article 31 de la loi organique montre bien le souci du législateur de protéger les personnes concernées. Toutefois, les statistiques présentées[178] montrent qu'en réalité la diligence de la personne concernée est indispensable pour le respect du droit de l'information. Tout manquement à ce droit doit être déclaré, surtout à l'I.N.P.D.C.P. La personne concernée peut aussi exiger la présence d'un label qui garantit le respect par le responsable du traitement du doit d'information.

45. Parmi les informations exigées par le législateur dans la loi organique, figure l'information sur le droit d'opposition[179]. Un droit d'opposition ne peut être réel que si la personne concernée a été informée du traitement[180]. Considéré comme étant « *(...) le seul moyen pour la personne concernée de se prémunir contre les possibilités de téléchargement de bases de données et le détournement de leur finalité (...)* »[181], le droit d'opposition nécessite lui aussi la diligence de la personne concernée pour garantir son effectivité. L'article 42 de la loi organique prévoit que : « *La personne concernée, ses héritiers ou son tuteur, a*

(d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment, ou le déroulement de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi ;
(e) un intérêt économique ou financier important de l'État ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal ;
(f) la protection de la personne concernée ou des droits et libertés d'autrui ».

177 V. S. LOUVEAUX, article précité, p. 205.

178 Après un an de l'entrée en vigueur de la nouvelle loi belge "*Vie privée*", seulement 74% des sites web belges communiquent le nom du responsable du traitement et 88 % communiquent la finalité du traitement. V. M. WALRAVE, article précité, p. 4.

179 V. J.-L. SOULIER et S. SLEE, article précité, p. 668.

180 V. S. LOUVEAUX, article précité, p. 206.

181 A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 118.

le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant pour des raisons valables, légitimes et sérieuses, sauf dans les cas où le traitement est prévu par la loi ou est exigé par la nature de l'obligation.

En outre, la personne concernée, ses héritiers ou son tuteur, a le droit de s'opposer à ce que les données à caractère personnel la concernant soient communiquées aux tiers en vue de les exploiter à des fins publicitaires. L'opposition suspend immédiatement le traitement ».

46. Cet article élargit la liste des personnes pouvant exercer le droit d'opposition, ce qui est de nature à donner plus de protection aux D.C.P.[182]Le même article prévoit que le droit d'opposition peut être exercé à tout moment[183]. En se référant à la définition de la notion de traitement[184], il est possible que ce droit soit exercé même lors de la collecte des D.C.P.[185]

47. Selon l'article 42, le droit d'opposition peut être exercé en cas de « *(...) raisons valables, légitimes et sérieuses (...)* ». Le législateur exige donc implicitement la justification ou la motivation de ce droit. L'article 30-1-a de la loi du Luxembourg exige explicitement la justification de ce droit[186].

---

182 L'art. 14 de la directive de 1995 et l'art. 30 de la loi du Luxembourg du 2 août 2002 prévoient que ce droit peut être exercé par la personne concernée seulement.

183 La même disposition a été prévue par l'art. 14-a de la directive de 1995 et l'art. 30-1-a de la loi du Luxembourg du 2 août 2002.

184 V. art. 6 de la loi organique.

185 Selon un chercheur « *C'est bizarre de considérer la collecte un traitement, car le traitement nécessite au préalable une collecte. Or, comment traiter des données qu'on n'a pas encore collecté (...)* ». V. W. JARRAYA, mémoire précité, p. 23.
En réalité, il n'y a rien de bizarre puisque la collecte, considérée par plusieurs textes juridiques comme étant un traitement (art. 2-b de la directive de 1995 et 2-s de la loi du Luxembourg de 2002), peut constituer en elle-même une atteinte aux D.C.P. L'élargissement de la notion de traitement est d'ailleurs bénéfique pour la protection des D.C.P.

186 L'art. 30-1-a de cette loi prévoit que toute personne concernée a le droit « *de s'opposer à tout moment pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de dispositions légales prévoyant expressément le traitement. En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut pas porter sur ces données* ».

Le ministère de la justice et des droits de l'homme avait précisé que les conditions exigées sont nécessaires pour empêcher l'excès dans l'exercice du droit d'opposition. Il a aussi donné deux exemples dans lesquels les conditions sont réunies et qui sont le cas où le responsable du traitement change les finalités déjà fixées, et le traitement des D.C.P. sans obtenir le consentement de la personne concernée dans les cas où ce consentement est exigé[187].

En réalité, l'exigence de ces trois conditions[188] peut être critiquée, puisqu'elle est de nature à limiter la protection accordée aux D.C.P. L'appréciation des conditions peut amener à certains abus surtout qu'elles restent soumises à l'évaluation du responsable du traitement et ce n'est qu'en cas de litige que l'I.N.P.D.C.P. peut être saisie[189]. D'ailleurs, l'Instance aura certainement des difficultés pour trouver des éléments clairs de distinction entre ce qui est valable et ce qui est légitime. Existent-elles réellement des raisons légitimes mais non valables ?

Il était plus cohérent d'exiger tout simplement des raisons légitimes comme l'avait fait la loi française du 6 janvier 1978, telle que modifiée par la loi de 2004[190].

Par ailleurs, si l'exigence de motivation de l'exercice du droit d'opposition peut être acceptée en cas de données ordinaires, il n'en est pas de même dans le cas de données sensibles[191], qui nécessitent par leur nature plus de protection.

---

187 V. débats parlementaires sur le projet de loi organique, précités, p. 1289.

188 L'art. 14 de la directive de 1995 et l'art. 30 de la loi du Luxembourg exigent des raisons prépondérantes et légitimes.

189 L'art. 43 de la loi organique prévoit que : « *L'instance Nationale de Protection des Données à Caractère Personnel est saisie de tout litige relatif à l'exercice du droit d'opposition.*
L'instance doit rendre sa décision dans le délai prévu par l'article 41 de la présente loi ».

190 *L'art. 38 de la loi française prévoit que : « Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

191 V.

نادر عمران، المقال السابق، ص. 180.

48. La loi organique n'a pas indiqué le caractère gratuit ou non du droit d'opposition. Certains textes juridiques[192] insistent sur la gratuité du droit d'opposition surtout en cas de traitement effectué à des fins de prospection. En pratique, la personne concernée peut exercer son droit par le fait de remplir un formulaire disponible sur l'internet ou simplement par un clic sur une icône qui existe sur le site du responsable du traitement[193].

49. Considéré comme étant un veto[194], le droit d'opposition met fin au traitement. L'article 42 prévoit expressément que : « *L'opposition suspend immédiatement le traitement* ». L'exercice du droit d'opposition qui « *(...) connaît un regain d'intérêt dans le cadre de l'Internet* »[195], commande la diligence de la personne concernée pour savoir si le responsable du traitement respecte ou non ses obligations. On peut douter qu'un internaute après avoir donné ses D.C.P. poursuit la méthode de leur traitement, surtout que l'immatérialité limite sérieusement cette poursuite. Le problème se complique d'avantage en cas de collecte indirecte, faite par exemple par des cookies. La personne concernée ne sait même pas dans ce cas que ses D.C.P. ont été collectées et traitées. Pour toutes ces raisons on peut affirmer que le droit d'opposition avait une efficacité pratique limitée. Le même constat peut être relevé concernant les droits exercés lors de la conservation des D.C.P.

192 V. l'art. 14-b de la directive de 1995 et l'art. 30-1-b de la loi du Luxembourg du 2 août 2002. V. aussi sur le droit belge S. LOUVEAUX, article précité, loc. cit.

193 V. notamment A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 117 ; M. WALRAVE, article précité, loc. cit.

194 V. A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 114.

195 Ibid., p. 119.

B- Les droits exercés lors de la conservation des D.C.P.

50. Lors de la conservation des D.C.P., le droit d'accès avait une importance cruciale puisqu'il permet aux personnes concernées de savoir si leurs D.C.P. sont en train d'être traitées ou non et toutes les informations concernant l'opération de traitement, comme la nature, la finalité, la communication et le transfert des D.C.P.[196]. Vu cette importance, le législateur a consacré une sous-section[197] dans la loi organique du 27 juillet 2004 pour régler le droit d'accès et les droits qui en découlent. L'article 32 de cette loi organique définit le droit d'accès comme étant : « *(...) le droit de la personne concernée, de ses héritiers ou de son tuteur de consulter toutes les données à caractère personnel la concernant, ainsi que le droit de les corriger, compléter, rectifier, mettre à jour, modifier, clarifier ou effacer lorsqu'elles s'avèrent inexactes, équivoques, ou que leur traitement est interdit.*

Le droit d'accès couvre également le droit d'obtenir une copie des données dans une langue claire et conforme au contenu des enregistrements, et sous une forme intelligible lorsqu'elles sont traitées à l'aide de procédés automatisés ».

51. Selon cet article, le droit d'accès peut être exercé par la personne concernée, ses héritiers ou son tuteur. L'élargissement de la liste des personnes, ayant le droit d'accès aux D.C.P., montre la volonté du législateur de consacrer une protection efficace. Cette volonté peut être confirmée par l'aspect direct de cet accès[198]. La personne concernée n'est pas obligée de recourir à un tiers pour l'exercice de son droit, même en ce qui concerne les données sensibles. En

---

196 V. W. JARRAYA, mémoire précité, p. 27 ;

نادر عمران، المقال السابق، ص. 169.

197 V. les arts. 32 à 41 et les arts. 55 et 56 de la loi organique.

198 V.

نادر عمران، المقال السابق، ص. 169.

France, l'accès aux données médicales traitées ne peut être qu'indirect[199]. La personne concernée doit désigner un médecin qui doit apprécier s'il peut ou non informer le requérant des secrets médicaux le concernant[200]. En Hongrie, le droit d'accès peut être exercé par un tiers appelé médiateur, qui a la possibilité de consulter même les D.C.P. classés secret d'État[201].

52. La définition du droit d'accès, telle que prévue par l'article 32, montre que le législateur confond entre le droit d'accès au sens propre et certains droits qui dérivent de ce droit, comme le droit de rectification et le droit de communication.

53. Étant d'ordre public[202], le droit d'accès peut être exercé normalement sans frais, même si le législateur n'a pas prévu cela expressément[203], la lecture de l'article 40 paragraphe 2 peut confirmer ce raisonnement[204].

54. Le législateur a prévu dans la loi organique deux conditions pour l'exercice du droit d'accès. La première condition a été détaillée dans l'article 34 qui prévoit que : « *Le droit d'accès est exercé par la personne concernée, ses héritiers ou son tuteur à des intervalles raisonnables et de façon non excessive* ».

55. L'expression « *(...) à des intervalles raisonnables et de façon non excessive* » suscite quelques interrogations. On sait que sur l'internet, les données peuvent changer d'un jour à l'autre, dans ce cas la question qui se pose est celle de savoir quelle est la durée du temps qui sera considérée comme étant raisonnable ?

---

199 V. les arts. 40 et 45 al. 3 de la loi de 1978.

200 V. A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 110.

201 V. E. SIMON, article précité, p. 2.

202 L'art. 33 de la loi organique prévoit que : « *On ne peut préalablement renoncer au droit d'accès* ».

203 Certains textes juridiques insistent sur le caractère gratuit du droit d'accès. V. sur ces textes, P. de LHONEUX, « Projet de loi sur la protection de la vie privée », in. A. B. MOURY et autres, Le droit des affaires en évolution, Bruxelles, BRUYLANT, 1992, p. 242.

204 L'art. 40 paragraphe 2 prévoit que : « *Elle peut en outre demander, sans frais et après l'accomplissement des procédures requises, la délivrance d'une copie des données à caractère personnel et indiquer ce qui n'a pas été réalisé en ce qui concerne ces données* ».

Selon le ministère concerné, le but de cette condition est de protéger le responsable du traitement contre les abus, puisque la personne concernée peut exiger de lui permettre d'exercer son droit le dimanche ou la nuit ou plusieurs fois dans le même jour[205]. Si l'exercice du droit d'accès plusieurs fois par jour peut être considéré comme non raisonnable et excessif, les deux autres exemples cités par le ministre peuvent être critiqués puisqu'ils négligent la possibilité de permettre à la personne concernée d'exercer son droit d'une manière automatisée, qui se moque du temps et des jours fériés. La question reste donc soumise à l'appréciation du responsable du traitement[206] et en cas de refus de permettre à la personne concernée d'accéder à ses données, l'Instance peut ordonner la consultation des informations la concernant[207].

La deuxième condition d'exercice du droit d'accès a été prévue dans l'article 56 de la même loi qui précise qu'en ce qui concerne les données traitées surtout par les établissements publics de santé, la personne concernée, ses héritiers ou son tuteur « *(…) peuvent, pour des raisons valables, demander de corriger, de compléter, de rectifier, de mettre à jour, de modifier, ou d'effacer les données lorsqu'elles s'avèrent inexactes et qu'ils en ont pris connaissance* ». Aussi paradoxalement que cela puisse paraître, le législateur exige la motivation du droit d'accès en ce qui concerne les données sensibles, alors qu'il dispense la personne concernée de la justification de son droit en cas de données ordinaires.

56. L'article 35 de la loi organique prévoit que : « *La limitation du droit d'accès de la personne concernée, de ses héritiers, ou de son tuteur aux données à caractère personnel la concernant n'est possible que dans les cas suivants :*

---

205 V. débats parlementaires sur le projet de loi organique, précités, p. 1289.

206 L'art. 39-II de la loi française du 6 janv. 1978, telle que modifiée par la loi du 6 août 2004 prévoit que : « *Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées* ».

207 V. l'art. 38 de la loi organique.

-lorsque le traitement des données à caractère personnel est effectué à des fins scientifiques et à condition que ces données n'affectent la vie privée de la personne concernée que d'une façon limitée ;
-si le motif recherché par la limitation du droit d'accès est la protection de la personne concernée elle-même ou des tiers ».

Cet article suscite les remarques suivantes :

D'abord, l'article parle de la limitation du droit d'accès et non de l'interdiction, comme c'est prévu par exemple dans l'article 56 de la même loi[208]. La limitation peut consister dans l'exigence des intervalles du temps bien déterminés ou la motivation des raisons d'exercice du droit d'accès.

Ensuite, le premier cas qui autorise la limitation du droit d'accès exige que le traitement des D.C.P. soit effectué à des fins scientifiques et à condition que ces données « *(...) n'affectent la vie privée de la personne concernée que d'une façon limitée* ». La question qui se pose, alors, est celle de savoir comment les données peuvent affecter la vie privée d'une façon limitée ?

Une telle expression peut amener à des abus car ce qui peut être considéré par les responsables du traitement comme une affectation limitée de la vie privée, peut au contraire être estimée, par la personne concernée, comme une atteinte sérieuse à sa vie privée. Le ministère concerné a essayé de donner un exemple, qui semble être un peu flou[209].

Enfin, la limitation du droit d'accès peut être justifiée par la protection de la personne concernée ou les tiers. Si la protection de la personne concernée peut être envisagée dans le domaine médical, il est difficile d'envisager la réalisation de ce cas dans le domaine du commerce électronique. Il est aussi difficile de

---

208 L'art. 56 alinéa premier de la loi organique prévoit que : « *Le droit d'accès aux données à caractère personnel traitées par les personnes mentionnées à l'article 53 ne peut être exercé* ».

209 L'exemple se limite à réitérer ce qui a été prévu dans l'art. 35. Le ministère considère aussi que le traitement fait à des fins scientifiques ne peut pas affecter la vie privée, ce qui n'est pas vrai dans tous les cas. V. débats parlementaires, précités, p. 1289.

concevoir l'exemple où l'exercice du droit d'accès aux données spécifiques à une personne bien déterminée peut léser un tiers. Malgré cela, la même exception a été prévue dans les articles 13-g de la directive de 1995 et 29-f de la loi du Luxembourg du 2 août 2002.

57. L'un des problèmes qui se posent est celui de savoir comment peut-on exercer le droit d'accès en ligne ?

Les statistiques montrent que 43 % des sites belges n'indiquent pas comment le droit d'accès peut être exercé en pratique. Le reste des sites indiquent une adresse e-mail ou un numéro de téléphone permettant à la personne concernée d'exercer son droit[210].

58. L'article 38 de la loi organique prévoit que : « *La demande d'accès est présentée par la personne concernée ou ses héritiers ou son tuteur par écrit ou par n'importe quel moyen laissant une trace écrite* ». La présentation de la demande d'accès[211] peut poser certains problèmes sur l'internet. Pour cette raison, l'article 37 de la même loi prévoit que : « *Le responsable du traitement automatisé des données à caractère personnel et le sous-traitant doivent mettre en œuvre les moyens techniques nécessaires pour permettre à la personne concernée, à ses héritiers ou à son tuteur l'envoi par voie électronique de sa demande de rectification, de modification, de correction, ou d'effacement des données à caractère personnel* ».

59. La demande d'accès, qui nécessite la diligence de la personne concernée, peut limiter sérieusement l'exercice du droit d'accès surtout que le législateur n'a pas imposé au responsable du traitement un délai bien déterminé pour répondre à cette demande, et ce contrairement à la demande d'obtention de

---

210 V. M. WALRAVE, article précité, loc. cit.

211 L'art. 36 de la loi organique prévoit que : « *Lorsqu'il y a plusieurs responsables du traitement des données à caractère personnel ou lorsque le traitement est effectué par un sous-traitant, le droit d'accès est exercé auprès de chacun d'eux* ».

copies des données. L'article 38 de la loi organique prévoit, en effet, que : « *La personne concernée, ses héritiers ou son tuteur peuvent demander de la même manière l'obtention de copies des données dans un délai ne dépassant pas un mois à compter de la dite demande* ». En cas de litige concernant l'exercice du droit d'accès ou d'obtenir copies des données, l'I.N.P.D.C.P. peut être saisie[212].

60. Malgré son importance, le droit d'accès « *(...) reste largement ignoré, ce qui explique en partie sa faible mise en œuvre et son efficacité pratique limitée, ce qui est tout à fait regrettable* »[213]. Sans l'exercice du droit d'accès, la personne concernée ne peut rectifier ses D.C.P.[214]. L'article 40 de la loi organique prévoit que : « *La personne concernée, ses héritiers ou son tuteur, peut demander de rectifier les données à caractère personnel la concernant, les compléter, les modifier, les clarifier, les mettre à jour, les effacer lorsqu'elles s'avèrent inexactes, incomplètes, ou ambiguës, ou demander leur destruction lorsque leur collecte ou leur utilisation a été effectuée en violation de la présente loi* ».

61. Le droit de rectification pose en pratique trois problèmes.

Le premier est relatif à la preuve de l'exactitude des D.C.P. L'article 39 de la loi organique tranche ce problème en prévoyant que : « *En cas de litige sur l'exactitude des données à caractère personnel, le responsable du traitement et le sous-traitant doivent mentionner l'existence de ce litige jusqu'à ce qu'il y soit statué* ».

Le deuxième problème que pose le droit de rectification, concerne le cas où les D.C.P. sont communiquées ou transférées à un tiers. Dans un tel cas, la personne concernée peut seulement rectifier les données traitées par le responsable ou le sous-traitant. Toutefois, le responsable et le sous-traitant sont

212 V. l'art. 38 als. 2, 3 et 4.
213 A. LUCAS, J. DEVEZE et J. FRAYSSINET, op. cit., p. 105.
214 V. J.-L. SOULIER et S. SLEE, article précité, p. 668 ; P. de LHONEUX, article précité, p. 243.

tenus selon l'article 21 de la loi organique de « *(...) corriger, compléter, modifier ou mettre à jour les fichiers dont ils disposent, et effacer les données à caractère personnel de ces fichiers s'ils ont eu connaissance de l'inexactitude ou de l'insuffisance de ces données* ». De même, ils « *(...) doivent informer, la personne concernée et le bénéficiaire de manière légitime des données de toute modification apportée aux données à caractère personnel (...)* ».

Il est clair donc que le législateur exige la notification de la rectification[215] aux tiers[216].

Le troisième problème consiste dans le fait que tout en étant dépendant du droit d'accès, le droit de rectification est très négligé en pratique. Le droit de rectification nécessite plus que les autres droits la diligence de la personne concernée. Or, il est difficile de concevoir qu'après avoir donné ses D.C.P., lors d'un contrat de vente électronique par exemple, la personne concernée va se souvenir, après deux ou trois ans du site du cybervendeur et procède ainsi à la rectification de ses données. Le phénomène de l'indifférence face au changement des D.C.P. est la règle sur le net. Vu le manque de diligence des personnes concernées et les risques que présente le réseau des réseaux, les internautes doivent être plus que jamais éduqués. Pour que la protection des D.C.P. soit efficace, le responsable du traitement doit détailler sa politique en la matière dans la première page du site, en recourant de préférence à un système de labellisation du site. L'internaute peut ainsi cliquer sur une icône qui décrit toutes les informations dont il avait besoin pour que ses données soient transmises en toute sécurité.

---

215 L'art. 21 al. 3 de la loi organique prévoit que : « *La notification s'effectue dans un délai de deux mois, à compter de la date de la modification, par voie de lettre recommandée avec accusé de réception ou par n'importe quel moyen laissant une trace écrite* ».

216 Selon S. KHALED, « *(...) la législation tunisienne n'exige pas la notification des rectifications, aux tiers auxquels les données ont été communiquées (...)* », ce qui est critiquable. V. S. KHALED, « Le droit à la protection des données personnelles », R.J.L., 2004, n° 12, p. 51.

62. Étant donné que les nouvelles technologies sont capables de collecter les données à l'insu de la personne concernée, il est nécessaire de trouver les solutions techniques équivalentes et de garantir à toute personne un "*droit à être laissé tranquille*"[217]. La protection des D.C.P. commande un travail "*en progrès*"[218]. Toute politique de protection doit être révisée de temps en temps pour que le droit ne soit pas dépassé par la technique[219].

63. La protection des D.C.P. doit être instaurée pour améliorer la confiance et la sécurité des personnes concernées par le traitement. Toutefois, dans certains cas la société mérite d'être protégée contre l'excès de liberté accordée à toute personne de divulguer ses D.C.P.[220]. On est, donc, en train de passer de la protection des D.C.P. de la personne concernée, à la protection de la société contre la divulgation inconsciente de la personne de ses propres D.C.P.

---

217 V. J.-P. GRIDEL et A. LACABARATS, « Droit à la vie privée et liberté d'expression : fond du droit et action en justice », Gaz. Pal., 2002, nov.-déc., p. 1643 ; H. KASSEM, L'internaute et son droit à être laissé tranquille, mémoire de D.E.A. informatique et droit, Université Montpellier 1, faculté de droit, 2003, pp. 1 et s.

218 P. BISCHOFF, article précité, p. 542.

219 V. J. LE CLAINCHE, article précité, pp. 28 et s.

220 V. sur l'affaire d'un professeur qui se dévoilait sur l'internet A. LEPAGE, « Le professeur se dévoilait sur Internet », Com.-Com. Elec., fév., 2007, pp. 39 et s.