Wissem Jarraya,

« La protection des données personnelles dans le commerce électronique »

Rapport de recherche, Faculté de droit de Sfax, 2013

La protection des données personnelles dans le commerce électronique

Wissem Jarraya

Doctorant à la Faculté de droit de Sfax

Juge au tribunal de 1ère instance Sfax 2

INTRODUCTION

« *Ce ne sont pas les philosophes avec leurs théories, ni les juristes avec leurs formules mais les ingénieurs avec leurs inventions qui font le droit et surtout le progrès du droit* »[1]. C'est ainsi que Albert de Geouffre de la Pradelle a décrit la relation entre le droit et le progrès scientifique. C'est que toute avancée technologique est suivie par la loi qui vient pour l'encadrer et essayer de limiter ses inconvénients ou les abus qu'il peut engendrer. Ceci est vrai pour le commerce électronique dont le développement passe nécessairement par la sécurisation du réseau et la protection des données à caractère personnelle.

En effet, « *le succès du commerce électronique dépend, en grande partie, de la confiance qu'ont les consommateurs vis-à-vis de la protection accordée aux données à caractère personnel qu'ils transmettent* »[2] .

Le commerce électronique, qui est défini comme étant la distribution, la commercialisation, la vente ou la livraison des biens ou des services par des moyens électroniques[3], est devenu un enjeu politique et économique majeur surtout

---

1 Cité par : C-A.COLLIARD, « La machine et le droit privé français contemporain », Mélange offert à Georges RIPERT, Paris, L.G.D.J., 1950, p. 115.

2 S.LOUVEAUX , « Le commerce électronique et la vie privée », in. Le droit des affaires en évolution , BRUYLANT, BRUXELLES, 1999, p. 183.

3 Centre du Commerce International, Guide à l'intention des entreprises : Le système commercial mondial, Genève, Centre du Commerce International C.N.U.C.E.D./O.M.C.., 2000, p. 332.

dans les pays industrialisés, son développement suppose la sécurité juridique et technique et la confiance des utilisateurs qui communiquent en réseaux ouverts[4].

Malheureusement, support principal du commerce électronique, « *Internet, la technologie la plus à la mode, montre le niveau de sécurité le plus bas* »[5]. En fait, l'atteinte à la vie privée est l'une des grandes menaces au commerce électronique. Or, la vie privée est une notion délicate, changeante dans le temps et dans l'espace[6], difficile à définir[7], malgré les tentatives de la doctrine[8], ce qui a permis de dire que définir la vie privée «(…) c'est vouloir définir l'incertain par le flou »[9]. Il est plus adéquat, dès lors, de parler de la protection des données à caractère personnel (D.C.P.) dans le commerce électronique.

Le législateur tunisien a défini la notion de D.C.P. dans l'article 4 de la loi organique n°2004-63 du 27 juillet 2004 portant sur la protection des données à caractère personnel [10] . L'article 4 de cette loi définit les 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 telle par la loi* ».

L'article 5 de la même loi ajoute que «*(…) est réputée identifiable, la personne physique susceptible d'être identifiée, directement ou indirectement, à*

---

4 E.A.CAPRIOLI, « Sécurité et confiance dans le commerce électronique : signature numérique et autorité de certification, J.C.P., 1998, ed.G., n°14, p. 83.

5 T.P.COUDOL,Echange électronique certification et sécurité, Paris, Litec, 2000, p. 8.

6 X.AGOSTINELLI, Le droit à l'information face à la protection civile de la vie privée, Paris, Librairie de l'Université, 1994, p. 88 et s.

7 F.RIGAUX, La protection de la vie privée et des autres biens de la personnalité, Paris, L.G.D.J., 1990, p. 724. ; L.GOLVERS, L'informatique et la protection de la vie privée, p.2, disponible sur : http://www.droit-technologie.org.

8 P.KAYSER, La protection de la vie privée, Paris, Economica 1995, p. 225. ; A.ROUX , La protection de la vie privée dans les rapports entre l'Etat et les particuliers, Paris, Economica, 1983, p. 7. ; S.TSIKLITRAS, La propriété effective des libertés publiques par le juge judiciaire en droit français, Paris, LGDJ, 1991, p. 153.

9 F.DEBOISSY et J.C.SAINT-PAU, « La divulgation d'une information patrimoniale », D.,2000, n.17,ch.,p.269.

10 J.O.R.T., n°61, 30 juillet 2004.p.1988.

travers plusieurs données ou symboles qui concernent notamment son identité, ses caractéristiques physiques, physiologiques, génétiques, psychologiques, sociales, économique ou culturelles ».

En droit comparé, la notion « donnée personnelle » est défini sous plusieurs dénominations[11]. D'après les lignes directrice de l'Organisation de Coopération et de Développement Economique (O.C.D.E.) régissant la protection de la vie privée et les flux transfrontalières de D.C.P., on entend par D.C.P. toute information relative à une personne physique identifiée ou identifiable[12].

Les D.C.P. des personnes physiques sont multiples. On peut les classer en trois types. D'abord, les D.C.P. classiques qui englobent nom, prénom, adresse, numéro de téléphone, numéro de la carte d'identité, numéro de sécurité sociale, date de naissance, numéro de la carte bancaire[13], adresse électronique et Internet Protocol (I.P.)[14]…

Ensuite, les données dites sensibles. Ces données sont celles qui révèlent l'origine raciale ou éthique, les opinions politiques, les convictions religieuses ou philosophique, l'appartenance syndicale ainsi que les données relatives à la vie sexuelle. Ces données sont plus intimes que celles de la première catégorie. C'est pourquoi elles nécessitent un régime plus protecteur.

Enfin, les données appelées en droit belge, comme en droit tunisien, données relatives à la santé[15], et qu'une partie de la doctrine appelle "données médicales"[16].

---

11 La doctrine utilise parfois les expressions suivantes : « données nominatives » ; « renseignements personnelles » ; « données sensibles ».

12 La convention pour la protection des personnes à l'égard du traitement automatisé des D.C.P. dite convention 108 adopte la même définition.

13 G.D-PASANAU, « Vente à distance et paiement par carte bancaire :quels enjeux pour la vie privée des consommateurs ? », Expertises, aout-sept., 2003, p.295.

14 Adresse IP ou encore Internet Protocol, c'est un numéro qui identifie de façon unique un ordinateur connecté au réseau Internet. C'est l'adresse d'une machine fonctionnant dans le cyberespace, un peu comme un numéro de téléphone. Une adresse IP se compose de quatre nombres séparés par des points (exemple : 194.232.1.20). D.KAPLAN, dir., op.cit.,. p. 205 ; voir aussi D.FOREST, « Piraterie en ligne et données personnelles :une équation insoluble ? », Expertises, juin, 2004, p. 222.

15 F.de BROUWER, « Protection des données à caractère personnel : un nouveau cadre légal Belge », R.D.A.I., n°2,1999, p.181.

Ces données présentent une importance extrême vue leur objet. On s'en souvient encore de l'affaire " Le Grand secret"[17] qui opposait le docteur Claude Gubler à son patient, l'ex-président de la France François Mitterrand. Certains parlent même des données génétiques[18]. Ces différentes catégories de données nécessitent une protection de plus en plus sérieuse avec l'émergence de l'informatique et du commerce électronique. En effet, les D.C.P. «*(...) deviennent une monnaie d'échange* »[19] ce qui nécessite une protection adaptée au réseau des réseaux tout en permettant le développement du commerce électronique dont le fonctionnement repose sur un marché de D.C.P.

Mais, qu'est-ce que ce phénomène du commerce électronique ?

Il n'y a pas de définition universellement acceptée de l'expression "commerce électronique". Le législateur tunisien a défini le commerce électronique dans la loi 2000-83 du 9 août 2000 relatives aux échanges et au commerce électronique[20]. Selon l'article 2 de cette loi, le commerce électronique consiste dans « *les opérations commerciales qui s'effectuent à travers les échanges électronique ».* Le même article définit les échanges électroniques comme ceux *« qui s'effectuent en utilisant des documents électroniques* ».

Cette définition est à la fois simple et large. Simple, parce qu'elle lie la notion du commerce électronique à celle du document électronique. Large, parce que toute utilisation d'un document électronique dans le cadre d'une opération commerciale constitue un acte de commerce électronique.

---

16 S.V-TAVERNIER, « La C.N.I.L et la protection des données médicales nominatives », Gaz.Pal.,1999, 2ème sem., p. 1153

17 Cass., 1er civ.,14 dec. 1999, S.A. Les Editions Plan et a.c/ cts Mitterand; J.C.P., n°5, jurisp., II, 10241.

18 M-I.MALAUZAT, Le droit face aux pouvoirs des données génétiques, Paris, Presses Universitaires D'Aix-Marseille.2000, p. 191.

19 L.CARON, Protection des données personnelles sur Internet et enjeux du commerce électronique, in. La galaxie Internet, Paris, UNICOMM, 1998, p. 159.

20 J.O.R.T., n°64 du 11 oct. 2000, p. 1887.

La doctrine est loin d'être d'accord sur une définition du commerce électronique. D'après Jérôme Huet, «*(…) le commerce électronique consiste principalement dans la possibilité offerte par des fournisseurs, privés ou publics, à des interlocuteurs, professionnels ou consommateurs, de passer commande de produit ou services, par le biais des communications numérisées généralisées sur les grands réseaux, ainsi que dans la publicité qui peut être faite pour ces produits ou services, notamment sur les sites Internet des entreprises qui les proposent* »[21].

Monsieur Eric Caprioli distingue entre trois approches de commerce électronique, notamment politique[22], économique[23] et technique[24].

Avec la création de bases de données dans le domaine du commerce électronique, les D.C.P. sont en péril, et derrière elles, les personnes auxquelles appartiennent ces données, surtout que la doctrine affirme que le commerce électronique se caractérise par trois"i"[25].

D'abord, immatérialité, puisque les échanges sur Internet sont souvent dématérialisés. Ensuite, interactivité, qui permet de naviguer par ci et par là grâce

---

21 J.HUET, « La problématique juridique du commerce électronique », Acte de colloque annuel de l'association droit et commerce, R.J.C.,2001, p.17.

22 Selon l'O.C.D.E., se sont « Toutes les formes de transaction liées aux activités commerciales, associant tant les particuliers que les organisations et reposant sur le traitement et la transmission de données numérisées notamment texte, son et image. Il désigne aussi les effets que l'échange électronique d'informations commerciales peut avoir sur les institutions et sur les processus qui facilitent et encadrent les activités commerciales ». E.A.CAPRIOLI, « Preuve et signature dans le commerce électronique », Droit et Patrimoine ,n°55, dec 1997, note. 3, p.56.

23 C'est le fait pour une entreprise d'utiliser l'informatique, associé au réseau de télécommunication, pour interagir avec son environnement. Ibidem., note 4 ; D'après l'article 14 de la loi Française de 21juin 2004 pour la confiance dans l'économie numérique « Le commerce électronique est l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services ».

24 Par exemple courrier électronique sur Internet, Echange de Données Informatisées, base de données partageables, transfert électronique de fonds, formulaire administratif électronique. Ibidem, note 5.

25 J.HUET, article précité, p.19.

aux liens hypertexte[26]. Enfin, le troisième "i" est celui de l'internationalité. Le commerce électronique est un monde sans frontières.

Ces caractéristiques reflètent les avantages du commerce électronique. On peut acheter un bien ou acquérir un service sans bouger de derrière son poste. On peut notamment communiquer avec des entreprises dans l'autre bout du monde, consulter leur site web, voir la marchandise et examiner ses caractéristiques comme dans un supermarché réel. Ce ci semble profitable pour un consommateur ou un simple visiteur du site. Ces avantages font progresser le commerce électronique. « *le trafic d'Internet double tous les cent jours* »[27].

Ce développement ne peut pas cacher les dangers que peut présenter le commerce électronique pour les données à caractère personnelle. Tout d'abord, l'Internet a mis en avant le problème de la "traçabilité".[28]Chaque connexion laisse forcément des traces, ce qui rend l'internaute transparent [29] et supprime la confidentialité des échanges. En effet, le développement du commerce électronique permet de « *tracer un profil de plus en plus complet de chaque individu* »[30]. L'absence de frontière permet de créer" un paradis de données" [31] et le développement du commerce électronique accentue la pression car les D.C.P. brutes ou traitées deviennent un enjeu économique considérable pour la connaissance et la possession des marchés. En fait, ces données sont devenues une

---

26 C'est la présentation de l'information qui permet une consultation non linéaire grâce à la présence de liens activables dans les documents, et conduisant l'utilisateur soit à un autre point du même document, soit à un autre document.

27 L.BOCHURBERG, Internet et commerce électronique : Site web. Contrats. Responsabilités. Contentieux , Paris, DELMAS, 2ème édition, 2001,p. 11.

28 A.LUCAS, J.DEVEZE et J.FRAYSSINET, Droit de l'informatique et de l'Internet, Paris, P.U.F., 1994, p. 14.

29 N.M-POUJOL, « Les libertés de l'individu face aux nouvelles technologies de l'information », Cahier français, n°296, 2000, p. 60.

30 E.DELEURY et D.GOUBAU, Le droit des personnes physiques, Qébec-Canada, Les éditions Yvon Blais Inc, 1994, p. 149.

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

précieuse marchandise qui s'achète et se vende[32] et la protection des D.C.P. est devenue un argument marketing.[33]Ces données-traces sont collectées par d'autres personnes et c'est un autre danger ; il s'agit de la collecte sauvage des données[34]qui peut se faire par les hackers.[35]On assiste, déjà « *(…) à l'apparition de nouveau type de criminels "cyberthief" qui utilisent les réseaux ouverts pour se procurer indirectement les numéros de carte de crédit…et accéder aux données confidentielles…* ».[36]D'autres acteurs importants du web sont des grands collecteurs comme les fournisseurs d'accès et les moteurs de recherche.[37]Et même à ce stade les dangers ne font que commencer. Le danger devient imminent lorsqu'il s'agit de la divulgation des données [38] ou leur déformation ou traitement ou encore détournement de la finalité pour laquelle elles ont été collectées.

La protection des D.C.P. dans le commerce électronique est réglementée par des textes nationaux et internationaux.

Au niveau national, c'est l'article 9 de la constitution de 1959 qui consacre la protection des D.C.P. Toutefois, il n'existe pas dans le C.O.C. un texte général qui consacre la protection de la vie privée à l'instar de l'article 9 C.civ. Français. Cela peut être expliqué par le fait que les dispositions de la responsabilité délictuelle englobent les cas d'atteinte à la vie privée. Le C.O.C. consacre aussi des cas spéciaux de protection de la vie privée comme l'abus de droit et les troubles de voisinage. La loi 2000-83 du 9 août 2000 relatives aux échanges et au commerce

---

32 M.LAIME, « Allons nous devoir vendre nos données personnelles », disponible sur : http://www.uzine.net.

33 A.MOLE et H. LEBON, « Publipostage électronique : entre certitudes et incertitudes », Gaz.Pal., juill., 2002, p. 1137.

34 Une étude a montré que plus que 90% des sites web belges collectent des D.C.P. Etude disponible sur : http:// www.vie privée.org/news120.

35 Ce sont des personnes qui se connectent à quelconque type de réseau pour décortiquer les applications en relation avec ce réseau, ce qui leur permet l'accès à des informations.

36 S.KALLEL, « Les autoroutes de l'information : aspects juridiques », R.J.L., juin, 1997, p.68 et s.

37 T.LEONARD, « E-marketing et protection des données à caractère personnel », disponible sur : http://www.droit-technologie.org.

38 Le professeur P.KAYSER fait toujours la distinction entre l'investigation et la divulgation de la vie privée.

électronique[39] consacre le chapitre VI à la protection des D.C.P. Mais, cette loi avait un champ d'application limité puisqu'elle n'est applicable qu'entre le fournisseur de service de certification électronique et le titulaire du certificat. L'année 2004 est une année heureuse pour les D.C.P. puisqu'elle a été marquée par la promulgation de la loi organique n°2004-63 du 27 juillet 2004, portant sur la protection des D.C.P[40]qui a une portée générale et qui a abrogé le chapitre VI de la loi de 2000.

Au niveau international, la protection de la vie privée est consacrée dans plusieurs textes ; on cite :

-L'article 12 de la déclaration universelle des droits de l'homme de 1948.[41]

-L'article 17 du pacte des Nations Unis relatif aux droits civils et politiques.[42]

-L'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentaux.[43]

-La convention n°108 pour la protection des personnes à l'égard du traitement automatisé des D.C.P.[44]

Il s'y ajoute les lignes directrices de l'O.C.D.E. régissant la protection de la vie privée et les flux transfrontaliers des D.C.P.[45] et la loi type sur le commerce électronique C.N.U.D.C.I.[46]

Les Etats-Unis privilégient l'adoption de mécanismes d'autoréglementation[47] à travers des codes de bonne conduite issus de l'industrie, sans qu'aucun dispositif

---

39 J.O.R.T., n°64, 11 août 2000, p.1887.

40 J.O.R.T., n°61, 30 juillet 2004, p.1988.

41 Disponible sur le site : http://www.justice.gouv.fr/textfond/dudh1948.

42 Disponible sur le site: http://www.droitshumains.org/uni/Formation/02pacte2_f.

43 Disponible sur le site : http://www.justice.gouv.fr/textfond/europ1.

44 R.COTE et R.LAPERRIERE, dir, « vie privée sous surveillance : la protection des renseignements personnels en droit québécois et comparé ». Annexe, p.267.

45 Ibidem , p.259.

46 J.D.I., n°2, 1997, annexe, p.394.

47 L'autoréglementation consiste en des «normes volontairement développées et acceptées par ceux qui prennent à une activité », Y.POULLET, « Quelques considérations sur le droit du cyberespace », Texte présenté à l'Académie royale belge des Sciences, le 20 mars 1998, p. 7.

de protection des D.C.P. ne soit mis en œuvre. Mais, ces dernières années, « *le gouvernement américain met désormais la protection des données personnelles au premier plan de priorité* ».[48]

La protection des D.C.P. et de la vie privée est très ancienne. Mais, ce sont les moyens de protection qui ont changé. Au début, on s'intéressait à la protection de la vie privée Tel que défini à la fin du XVIII ème siècle, notamment à travers la déclaration des droits de l'homme et du citoyen de 1789, « la protection de la vie privée n'avait pas trouvé sa place en tant que tel ».[49]Ce n'est qu'après la seconde guerre mondiale qu'on a admis une "*conception élargie des droits de l'homme*".[50]

Cette protection s'est renforcée avec l'apparition de l'Internet et du commerce électronique qui constituent une véritable menace pour les D.C.P. En effet, le commerce électronique est apparu avec les échanges des données informatisées (E.D.I.) utilisés entre les entreprises.[51]. La vie privée était protégée par des instruments juridiques généraux. C'est vers la fin des années 60 que l'exigence de la protection des D.C.P. est apparue. Elle est liée au développement de l'informatique et la crainte de voir les techniques informatiques peser lourdement sur les libertés publiques. L'Allemagne était la première à adopter une loi relative à la protection des D.C.P. Le Land de Hesse a adopté en 1970 une loi relative au « *traitement automatisé des informations nominatives* ».[52] Les Etats-Unis adoptent le"Privacy Act" qui ne concerne que les fichiers détenus par les administrations fédérales.[53] Ce n'est qu'en 1978 que la France s'est dotée d'une loi protégeant les D.C.P., il s'agit de la loi Informatique et Liberté qui trouve son

---

48 L.CARON, article précité, p.163.
49 X. AGOSTINELLI, op.cit, p.143.
50 Ibidem, loc.cit.
51 J.HUET, article précité, p.1.
52 U.BRUHANN, « La directive européenne relative à la protection des données : fondement, histoire, points forts », R.F.A.P., n°89, 1999, p.9.
53 M-P.F-TROUSSEAU et G.HAAS, Internet et protection des données personnelles, Paris, Litec, 2000,p. 10.

origine dans l'affaire "Safari", [54]avant d'adopter la loi numéro 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique[55] et la loi de 6 août 2004.[56] La loi organique du 27 juillet 2004[57] témoigne de la conscience du législateur tunisien de l'importance de la question et on est devenu devant une multitude de textes, nationales et internationales, qui ont vocation à s'appliquer pour la protection des D.C.P. dans le commerce électronique qui est un domaine technique par excellence, ce qui pose le problème suivant : *la protection juridique des D.C.P dans le commerce électronique est-elle suffisamment efficace ?*

Les textes juridiques offrent une protection a priori qui est non respecté en pratique (**Première partie 1**) et une protection a posteriori inefficace par sa nature (**Première partie 2**).

---

54 Ibidem, p.11 ; H.MAISL, « Etat de la législation française et tendances de la jurisprudence relatives à la protection des données personnelles », R.I.D.C., n°3, 1987, p.559.

55 J.O., n°143 du 22 juin 2004, p.11168, texte n°2, disponible sur : http://www.Legifrance.gouv.fr. ; voir également :L.GRYNBAUM, « Projet loi « pour la confiance dans l'économie numériques » :encore un petit effort et rigueur juridique pour un « contrat électronique » fiable », D., 2003, n°11, p.746.

56 Loi précitée.

57 Loi précitée.

Première partie :
Le non-respect de la protection a priori

Devant la sensibilité de la question de la protection des D.C.P., la prévention devient de plus en plus sollicitée et l'adage « mieux vaut prévenir que guérir » trouve son application.

Toutefois, la prévention passe nécessairement par l'exercice des personnes concernées de leurs droits (**Section 1**) et le respect des responsables du traitement de leurs obligations (**Section 2**).

Section 1: Les droits des personnes concernées

Législation et doctrine s'accordent sur quatre droits principaux pour toute personne concernée. Il s'agit du droit à l'information, du droit d'opposition, du droit d'accès et du droit de rectification[58].

A- Le droit à l'information

On entend par le droit à l'information le droit que possède la personne concernée dans une opération de commerce électronique d'obtenir du cyber-

---

58 S. LOUVEAUX, article précité, p. 203 et s ; A.BENSOUSSAN, Le commerce électronique : aspects juridiques, Paris, Hermes, 1998, p81 et s; C.ROJINSKY et O.LEAURANT, créer et exploiter un site Web : guide juridique et pratique, Paris, Lamy/Les Echos, 2000, p. 128 et s.
نعيم مغبغب، مخاطر المعلوماتية و الانترنات. المخاطر على الحياة الخاصة و حمايتها دراسة في القانون المقارن، بيروت، 1998، ص247 .

commerçant des informations satisfaisantes et pertinentes concernant l'utilisation de ses données personnelles.

Après avoir consacré le droit à l'information dans son alinéa premier, l'art 31 de la loi 2004 précise dans son deuxième alinéa le contenu de cette information. En effet, l'art 31 dispose que « …il faut informer au préalable…de ce qui suit :

-la nature de DCP concernée par le traitement ;

-les finalités du traitement des DCP ;

-le caractère obligatoire ou facultatif de leur réponse ;

-les conséquences du défaut de 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 ;

-leur droit de revenir, à tout moment, sur l'acceptation du traitement ;

-leur droit de s'opposer au traitement de leur D.C.P. ;

-la durée de conservation des D.C.P. ;

-une description sommaire des mesures mises en œuvre pour garantir la sécurité des D.C.P. ;

-le pays vers lequel le responsable du traitement entend, le cas échéant, transférer les D.C.P. ;… ».

Ainsi formulé, l'art 31 exige une information complète de la personne concernée qui assure la transparence des transactions. Cette information englobe les droits des personnes concernées à savoir, le droit d'accès, le droit de revenir sur l'acceptation du traitement et le droit d'opposition. La personne concernée a, aussi, un droit à l'information du caractère obligatoire ou facultatif de sa réponse, ainsi

que les conséquences d'un défaut de réponse, ce qui lui permet de décider de répondre ou non en toute connaissance de cause.

La personne concernée a aussi le droit d'être informée de la finalité du traitement[59], de l'identité du bénéficiaire et du responsable du traitement, de la durée de conservation des données et des mesures mises en œuvre pour garantir leur sécurité. Cette information permettra à la personne concernée d'évaluer si ses données sont en toute sécurité.

La loi Belge ajoute que l'information doit porter sur l'existence de procédé de collecte automatique de données(cookies)[60] ainsi que les mesures de sécurité garantissant l'authenticité du site, l'intégrité et la confidentialité des informations transmises sur le réseau.

La réalité témoigne que cette disposition est peu respectée. En l'absence de statistique en Tunisie, une étude belge réalisée en 2002 montre que 67% des sites Web utilisent des cookies et seulement 12% des sites concernés en informent les visiteurs[61].

On remarque que c'est une obligation lourde, coûteuse et complexe à mettre en œuvre. Elle est notamment gênante pour le domaine du commerce électronique y compris sur Internet[62].

Il s'ajoute à tout cela les modalités d'information. L'information doit être fournie d'une façon pratique et efficace. Les alinéas 1 et 3 de l'article 31 de la loi 2004 ne sont pas conformes sur les modalités d'information. D'une part, l'alinéa premier dispose qu'il faut informer au préalable « *par n'importe quel moyen laissant une trace écrite* ». D'autre part, l'alinéa 3 dispose que « *la notification*

---

59 Par exemple, lorsque les données sont collectées pour l'exécution d'un contrat et pour des opérations de prospection, le responsable du traitement doit indiquer clairement ces deux finalités.

60 Les cookies sont des fichiers envoyés sur le disque dur de l'ordinateur des personnes qui visitent un site. Ces fichiers enregistrent des informations quand le visiteur accède au site et lors de ses connexions futures. Le visiteur sera donc, suivi dans sa navigation., L.CARON, op.cit., note, 2, p. 159.

61 Etude disponible sur : http://www.vie privée.org.news120.

62 A .LUCAS, J. DEVEZE, J. FRAYSSINET, op.cit., p.136.

s'effectue par lettre recommandé avec accusé de réception ou par n'importe quel moyen laissant une trace écrite… ».

L'option offerte par l'alinéa 3 est inutile car la lettre recommandée avec accusé de réception est en elle-même un moyen laissant une trace écrite.

L'article 31 insiste donc que l'information laisse une trace écrite. En pratique, les responsables du traitement utilisent des moyens techniques pour informer l'internaute. Ce dernier n'a qu'à cliquer sur la fenêtre « *données personnelles* » pour voir s'afficher dans son écran la politique du responsable des traitements dans la protection des D.C.P. Cette fenêtre doit apparaître soit dans la page d'accueil, soit au début du document électronique pour que l'information soit facilement accessible à l'utilisateur.

L'information doit être fournie, conformément à l'article 31, après le délai de réponse de l'Instance à l'autorisation fixé à l'article 7 et au préalable à la collecte et « *(…) dans un délai d'un mois au moins avant la date fixée pour le traitement des D.C.P.* ».

Le but de l'octroi d'un droit d'information est d'assurer la transparence lors de la collecte des données et de permettre aux personnes concernées d'exprimer leur opposition.

B- Le droit d'opposition

Indépendamment de l'idée de transparence, le droit d'opposition renforce la maîtrise des individus de leurs données personnelles. Le droit d'opposition est donc le complément du droit à l'information. Une fois la personne informée lors de la collecte, elle pourra par suite soit accepter soit s'opposer à ce que ses données soient collectées.

L'article 42 alinéa premier dispose que « *La personne concernée, ses héritiers ou son tuteur, a le droit de s'opposer à tout moment au traitement des données à caractère personnel le concernant pour des raisons valables, légitimes et sérieuses, sauf dans le cas où le traitement est prévu par la loi ou exigé par la nature de l'obligation* ».

Le droit d'opposition s'exerce donc, "*à tout moment au traitement des données*". Il en découle que ce droit peut s'exercer avant la collecte des données étant donné que l'article 6 de la loi 2004 considère, paradoxalement[63], la collecte des données un traitement.

La plus importante remarque que soulève cet article est qu'il subordonne l'exercice du droit d'opposition à l'existence de raisons valables, légitimes et sérieuses. Puis, il prévoit deux exceptions dans lesquelles la personne concernée est privée de ce droit. Le droit français parle de motifs légitimes alors que son homologue belge utilise l'expression « *raisons sérieuses et légitimes* » que la loi tunisienne a choisi d'y ajouter "valables".

Les raisons légitimes signifient que ces raisons ne doivent pas être contraires à la loi et aux bonnes mœurs. Quant aux raisons sérieuses et valables, on ne voie pas de différence entre les deux. On peut les interpréter comme étant des raisons existantes et indispensables. En plus, ces raisons posent le problème de leur appréciation, ce qui nécessite le recours à l'Instance Nationale De Protection Des Données Personnelles en cas de litige conformément à l'article 43 de la loi 2004 ce qui signifie aussi de plus en plus de temps perdu.

Plus grave encore, la personne concernée est privée de son droit d'opposition « *dans le cas où le traitement est prévu par la loi ou exigé par la nature de*

63 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, et malgré les interrogations des députés lors des débats parlementaires concernant la loi de 2004, le ministre de la justice et des droits de l'homme a insisté que la collecte est une opération de traitement des D.C.P. Voir : J.O.R.T. n°34 du 21 juill. 2004, débats parlementaires, p.1302.

l'obligation ». L'article 44 ajoute « *le consentement n'est pas requis lorsque la collecte…auprès de la personne concernée implique des efforts disproportionnés ou s'il s'avère manifestement que la collecte n'affecte pas ses intérêts légitimes, ou lorsque la personne concernée est décédée* ».

Il est regrettable que la loi ait multiplié les exceptions de telle façon, qu'il est légitime de craindre que le principe devienne exception et que l'exception devienne principe. Les deux dernières exceptions sont, en effet, inadmissibles. Il est évident que la collecte des données, en elle-même, n'affecte pas les intérêts légitimes de la personne. Ce sont, en fait, les opérations postérieures à la collecte qui sont dangereuses.

Le droit d'opposition devra s'exercer d'une manière aisée et gratuite surtout si les données sont collectées à des fins de direct marketing[64]. En pratique, la personne exprime son opposition soit en marquant "la case à cocher" soit en décochant cette case[65].

Le droit d'opposition, consacré aussi par la directive 95/46/CE[66], connaît un regain d'intérêt dans le cadre d'Internet qui multiplie les occasions de collecte de données et leur commercialisation. Il rend illégal les cookies non désirés, ainsi que les messages non sollicités.

Il faut signaler que le droit d'opposition n'est pas toujours facile à mettre en œuvre. Il n'est pas, non plus sans inconvénients. D'abord, il va à l'encontre des promoteurs du commerce électronique et reste difficilement applicable pour les sites dont la législation ne consacre pas en raison du caractère transfrontalier du commerce électronique[67]. Ensuite, on peut se demander si le droit d'opposition peut

64 S. LOUVEAUX, article précité, p.206.
65 A .LUCAS, J. DEVEZE, J. FRAYSSINET, op.cit.,p.117
66 Voir article 14 de la directive 95/46/CE .
67 A .LUCAS, J. DEVEZE, J. FRAYSSINET, op.cit.p.119.

jouer lorsque les données n'ont pas été collectées directement[68]. Enfin, lorsque le droit d'opposition est exercé après la collecte, et que les données seront déjà stockées dans un CD ROM, comment supprimer une seule information d'un CD ROM ?

C- Le droit d'accès et de communication

L'article 32 de cette loi de 2004 dispose que « *Au sens de la présente loi, on entend par droit d'accès, 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 ».

La loi donne une définition si large au droit d'accès qu'elle confond avec le droit de rectification puisqu'elle définit le droit d'accès comme le droit de corriger les D.C.P. En fait, la personne a même le droit d'obtenir une copie de ses données. L'alinéa 2 de l'article 32 intègre le droit de communication dans le droit d'accès.

Le fait de donner au droit d'accès un domaine large est, certes, en faveur de la personne concernée. Cette faveur est renforcée par l'article 33 qui dispose que « *On ne peut préalablement renoncer au droit d'accès* ». Cette position est confirmée par la doctrine qui considère que le droit d'accès constitue «*(...) la*

---

68 H.MAISL, « Etat de la législation française et tendance de la jurisprudence relatives à la protection des données personnelles », R.I.D.C. 3. 1987. P.577.

pierre angulaire de la protection des données »[69] dans la mesure où il permet une maîtrise de la personne sur ses données. En l'occurrence, toute personne doit pouvoir obtenir communication de ses données qui doivent être conforme au contenue des enregistrements[70].

La loi 2004 a réglementé également les procédures d'exercice du droit d'accès. Ce dernier s'exerce conformément à l'article 32 sur" toutes les données à caractère personnel". Et même en cas de pluralité de traitants ou de sous-traitants, l'article 36 dispose 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* ».

Toutefois, l'article 35 de la loi consacre des limites à ce droit en disposant 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 suivant :*

-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 ».

Ces exceptions sont dangereuses étant donné l'ambiguïté de leurs expressions. Or, qu'est-ce qu'une atteinte limitée à la vie privée ? Et qui a l'autorité de dire qu'il s'agit d'une atteinte limitée ? En plus, il est à craindre que la deuxième exception soit utilisée pour empêcher le droit d'accès.

---

69 D.MARTIN, « La directive 95/46/CE (protection des données) et sa transposition en droit français », Gaz.Pal., 1998, 1er sem., p.608.

70 S.GUINCHARD, M.HARICHAUX et R. de TOURDONNET, Internet pour le droit : connexion- recherche-droit, Paris, 2ème éd., MONTCHRESTIEN, E.J.A.,2001, p.176.

La loi a réglementé la procédure d'exercice du droit d'accès. D'abord, ce droit est exercé par la personne concernée, ses héritiers ou son tuteur. On en déduit que c'est un droit personnel. Ce qui a poussé à dire que c'est un droit de la personnalité[71]. Cependant, ce droit "*peut être utilisé pour protéger des intérêts patrimoniaux*"[72].

Ensuite, la demande d'accès est présentée « *(…) par écrit ou par n'importe quel moyen laissant une trace écrite. La personne concernée, ses héritiers ou son tuteur peuvent demander de la même manière l'obtention de copie des données dans un délai ne dépassant pas un mois à compter de la dite demande* »[73]. La demande doit être adressée au responsable des traitements ou au sous-traitant, selon le cas. Ces derniers doivent « *mettre en œuvre les moyens techniques nécessaires pour permettre à la personne concernée, ses héritiers ou à son tuteur l'envoi par voie électronique de sa demande (…)* ».

Mais, notre législateur semble limiter l'exercice du droit d'accès par l'article 34 qui dispose 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* ».

Il est clair que le but de cet article est de ne pas marginaliser le droit d'accès et d'éviter que la personne concernée n'abuse de son droit. Mais cela risque de réduire la portée du droit d'accès en tant que moyen de contrôle des données. Or, dire que ce droit doit être exercé à des intervalles raisonnables et de façon non excessive est une chose imprécise[74]. On peut se demander si la demande d'accès une fois par semaine est excessive ?

---

71 P.KAYSER, op.cit., p.362.

72 P.ANCEL, « La protection des données personnelles aspects de droit privé français », R.I.D.C.,3-1987., p.622.

73 Art. 38 de la loi du 27 juillet 2004.

74 L'art.39 II de la loi française Informatique et Liberté tel que modifiée par la loi de 6 août 2004 dispose 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. »

Dans la pratique, le droit d'accès aux données personnelles…reste largement ignoré ce qui explique en partie sa faible mise en œuvre et son efficacité pratique limitée.

D-Le droit de rectification

Le droit d'accès ne trouve toute son efficacité que si la personne concernée pourrait rectifier ses données. C'est ainsi que l'article 40 de la loi 2004 dispose 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…* ».

Ce texte donne au droit de rectification un domaine étendu et permet même d'assurer une maîtrise complète de la personne sur ses données. Mais, ce droit pose le problème de la preuve de l'exactitude des données. Ce problème n'a pas échappé à la loi 2004. En effet, l'article 39 dispose 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 soit statué* ».

Le législateur, tout en étant conscient du problème de la preuve de l'exactitude des données, a choisi de ne pas donner une solution. En fait, qu'elle est l'utilité de mentionner que ces données font l'objet d'un litige ?

L'article 21 de la loi 2004 a le mérite d'obliger le responsable du traitement à une rectification d'office. En effet, cet article dispose que « *Le responsable du traitement et le sous-traitant doivent 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… »

Malgré cela, le droit de rectification reste une simple consécration législative sans issue. Ce droit est déjà difficile à mettre en œuvre puisqu'il constitue la fin des maillons des droits des personnes concernées. En effet, il est un droit dépendant de l'exercice des autres droits. Si l'une des autres droits fait défaut, il devient impossible de rectifier ces données. En plus, on sent une négligence chez les personnes concernées à l'égard de ce droit.

Section 2 : Les obligations des responsables du traitement

Les responsables du traitement doivent respecter leurs obligations. Il est à remarquer d'abord, que la majorité des obligations des responsables du traitement ont pour objet de permettre aux individus d'exercer leurs droits et de leur faciliter la tâche à travers le respect de certains principes et la bonne gestion des D.C.P.

A-Le principe de loyauté

L'article 9 de la loi 2004 dispose que « *Le traitement des données à caractère personnel doit se faire dans le cadre du respect de la dignité humaine, de la vie privée et des libertés publiques.*

Le traitement des données à caractère personnel, quelle que soit son origine ou sa forme, ne doit pas porter atteinte aux droits des personnes protégées par la loi et les règlements en vigueur, et il est, dans tous les cas, interdit d'utiliser ces données pour porter atteinte aux personnes ou à leur réputation ».

Cela signifie que la collecte, en tant qu'opération de traitement, doit être loyale. Ceci est confirmé par l'article 11 qui dispose que « *Les données à caractère*

personnel doivent être traitées loyalement, et dans la limite nécessaire au regard des finalités pour lesquelles elles ont été collectées… ».

Selon monsieur Ali Kahloun, le principe de la loyauté dans la collecte des données signifie que ne doivent être collectées que les données nécessaires à l'opération pour laquelle elles ont été collectées, et que ces données ne doivent pas être utilisées à des fins illicites[75].

En effet, la loyauté dans la collecte suppose "d'une part, que les données ne soient pas collectées à l'insu de la personne concernée"[76]. D'autre part, que les données collectées soient, non pas nécessaires, mais, indispensables pour accomplir une opération licite.

Pour que la collecte des données soit loyale, le responsable du traitement doit informer la personne concernée que ses données font l'objet d'une collecte. Mais, en pratique, les commerçants via Internet font tout leur possible pour collecter des D.C.P. à l'insu des utilisateurs du réseau. Pour atteindre cet objectif, ils utilisent principalement les cookies qui sont très efficaces.

Les cookies[77]sont des « *petits programmes espions* »[78] qui ressemblent à un morceau de gâteau empoisonné. Il s'agit « *d'une empreinte que le site visité dépose dans le disque dur de l'ordinateur de l'internaute. Cette empreinte permettra, lors de la prochaine connexion de l'utilisateur à ce serveur, de repérer la précédente consultation, ainsi que les pages du site qui avaient été consultées* »[79]. Les cookies

---

75 علي كحلون، الجوانب القانونية لقنوات الاتصال الحديثة و التجارة الإلكترونية، تونس، دار إسهامات في أدبيات المؤسسة،2002، ص. 355.

76 J.BOYER, « L'Internet et la protection des données personnelles et de la vie privée », Cahier Français, n°295, p.74.

77 Sur les cookies voir: C.ALVERGNAT, Dir.D.KAPLAN, Guide du commerce électronique, Paris, ECHANGEUR Maisonneuve & LAROSR, 2000, p.108. ; F-J.PANSIER et E.JEZ, L'initiation à l'Internet juridique, Paris, Litec, 1998, p.72 ; M-P.F-TROUSSEAU et G.HAAS, op. cit., p.135 ; J.BOYER, article précité, p.76 ; A.BENSOUSSAN, Dir., op.cit., p.85 ; C.ROJINSKYet O.LEAURANT, op.cit.,p.127.

78 F-J.PANSIER et E.JEZ. op.cit.,p.72.

79 J.BOYER, article precité, loc.cit.

permettent alors, d'assurer la traçabilité de la navigation et transforment, dès lors, la souris en véritable "*bracelet électronique*"[80].

Le fait d'informer la personne lors de la collecte des données ne suffit pas pour considérer que c'est une collecte loyale, car il faut encore que ces données soient indispensables pour l'accomplissement de l'opération pour laquelle elles ont été collectées. C'est ainsi que l'article 11 de la loi 2004 prévoit que « *Les données à caractère personnel doivent être traitées loyalement, et dans la limite nécessaire au regard des finalités pour lesquelles elles ont été collectées…* ».

Le non-respect du principe de loyauté est causé par le contenu ambigu de ce principe. La loi ne définit ni les moyens frauduleux de la collection, ni les moyens déloyaux. Le principe de loyauté parait « riche de sens mais flou, impliquant une appréciation morale ou éthique autant que juridique, intégrant fortement les faits contextuels »[81], d'où, l'importance du rôle du juge. Ce non-respect ne se limite pas au principe de loyauté et les choses deviennent de plus en plus dangereuses puisqu'il s'étend au principe de finalité.

B-Le principe de finalité

Le principe de la finalité consiste à ce que le collecteur des données doit faire apparaître les objectifs qu'il désire atteindre par la collecte.

L'art 10 de la loi 2004 dispose que « *La collecte des données à caractère personnel ne peut être effectuée que pour des finalités licites, déterminées et explicites* ». Il en découle que la finalité doit être d'une part, déterminée et explicite, c'est-à-dire ni trop large, ni trop ambiguë et équivoque, et ce, à fin d'éviter le risque de détournement de finalité. D'autre part, la finalité doit être

---

80 Ibidem. p. 77.

81 A .LUCAS, J. DEVEZE, J. FRAYSSINET, op.cit., p.126.

licite, c'est-à-dire conforme à la loi et aux bonnes mœurs. L'article 17 de la loi de 2004 confirme cette idée en disposant que « *Il est, dans tous les cas, strictement interdit de lier la prestation d'un service ou l'octroi d'un avantage à une personne à son acceptation du traitement de ses données personnelles ou de leur exploitation à des fins autres que celles pour lesquelles elles ont été collectées* ».

Le fait que la finalité soit explicite et déterminée, permet à l'internaute de consentir à la collecte en toute connaissance de cause.

Toutefois, selon l'art 12, les D.C.P. peuvent être utilisées à des fins autres que celles déclarées lors de la collecte si d'abord, la personne concernée a donné son consentement. En fait, cette disposition qui semble être une exception, ne l'est pas. Si la personne concernée a donné son consentement c'est qu'il a été déjà informé. On n'est plus donc devant une exception. Ensuite, les D.C.P. peuvent être utilisées à d'autres fins, si le traitement est nécessaire à la sauvegarde d'un intérêt vital de la personne concernée. Cette exception qui semble être au profit de la personne est ambiguë. Or, quel intérêt vital peut-on sauvegarder en détournant la finalité des données collectées dans une opération de commerce électronique ? Au cours du débat parlementaire, cette question a été posée au ministre de la justice et des droits de l'homme, le député a signalé que la personne concernée est censée savoir, plus que les autres, son intérêt[82]. Le ministre a répondu à travers un exemple qui se rapporte au domaine médical [83] et non du domaine du commerce électronique, et a laissé, ainsi, la question sans réponse précise. Toutefois, il a signalé qu'en cas de litige, c'est l'Instance qui sera compétente pour le trancher. Enfin, si le traitement mis en œuvre est nécessaire à des fins scientifiques certaines,

---

82 Débat parlementaire de la loi de 27 juillet 2004, J.O.R.T. des débats parlementaire, n°34, 21 juillet 2004, p.1303.

83 L'exemple qu'a donné monsieur le ministre est le suivant : Si une personne a consenti à un vaccin de type P.C.G., et que ce vaccin aide à la découverte d'une autre maladie, on considère alors ici qu'il s'agit d'un intérêt vital pour la personne concerné et on ne demande plus son consentement pour lui faire le vaccin contre l'autre maladie.

le principe de finalité ne joue plus. L'article utilise l'expression "certaine", et on sait que les recherches et les expériences scientifiques n'ont jamais été certaines et, donc, cette expression ne manque pas d'ambiguïté.

Bien que le législateur ait voulu limiter les exceptions au principe de finalité, on assiste, malheureusement, en pratique à un détournement de finalité. Ainsi, les données collectées pour une finalité déclarée peuvent servir à d'autres fins. Le détournement le plus fréquent consiste à utiliser ces données pour faire du publipostage abusif, appelé couramment le spamming.

Le spamming ou encore publipostage électronique[84]consiste en « *la diffusion généralisée de messages non sollicitées à un grand nombre d'utilisateurs de l'Internet* »[85].

Devant les inconvénients du spamming, [86]le législateur tunisien a réagi. L'article 30 de la loi 2004 dispose dans son alinéa 2 que « *Il est interdit d'utiliser le traitement des données à caractère personnel à des fins publicitaires sauf consentement exprès et particulier de la personne concernée, de ses héritiers ou de son tuteur. Le consentement à cet égard est soumis aux règles générales de droit* ». Selon cet article, le responsable du traitement ne peut utiliser les D.C.P. à des fins publicitaires qu'après avoir obtenu le consentement de la personne concernée. On en déduit que le législateur opte pour le système de "l'opt-in" qui s'oppose à celle de "l'opt-out".

Le système de "l'opt-out" « *repose sur une autorisation de principe d'envoyer des communications commerciales non sollicitées à moins que le destinataire ne s'y oppose expressément* »[87]. Ce système est fondé sur le principe

---

84 A.MOLE et H.LEBON, article précité, p.1134.

85 M.ANTOINE et les autres, Le commerce électronique européen sur les rails ? analyse et proposition de mise en œuvre de la directive sur le commerce électronique, C.R.I.D., Bruxelles, BRUYLANT 2001, p.132.

86 M.ANTOINE et autres, op.cit., p.134 et s ; Voir aussi, J. MORLEC, Le spam, mémoire préparé dans le cadre de la maîtrise de droit des affaires de la Faculté de droit de Nantes, 2003, p. 10 et s.

87 Ibidem, p.140.

de la liberté du commerce. Il intervient *a posteriori* par l'exercice du droit d'opposition. Mais, ce système a commencé à être délaissé en faveur du système de l'opt-in[88]. En effet, reposant sur le principe de la protection des D.C.P., l'opt-in est basé sur une interdiction de principe d'envoyer des communications commerciales non sollicitées à moins que le destinataire n'ait préalablement marqué son consentement. La loi 2004 rejoint la directive européenne de 30 mai 2002 et la loi Française[89] sur ce point. En réalité, le publipostage devient illégal du moment où le responsable du traitement déclare une finalité autre que le publipostage lors de la collecte des données. Le juge des référés du Tribunal de Grand Instance de Paris a jugé, le 15 janvier 2002[90], qu'un fournisseur d'accès pouvait résilier le contrat d'un client pour avoir pratiqué du spamming. Le juge des référés a estimé que le cyber-commerçant a perturbé l'équilibre des réseaux. Le juge a également relevé que « *La pratique du spamming, considérée dans le milieu de l'Internet comme une pratique déloyale et gravement perturbatrice, est contraire aux dispositions de la charte de bonne conduite* ».

Pour échapper à une telle obligation, les sites web formulent la finalité de collecte d'une façon assez vague. Par exemple "*usage interne*", "*actions commerciales et contractuelles*", "*vous offrir une meilleur expérience Web*"[91], ce qui réduit l'efficacité et la portée du principe de finalité.

C-La sécurité des données

88 D.FOREST, « Le spamming en quête de régulation », Expertises, fev. 2003, p.61.

89 L'article 22 de la loi Française de 2004 pour la confiance dans l'économie numérique dispose que « Est interdite la prospection directe...utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes... ». Et le même article ajoute que « Constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ».

90 T.G.I. Paris, ord.réf., 15 janvier 2002. R.G.n 01/59336, cité par A. MOLE et H. LEBON article précité, p. 1137, note 2. voir notamment la position de la jurisprudence française du spamming : D.FOREST, article précité, p.62.

91 Etude disponible sur : http://www.vie privée.org/news 120.

Les D.C.P. doivent être protégées à l'abri des regards indiscrets. C'est ainsi que le responsable du traitement doit prendre toutes les précautions utiles afin de garantir la confidentialité des données et d'empêcher leur déformation, endommagement, ou communication à un tiers non autorisé.

La loi 2004 consacre le principe de sécurité des données dans les articles 18 et 19. L'article 18 dispose 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 toute les précautions nécessaires pour assurer la sécurité de ses données et empêcher les tiers de procéder à leur modification, à leur altération ou à leur consultation sans l'autorisation de la personne concernée* ».

L'article 19 ajoute que « *Les précautions prévues à l'article 19 de la présente loi doivent :*

-empêcher que les équipements et les installations utilisés dans le traitement des données à caractère personnel soient placés dans des conditions ou des lieux permettant à des personnes non autorisées d'y accéder ;

-empêcher que les supports des données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée ;

-empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, tout effacement ou toute radiation des données enregistrées ;

-empêcher que le système de traitement d'information puisse être utilisé par des personnes non autorisées ;

-garantir que puisse être vérifiée a posteriori l'identité des personnes ayant eu accès au système d'information, les données qui ont été introduites dans le système, le moment de cette introduction ainsi que la personne qui l'a effectuée ;

-empêcher que les données puissent être lues, copiées, modifiées, effacées ou radiées, lors de leur communication où du transport de leur support ;

-sauvegarder les données par la constitution de copie de réserve sécurisées ; ».

Ces articles visent à garantir la sécurité des données lors de leur conservation en assurant leur intégrité et leur confidentialité. En assurant ces deux fonctions, la loi tunisienne reprend l'obligation posée par les articles 16 et 17 de la directive européenne de 1995, l'article 34 de la loi Informatique et Liberté et l'article 7 de la convention 108.

L'obligation de sécurité a un caractère préventif puisqu'elle intervient avant toute divulgation des données et avant que la personne ne subisse un préjudice.

Pour assurer une protection complète des données lors de leur conservation, il faudrait réglementer aussi la durée de leur conservation. C'est ce que la doctrine appelle "le droit à l'oubli"[92]. Le droit à l'oubli est le droit de voir les données oubliées après un certain temps.[93]La loi 2004 consacre ce droit dans l'article 24 *in fine* et l'article 26. Selon l'article 24, au cas où le responsable du traitement des D.C.P. ou le sous-traitant envisage de cesser son activité, ou en cas de son décès ou sa faillite, l'I.N.P.D.C.P. [94]doit en être informée. « L'Instance, dans un délai ne dépassant pas un mois à compter de la date de son information…autorise la destruction des données à caractère personnel ». L'article 26 ajoute que «En cas de cessation de l'activité du responsable du traitement ou du sous-traitant pour les motifs indiqués à l'article 24 de la présente loi, la personne concernée, ses héritiers ou toute personne ayant intérêt ou le ministère public peuvent, à tout moment, demander de l'Instance de prendre toutes les mesures appropriées pour la

---

92 R.LIDON, La création prétorienne en matière de droit de la personnalité et son incidence sur la notion de famille, Paris, DALLOZ, 1974, p.25 ; M-P.F-TROUSSEAU, op.cit, p.56 ; N.M-POUJOL, article précité, p.60 ; A.R.BERTAND, op.cit., p.929.

93 Voir le site : http://www.parodie.com .

94 Instance Nationale de Protection des Données à Caractère Personnel.

conservation et la protection des données à caractère personnel, ainsi que leur destruction.

L'Instance doit rendre sa décision dans un délai de dix jours à compter de la date de sa saisine.»

Ces deux articles soulèvent les remarques suivantes :

D'abord, la destruction des données peut se faire à l'insu de la personne concernée et ce au cas où le responsable du traitement ou le sous-traitant va cesser définitivement son activité conformément à l'article24 alinéa premier.

Ensuite, dans tous les cas de destruction des données, la personne concernée n'aura aucun contact direct avec le responsable du traitement et dans tous les cas, c'est l'Instance qui autorise la destruction des données ou qui prenne les mesures appropriées pour la destruction.

Enfin, le législateur a raté l'occasion de consacrer un véritable droit à l'oubli. En effet, le droit à l'oubli signifie que les D.C.P. doivent être détruites après un certain temps. Or, la loi 2004 n'a pas déterminé une période après laquelle les D.C.P. seront détruites. Cette durée ne doit cependant pas excéder ce qui est strictement nécessaire, après quoi, pour être conservées, les informations doivent être rendues anonymes[95].

Devant cette lacune de la législation, le principe de la finalité apparaît comme le chevalier sauveteur. En fait, il faut interpréter les dispositions de la loi 2004 dans le sens à admettre que les données doivent être conservées jusqu'à la réalisation de la finalité déclarée. Une fois cette finalité est achevée, les données perdent leur raison d'être[96] et doivent être détruites[97].

---

95 M-P.F-TROUSSEAU et G.HAAS , op.cit., p.56.

96 Par exemple, si les données ont été collectées à l'occasion d'un contrat de consommation, et que ce contrat a été résilié ou annulé, ces données doivent être détruites puisque la raison pour laquelle elles ont été collectées est éteinte.

97 C'est la solution adoptée par le législateur français puisque l'article 6 cinquièmement de la loi Informatique et Libertés dispose que «Elles sont conservées…pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ».

D- La gestion adéquate des données

La gestion adéquate des données personnelles doit obéir à des règles qui assurent leur protection et ce par le respect des règles relatives au traitement des D.C.P. et les règles relatives aux flux transfrontaliers des données, voire même leur commercialisation.

1- Le traitement des D.C.P.

L'article 6 de la loi 2004 définit la notion de traitement des D.C.P. en ces termes « *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* »

Ainsi défini, la constitution par un cyber-commerçant des fichiers[98] pour ses clients constitue un traitement[99], de même pour la répartition des clients selon des catégories. La jurisprudence semble appuyer cette définition. En effet, tout en connaissant à une photo publiée sur Internet le caractère de D.C.P., laquelle était complétée par un texte faisant apparaître les mœurs de l'intéressé, le tribunal de Grand Instance de Pivas a précisé que par traitement automatisé il convient

---

98 Un fichier est définit par l'article 6 de la loi 2004 comme étant « Ensemble de D.C.P. structuré et regroupé susceptible d'être consulté selon des critères déterminés et permettant d'identifier une personne déterminée ».

99 S.GUINCHARD , M. HARICHAUX et R.de TOURDONNET ; op.cit., p. 170.

d'entendre « l'extraction, la consultation, l'utilisation, la commercialisation par transmission, la diffusion ou tout autre forme de mise à disposition de D.C.P.[100] ».

Le traitement des D.C.P. en lui-même n'est pas illicite. Cependant, au préalable, le responsable du traitement doit informer la personne concernée et obtenir son consentement conformément à l'article 27 de la loi 2004 qui dispose que « *à 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.*

La personne concernée ou son tuteur peut, à tout moment, se rétracter ». Cet article soulève les remarques suivantes :

D'abord, le traitement des D.C.P. ne peut s'effectuer qu'avec le consentement exprès et écrit de la personne concernée. La loi 2004 n'a pas défini le consentement et ce contrairement à la directive européenne de 1995 qui l'a défini comme « *toute manifestation de la 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* »[101]. Le consentement doit aussi être spécifique, il « doit porter sur des traitements précisément définis et non sur des objets généraux »[102]. Le consentement doit être, enfin, informé. Cela implique que les sites doivent informer les visiteurs des risques du commerce électronique vis-à-vis de la protection des D.C.P. Cela leur permet « de mettre en balance ces risques avec les bénéfices attendus »[103].

---

100 T.G.I. Pivas, 3 septembre 1997, Expertise, n° 213, mars 1998, p.79.
101 Voir art 2-h de la directive 95/46/CE.
102 S. LOUVEAUX, article précité, p.195.
103 Ibidem, loc.cit.

Ensuite, si la personne est incapable ou interdite ou incapable de signer, le consentement est régi par les règles générales de droit[104]. L'article 28 de la loi ajoute dans ce contexte que « *le traitement des données à caractère personnel qui concerne un enfant ne peut s'effectuer qu'après l'obtention du consentement de son tuteur et de l'autorisation du juge de famille* »[105].

Enfin, l'article 27 consacre un droit de rétractation. En effet, l'article 27 *in fine* prévoit que « *La personne concernée ou son tuteur peut, à tout moment, se rétracter* ». Ce droit, bien qu'il soit en faveur de la personne concernée, il met en péril la stabilité des transactions.

L'article 29 prévoit des cas où le consentement n'est plus nécessaire pour le traitement. Il s'agit du cas où il s'avère manifestement que le traitement est effectué dans l'intérêt de la personne concernée et que le contact avec celui-ci se révèle impossible. Il s'agit de deux conditions cumulatives ce qui semble favoriser la personne concernée.

Le consentement n'est plus nécessaire aussi, dans le cas où le traitement des D.C.P. est prévu par la loi ou une convention dans laquelle la personne concernée est partie. Dans ce cas, la non exigence du consentement est expliquée par la force de la loi et par la force de la convention.

2-Les flux transfrontaliers et la commercialisation des D.C.P.

Les D.C.P. sont devenus dans le commerce électronique des marchandises dont les sociétés privées assurent la vente.[106] Ces données acquièrent "une valeur marchande"[107] qui séduit ces sociétés à les commercialiser et incite même leur

---

104 Se sont les articles du C.O.C. qui s'appliquent ainsi que les articles 156 et 157 C.S.P.

105 Selon l'art. 3 de la loi n°95-92 du 9/11/1995, relative à la publication du code de la protection de l'enfant, l'enfant est « toute personne humaine agée de moins de dix-huit ans et qui n'a pas encore atteint l'age de la majorité par disposition spéciales », J.O.R.T., n°90 du 10/11/1995, p. 2096.

106 F. GARNIER, « Solutions concrètes pour un business éthique sur Internet », p.2, Disponible sur : http://www.droit-technologie.org.

107 M-P.F-TROUSSEAU et G.HAAS , op.cit., p.111.

titulaire à les vendre ; ainsi, la doctrine s'est posée la question si "nous allons devoir vendre nos données personnelles ?" [108] Cette commercialisation prend souvent la forme de flux transfrontaliers, c'est-à-dire un transfert des données d'un pays à un autre, ce qui témoigne du caractère international du commerce électronique.

Le problème est que le niveau de protection n'est pas le même dans tous les Etats.

L'examen de la loi 2004 montre que le transfert des D.C.P. est parfois, interdit et parfois, autorisé.

L'article 47 alinéa 1 dispose que « *Il est interdit de communiquer des données à caractère personnel aux tiers sans le consentement exprès donné par n'importe quel moyen laissant une trace écrite, de la personne concernée, de ses héritiers ou de son tuteur…* ». L'article 50 ajoute que « *Il est interdit, dans tous les cas, de communiquer ou de transférer des données à caractère personnel vers un pays étranger lorsque ceci est susceptible de porter atteinte à la sécurité publique ou aux intérêts vitaux de la Tunisie* ».

Le ton de ces articles est très ferme. Il est interdit de communiquer les D.C.P. à un tiers sans le consentement exprès laissant une trace écrite, donné par la personne concernée, ses héritiers ou son tuteur. En effet, on remarque que le consentement se révèle tout au long du chemin des D.C.P. de la collecte jusqu'au transfert.

L'article 50 reprend l'interdiction du transfert des D.C.P à des pays étrangers lorsque ceci est susceptible de porter atteinte à la sécurité publique ou aux intérêts vitaux de la Tunisie.

Toutefois, ce ton ferme est vite assoupli. En fait, le transfert est autorisé dans les cas prévus par les articles 47, 49, 51 et 52. L'alinéa 2 de l'article 47 dispose que

---

108 M.LAIME, article précité, disponible sur : http://www.uzine.net.

«l'Instance peut autoriser la communication des données à caractère personnel en cas de refus, écrit et explicite, de la personne concernée, de ses héritiers ou de son tuteur lorsqu'une telle communication s'avère nécessaire pour la réalisation de leurs intérêts vitaux, ou pour l'accomplissement des recherches et études historiques ou scientifiques, ou encore en vue de l'exécution d'un contrat auquel la personne concernée est partie, et ce, à condition que la personne à qui les données à caractère personnel sont communiquées s'engage à mettre en œuvre toutes les garanties nécessaires à la protection des données et des droits qui s'y rattachent conformément aux directives de l'Instance, et d'assurer qu'elles ne seront pas utilisées à des fins autres que celles pour lesquelles elles ont été communiquées. ». Il en découle les remarques suivantes :

Contrairement à l'article 29 de la loi qui écarte le consentement s'il s'avère que le traitement est manifestement nécessaire, cet article se contente par l'expression "nécessaire". Il est donc légitime de se demander sur la différence entre "manifestement nécessaire" et "nécessaire". Le législateur aurait dû utiliser l'expression "indispensable" au lieu de "manifestement nécessaire".

Plus important encore, l'article 51 dispose que « *Le transfert vers un autre pays des 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…* ».

Cet article reprend l'expression de l'article 25 de la directive européenne de 1995. Le terme "adéquat", utilisé aussi par la version originale de la loi Informatique et Liberté[109] nécessite des clarifications.[110] C'est ainsi que l'article 51

---

109 Le terme « adéquat » a été remplacé lors de la modification de la loi Informatique et Liberté par la loi de 6 août 2004 par le terme « suffisant » tout en prévoyant dans l'article 68 al.2 que « Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurités qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées ».

de la loi 2004 précise que le caractère adéquat est « *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…* ».

Le problème que soulève l'article 51, et qui a été soulevé par la directive de 1995[111], est le suivant : Est-ce que les Etats-Unis, qui optent, dans la protection des D.C.P., à l'autorégulation à travers des codes de bonne conduite, [112]offrent une protection adéquate aux données transférées vers elles ? Devant ce problème, la négociation [113] entre la commission européenne et le ministère américain de commerce a engendré l'adoption de la sphère de sécurité dite "le safe harbor"[114].

Le safe harbor est un accord en vertu duquel les entreprises adhérentes s'engagent à appliquer et respecter 7 principes protecteurs des D.C.P. transférées[115].

Deuxième partie : Inefficacité de la protection *a posteriori*

Il est difficile pour l'individu de pouvoir s'opposer à la collecte ou au traitement de ses D.C.P. « *C'est bien après la réalisation de l'atteinte que la*

---

110 Art. 25 al. 2 de la directive : «Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de tous les circonstances relatives à un transfert ou à une catégorie de transfert de données ; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, le 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 s'y sont respectées ».

111 Y. POULLET, « Pour une justification des articles 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontalières et de protection des données », Com-Com.Elec., Dec., 2003.,p. 9.

112 J.FRAYSSINET, « Le transfert et la protection des données personnelles en provenance de l'Union Européen vers les Etats-Unis : l'accord dit : sphère de sécurité (ou safe harbor) », Com-Com.Elec., mars, 2001, p.10

113 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., doct., 22 janv., 2004, p.89.

114 Y.POULLET, « Les Safe Harbor Principles- Une protection adéquate ? », Disponible sur : http://www.juriscom.net.

115 J.FRAYSSINET,article précité, p.10 ; Y.POULLET, « Internet et vie privée : entre risques et espoirs », J.T., n° 6000, 17 fev. 2001, p.161.disponible aussi sur : http://www.lancier.be/jt6000

victime aura vocation à intervenir »[116]. Déjà même dans la directive de 1995, on assiste à un « *glissement de contrôle a priori vers un contrôle a posteriori* »[117].

Les victimes qui souhaitent voir leur préjudice réparé se heurtent à la difficulté de l'engagement de la responsabilité civile devant les tribunaux étatiques d'une part (**Section 1**), et à la difficulté du recours à l'arbitrage d'autre part (**Section 2**).

Section 1 : La difficulté de l'engagement de la responsabilité civile

La nature des transactions dans le commerce électronique et la particularité de la relation entre les intervenants en matière de protection des D.C.P. rendent difficile l'engagement de la responsabilité des responsables du traitement, car, malgré l'existence de deux fondements pour engager leur responsabilité, sa mise en œuvre est compliquée et difficile.

A- Les fondements de la responsabilité

Malgré l'absence d'une consécration législative expresse de la protection des D.C.P. dans notre C.O.C., le recours aux textes généraux reste possible. Ainsi, la faute constitue un fondement incontestable pour engager la responsabilité du responsable du traitement, par ailleurs, le droit subjectif offre à la victime un autre fondement qui demeure possible.

---

116 X.AGOSTINELLI, op.cit., p.136.

117 M.P.F-TROUSSEAU et G.HAAS, op.cit., p.31 et s.

L'article 82 C.O.C. dispose que « *Tout fait quelconque de l'homme qui, sans l'autorité de la loi, cause sciemment et volontairement à autrui un dommage matériel ou moral, oblige son auteur à réparer le dommage résultant de son fait, lorsqu'il est établi que ce fait en est la cause directe…* ».

L'article 83 ajoute que « *Chacun est responsable du dommage moral ou matériel qu'il a causé, non seulement par son fait, mais par sa faute, lorsqu'il est établi que cette faute en est la cause directe…*

La faute consiste, soit à omettre ce qu'on était tenu de faire, soit à faire ce dont on était tenu de s'abstenir, sans intention de causer un dommage ».

Ces deux textes constituent la base légale de la responsabilité délictuelle en droit tunisien. En effet, pour que la victime obtienne réparation, elle doit prouver qu'elle a subi un préjudice causé par le fait ou la faute d'autrui.

On en déduit que si le responsable du traitement manque à ses obligations en causant préjudice à la personne concernée, ce dernier peut intenter une action en responsabilité délictuelle pour la réparation du dommage. Mais encore, faut-il qu'il prouve la faute du responsable du traitement, le préjudice et le lien de causalité. La preuve pouvant être ramenée par tous les moyens étant donné qu'il s'agit de prouver un fait juridique.

La faute peut prendre soit la forme d'un fait positif comme la collecte déloyale, le traitement déloyal, la divulgation non autorisée des données ou le détournement de finalité, soit la forme d'un fait négatif telle que le défaut d'information lors de la collecte des données ou le refus de permission d'exercer le droit d'accès et de rectification.

Il est difficile de prouver une faute pareille, mais un jugement pénal fondé sur les articles 199 bis ou 199 ter C.P. peut servir de preuve.

Le deuxième élément pour engager la responsabilité est la réalisation d'un préjudice à la personne concernée. Le préjudice peut être moral ou matériel vu la valeur marchande qu'acquièrent les D.C.P.

L'indemnité allouée doit réparer tout le dommage. La victime ne doit ni souffrir du dommage ni s'enrichir de la réparation[118].

Le troisième élément de la responsabilité est le lien de causalité entre la faute et le préjudice.

Cependant, les inconvénients de l'action fondée sur l'art 82 sont multiples. D'abord, on sait que les audiences lors des jugements sont publiques outre que ces jugements peuvent être publiés. Dès lors, la victime d'une divulgation de ses données sera doublement lésée s'il intente une telle action puisque ses données, qui sont déjà divulguées, feront l'objet d'un jugement publié[119].

Ensuite, il parait difficile de prouver la faute du responsable du traitement surtout lorsque le dommage est dû à une abstention telle que le défaut d'information.

Enfin, le recours ouvert à la victime n'est possible qu'après avoir subi un préjudice, alors qu'il vaut mieux éviter le dommage que de le réparer. Dans ce cas, le recours au référé peut être une solution efficace[120] dès que ses deux conditions, à savoir l'urgence et de ne pas toucher au fond, sont réunies. La doctrine parle même de "référé Internet "[121].Cette institution est consacrée par le législateur français au sein de la loi pour la confiance dans l'économie numérique. Cette mesure appliquée au droit d'auteur et aux droits voisins, dont le droit au respect des D.C.P., est plus simple et efficace contrairement à l'action en responsabilité qui s'avère complexe,

---

118 P. MALAURIE et L. AYNES , Les obligations, Paris, CUJAS, 1999/2000, p. 143.

119 E.LASKARIDIS, « La publicité des jugements civils et la protection des données personnelles », Expertises, juill., 2004, p.263.

120 D. BECOURT, « Réflexions sur le projet de loi relatif à la protection de la vie privée », Gaz.Pal.,1970, 1er sem., doct., p.204.

121 T. VERBIEST, «Projet de loi pour la confiance dans l'économie numérique : analyse critique », Com-Com. Elec., fev.,2003, p.12.

coûteuse, voire même inefficace dans certains cas. L'intervention rapide du juge des référés permet d'éviter le pire.

Tout en affirmant la possibilité pour la victime de fonder son action sur la faute, une partie de la doctrine insiste sur l'idée que la victime possède un droit subjectif qui lui facilite la tâche de demander dommages et intérêts.

Dès 1965, P. Kayser note qu'au-delà des règles de la responsabilité délictuelle, il convient mieux, afin d'assurer une protection plus efficace, d'ériger l'intérêt que possède toute personne au secret de sa vie privée en un droit subjectif[122].

La jurisprudence française antérieure à 1970, date de modification de l'art 9 du Code civil français, a consacré cette idée[123] avant que le législateur français consacre expressément le droit au respect de la vie privée. En effet, l'article 9 du Code civil français dispose que « *Chacun à droit au respect de sa vie privé….* »

La doctrine s'accorde à ce que cet article consacre un véritable droit subjectif[124].

L'article premier de la loi 2004 reprend les dispositions de l'article 9 du code civil en ces termes « *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* ».

---

122 P.KAYSER, « Le secret de la vie privée et la jurisprudence civil », mélange offert à René Savatier, Dalloz, 1965, p.405 et s.

123 T.G.I. Paris, 25 nov.1966, affaire France.Gall, Gaz. Pal., 1967-1, jurisp., p.201. voir aussi N.MEZGHANI, La protection civile de la vie privée, thèse pour le doctorat d'Etat, Université de Droit D'Economie et de Sciences Sociales de Paris II, p. 306.

124 J.CARBONNIER, Droit civil :1/les personnes, Paris, P.U.F., 1988, p.157.

Ce texte consacre un droit subjectif de protection des D.C.P. Mais, si la doctrine est unanime à ce que l'article 9 du code civil consacre un droit subjectif, elle est loin d'être unanime sur la définition de ce droit.

La notion de droit subjectif a été largement controversée. La doctrine a pris le soin de définir et redéfinir le « *droit subjectif* » en se référant à plusieurs critères.[125] Bien que les définitions du droit subjectif soient différentes, elles s'accordent à ce que la victime d'une atteinte à ses D.C.P., n'a pas besoin de prouver la faute d'autrui pour engager la responsabilité de l'auteur de l'atteinte. En effet, l'article 1 de la loi 2004 ne mentionne pas la faute comme condition d'engagement de la responsabilité en cas d'atteinte au D.C.P. L'article 1 de la loi 2004 va jusqu'à considérer qu'il s'agit d'un droit fondamental et que le traitement des D.C.P. doit se faire conformément aux dispositions de la loi. Or, on a vu que, à plusieurs reprises, la loi prévoit quelques exceptions qui peuvent atténuer cette protection, ce qui accentue la crainte que la protection des D.C.P. devienne "*une caricature illusoire des droits subjectifs traditionnels*"[126].

Il faut, en effet, remarquer, comme l'a fait d'ailleurs Pierre Kayser que les deux modes de protection, à savoir la responsabilité délictuelle et le droit subjectif ne s'excluent pas. La victime d'une atteinte aux D.C.P. peut exercer simultanément une action en justice fondé sur le droit subjectif ayant pour objet de mettre fin à l'atteinte, et une autre action en dommages et intérêts, fondée sur la faute de l'auteur de l'atteinte. Mais, vu l'aspect international du commerce électronique, il n'est pas toujours facile de mettre en œuvre cette action.

---

125 SAVIGNY le fonde sur la volonté en le définissant comme « un pouvoir appartenant à la personne, un domaine où règne sa volonté… ».IHERING le fonde sur l'intérêt et le considère comme « des intérêts juridiquement protégés ». Prenant une position intermédiaire, JELLINECK définit le droit subjectif comme « la puissance de volonté humaine reconnue et protégé par l'ordre juridique et qui a pour objet un bien ou un intérêt ». Jean DABIN a définit le droit subjectif en se référant à deux mots à savoir appartenance et maîtrise. En fait, selon lui, le droit subjectif se présente comme une relation d'appartenance entre le sujet et une chose et parce que la chose appartient au sujet, il a un pouvoir sur elle ; Cité par X.AGOSTINELLI , op.cit.,p.119 et s.

126 F.RIGAUX, op.cit., p.766.

B- Difficulté de la mise en œuvre de la responsabilité

Le commerce électronique est par nature un commerce transfrontalier. Dès lors, le droit international privé est invité à gérer le trafic incité par les réseaux électroniques.

Confronté aux effets internationaux du commerce électronique dont il est le plus souvent peu conscient, l'internaute « risque de se perdre dans un labyrinthe juridique »[127]. La complexité conséquente de l'extranéité de l'Internet, ne lui permet guère de prévoir le cadre législatif auquel il doit conformer son comportement sur le web. Les utilisateurs du réseau mondial sont amenés à s'interroger alors sur le juge compétent lors du litige ainsi que sur la loi applicable à ce litige.

Le législateur tunisien a réglementé la question de la compétence judiciaire dans le code de droit international privé (C.D.I.P.), promulgué par la loi n° 97 du 27 novembre 1998. Les articles de 2 à 9 déterminent les chefs de compétence des tribunaux tunisiens. Mais, il faut, au préalable, préciser que l'atteinte aux D.C.P. constitue un délit. Cette qualification est indispensable pour la détermination de la juridiction compétente.

L'article 3 C.D.I.P. consacre la compétence ordinaire des tribunaux tunisiens lorsque le domicile du défendeur est situé sur le territoire tunisien. La notion du domicile doit être comprise à la lumière des articles 7 C.P.C.C.[128] et 10 C.S.C.[129]

---

127 B.D. GROOTE et J-F. DERROITTE, « L'Internet et le droit international privé : un mariage boiteux ? », R. Ubiquité- Droit des technologies de l'information, 2003, n°16, p. 62.

128 L'art 7 C.P.C.C. dispose que « Le domicile réel d'une personne physique est le lieu où elle réside habituellement.
Le lieu ou une personne physique exerce sa profession ou son commerce constitue le domicile réel en ce qui concerne les transactions relatives à cette activité.
Le domicile élu est le lieu indiqué par la convention ou par la loi pour l'exécution d'une obligation ou pour l'accomplissement d'un acte judiciaire »

Cette solution est préjudiciable à la victime d'une atteinte aux D.C.P. en matière de commerce électronique car la victime se trouve souvent obligée de se déplacer d'un continent à un autre pour intenter son action.

L'article 4 C.D.I.P. précise que les tribunaux tunisiens deviennent compétents si le défendeur, non domicilié en Tunisie, accepte d'être jugé par elles. Cette acceptation peut être soit expresse soit tacite si le défendeur ne conteste pas la compétence des tribunaux tunisiens. Toutefois, l'article 10 C.D.I.P. dispose que « *L'exception d'incompétence des juridictions tunisiennes doit être soulevé avant tout débat quant au fond ».* Selon cet article, l'exception d'incompétence doit être soulevée par le défendeur in limine litis[130].

L'article 5 C.D.I.P. est d'une grande importance pour la protection des D.C.P dans le commerce électronique ; son alinéa premier dispose que « *Les juridictions tunisiennes connaissent également :*

1-des actions relatives à la responsabilité civile délictuelle si le fait générateur de responsabilité ou le préjudice est survenu sur le territoire tunisien ».

Cet article offre à la victime une option. En effet, elle dispose d'un choix entre le lieu du fait générateur de la responsabilité et le lieu où le préjudice est survenu.

Toutefois, le problème réside dans la délocalisation du préjudice et notre Code ignore cette éventualité.

L'article 5 de la convention de Bruxelles, tel que interprété par la Cour de Justice des Communautés Européennes, aboutit à une « *universalisation de la compétence des tribunaux dès lors que l'acte litigieux a été commis sur le*

---

129 L'art. 10 al. 2 C.S.C. dispose que « Le siège social est le lieu du principal établissement dans lequel se trouve l'administration effective de la société » .

130 Avant tout débat quant au fond.

réseau »[131]. La jurisprudence française a affirmé cette position dans la fameuse affaire Yahoo ![132]

Cette solution aboutit à admettre que la victime peut intenter son action devant n'importe quelle juridiction.

Dans ce contexte, la Cour de Justice a considéré dans l'affaire Shevill c. Press Alliance que la victime peut intenter une action en dommages et intérêts devant les tribunaux de chaque Etat où la publication a été faite et où la victime peut prétendre avoir subi une atteinte. Mais selon cette jurisprudence, les tribunaux de l'Etat où l'auteur de l'atteinte est situé, ont compétence pour allouer des dommages et intérêts couvrant la totalité du préjudice, alors que les tribunaux de chaque Etat où la publication a été faite, ne peuvent qu'allouer des dommages et intérêts couvrant le préjudice subi respectivement dans chaque pays. [133] Cette solution est confirmée par une autre décision de la même cour dans l'affaire Marinari c. Lloyds Bank dans laquelle, la Cour a estimé que la notion de "lieu où le fait dommageable s'est produit" ne pouvait être entendu de manière trop extensive au point d'englober tout lieu où peuvent être ressenties les conséquences préjudiciables d'un fait ayant déjà causé un dommage effectivement survenu dans un autre lieu[134]. On en déduit que la cour incite la victime, pour obtenir la totalité des dommages et intérêts, à intenter son action devant la juridiction de l'Etat où s'est produit le fait générateur du dommage. Si non, il n'obtiendra qu'une partie des dommages et intérêts qui serait proportionnelle au préjudice subi dans l'Etat dans

---

131 T.VERBIEST, « Proposition de règlement"loi applicable aux obligations non contractuelles" (Rome II) : adaptée aux nouvelles technologies de la communication ? » , Com-Com. Elec., nov., 2003, p.10.

132 J.R.REIDENBERG, « L'affaire Yahoo ! et la démocratisation internationale d'Internet », Com-Com.Elec., mai, 2001, p.14. Le T.G.I. de Paris a affirmé sa compétence dans l'affaire Yahoo !, société américaine, malgré que cette dernière a soulevé l'incompétence des juridictions françaises en cherchant à se réfugier derrière la localisation géographique de ses serveurs.

133 Cour de justice de la communauté européenne, affaire Shevill c. Press alliance, cité par T. VAN OVERSTRAETEN, « Droit applicable et juridiction compétente sur Internet », R.D.A.I. ,n°3,1998, p.379.

134 Cour de justice de la communauté européenne : affaire Marinari c.Lloyds Bank, cité par T. VAN OVERSTRAETEN, article précité, loc.cit.

lequel ce dernier est survenu. Cette solution parait efficace puisqu'elle établit l'équilibre entre le préjudice et le montant de la réparation.

Toutefois, le tribunal de grande instance de Paris a pris, dans deux décisions[135], une position originale. Se basant sur la "théorie de la focalisation"[136] le juge français s'est déclaré compétent dès lors que le site contre lequel l'action est dirigée est accessible depuis le territoire français et que les écrans sont en langue française. Le juge a affirmé que l'emploi de la langue française prouve que le site est destiné aux clients situés notamment sur le territoire français.

Cette position qu'on peut qualifier d'audacieuse, est en mesure d'assurer l'internaute étant donné qu'elle peut réduire l'insécurité juridique qu'engendre l'internationalité du commerce électronique. En fait, cette position permettra à l'internaute de connaître les juridictions compétentes dès qu'il voie la langue par laquelle le site est présenté. Cette théorie serait donc, un facteur de prévisibilité des solutions et non un facteur d'insécurité juridique.

Mais, en l'absence de définition uniforme des critères de la focalisation[137], il serait plus adéquat d'associer à la langue utilisée d'autres considérants. C'est ainsi que le tribunal de grand instance de Paris a fondé son jugement à partir de la nationalité de l'éditeur qui était allemand.

Enfin, dire que le juge compétent est celui de la langue utilisée par le site peut inciter ce dernier à utiliser une langue précise pour échapper à la compétence de certains tribunaux. Dans ce cas, la solution du tribunal de grande instance de Paris semblerait un cadeau empoisonné. C'est un cadeau parce qu'il facilitera la connaissance du juge compétent. Et il est empoisonné parce que ce juge peut être choisi frauduleusement par le site.

---

135 T.G.I. Paris, 11 fev., 2003 et 11 mars 2003, J.D.I., 2004, 2, p. 491 et s.

136 C'est une théorie d'origine américaine qui prend en considération, pour la détermination du juge compétent, le public visé par le site Internet. Par exemple, si le juge français s'aperçoit que le site vise le public français, il se déclare compétent. Voir note de J-S.BERGE, J.D.I.,2004, 2, p.496.

137 O.CACHARD, La régulation internationale du marché électronique, Paris, L.G.D.J., 2002, p. 403.

La difficulté que rencontre la victime de l'atteinte aux D.C.P., en matière de commerce électronique ne s'arrête pas au niveau de la consultation du juge compétent, mais s'étend lors de l'exécution de la décision du juge, surtout lorsque cette décision a été rendue dans un Etat autre que celui dans lequel elle devra être exécutée. Il s'agit du problème de l'exequatur.

L'exequatur est l'ensemble des règles qui ont pour objet de conférer à un jugement étranger une force exécutoire sur le territoire du for[138].

Il est à noter que conformément à l'article 16 C.D.I.P., les actions relatives à l'exequatur sont introduites devant le tribunal de première instance du lieu du domicile de la partie contre laquelle la décision étrangère est invoquée. A défaut d'un domicile en Tunisie, l'action est portée devant le tribunal de première instance de Tunis.

Jusqu'à là, la victime n'est pas au bout de ses peines. La difficulté de la détermination du juge compétent est doublée par celle que trouve le juge pour déterminer la loi applicable au litige. En effet, dans une opération simple du commerce électronique, trois types d'acteurs y participent. Le fournisseur de bien ou de service, le client et un ensemble d'intermédiaires comme le fournisseur d'accès ou le serveur web. Ces personnes, qu'elles soient physiques ou morales, résident souvent dans des Etats différents. Cela aboutit à ce que le moindre litige entre deux intervenants sur le net aura pour conséquence un conflit de loi. Cela est vrai notamment en cas d'action visant à protéger les D.C.P.

Certains avancent que le net est un espace de "non droit"[139] à cause de la nature transfrontalière du net et du changement continuelle des informations sur le

---

138 A.MEZGHANI, Droit international privé, états nouveaux et relations privées internationales, Tunis, éd. CERES, 1995, p.392.

139 C. GADDES, Usuel d'informatique, Tunis, Centre De Publication Universitaire, 2000, p.127.

web. Mais, cette opinion est largement dépassée[140]. Mr. Vincent Tilman affirme que « *dès qu'il est lieu social, il y a de place pour le droit* »[141]. Mais, déterminer la loi applicable à un litige de commerce électronique n'est pas facile. En effet, la compétence du juge du for n'implique pas forcément l'application au fond de la lex fori, et vice versa. Dans une affaire de droit international privé, le juge va consulter sa propre règle de conflit pour déterminer la loi applicable. La règle de conflit est « *une norme juridique qui désigne la règle à régir un litige comportant un élément d'extranéité par référence à un élément de rattachement* »[142].

L'article 70 C.D.I.P. dispose que « *La responsabilité extracontractuelle est soumise à la loi de l'Etat sur le territoire duquel s'est produit le fait dommageable.*

Toutefois, si le dommage s'est produit dans un autre Etat, le droit de cet Etat est applicable à la demande de la victime …».

Cet article consacre, en principe, la lex loci delicti. Toutefois, il laisse la possibilité à la victime, si le dommage s'est produit dans un autre Etat, d'exiger l'application du droit de cet Etat.

La mise en œuvre de cette règle dans le commerce électronique parait difficile. En fait, le dommage causé par l'atteinte aux D.C.P. peut survenir partout dans le monde et dans ce cas, on ne peut pas voir toutes les lois du monde s'appliquer en une même affaire. Dans ce contexte, la Cour d'appel de Paris a déclaré que « *La publication d'un texte sur un site Internet rend celui-ci consultable depuis tous les pays du monde sans pour autant être adressé à un destinataire précis. Ainsi par la nature même du support la possibilité d'accès est universelle, il ne saurait cependant en résulter une applicabilité de tous les droits*

---

140 W.CAPLLER, « Un net pas très net. Réflexions sur la criminalité virtuelle », Arch. Phil. Droit, n°43, 1999, p.180.

141 V.TILMAN, « Arbitrage et nouvelles technologies : Alternative cyber dispute résolution », R. Ubiquité, 1999, n°2, p.47-64 ; disponible sur : http://www.droit.fundp.ac_be/textes/ADR.

142 M.A. HACHEM, Leçon de droit international privé, Livre II, Tunis, Centre de Publication Universitaire,1997, p. 29.

existants au contenu du texte ce qui aboutirait à créer une totale insécurité juridique… »[143].

L'article 70 alinéa premier C.D.I.P. déclare applicable la loi du lieu du fait générateur de la responsabilité. Il en résulte qu'un site américain ayant collecté et divulgué des données d'un tunisien va se voir appliquer la loi américaine qui ne condamne pas ces pratiques. Il est clair alors, que l'application de la loi du pays du fait générateur permettrait des abus. « *Il est facile, par ce biais, d'instaurer des paradis informationnels ou pourrait instillées en toute impunité les pires choses* »[144], et dans ce cas, la fraude à la loi pourrait être invoquée[145].

Devant ce problème, l'article 26 C.D.I.P. Vient au secours du juge. Ledit article dispose que « *Lorsque le rapport juridique est international, le juge fera application des règles prévues par le présent code, à défaut de règles, il dégagera la loi applicable par une détermination objective de la catégorie juridique de rattachement* ».

Cet article consacre le principe de proximité. Il « *exprime l'idée du rattachement du rapport du droit à l'ordre juridique avec lequel il présente les liens les plus étroits* »[146].

Mais, la règle de l'article 26 C.D.I.P. rend la loi applicable imprévisible. C'est pourquoi le professeur Ali MEZGHANI parle même du rejet du principe de proximité.[147]

Consciente de l'importance de la question, la Commission Européenne a rendu public le 22 juillet 2003 une proposition de règlement qui vise à harmoniser

---

143 C.A.Paris, 10 nov. 1999, cité par M.VIVANT, « Le commerce électronique, défi pour le juge », D., 2003, n°10, note 3, p.675.

144 M. VIVANT, « Cybermonde : Droit et droit des réseaux », J.C.P., 1996, éd .G., n°43, p.403.

145 T.VERBIEST et B. VANDEVELDE, article précité, p.3.

146 A. MEZGHANI, Commentaire du code de Droit International Privé, Tunis, Centre de Publication Universitaire, 1999, p. 39.

147 A. MEZGHANI, Commentaire du code de Droit International Privé, Tunis, Centre de Publication Universitaire, 1999, loc.cit.

les règles concernant la loi applicable aux obligations non contractuelles (Rome II)[148]. Ce texte aura vocation à s'appliquer aux litiges survenant sur Internet, y compris l'atteinte à la vie privée et aux droits de la personnalité.

Devant l'échec de la méthode conflictuelle traditionnelle, la doctrine affirme « *qu'un véritable lex electronica…est en train de se développer* »[149].

Monsieur Vincent Gautrais définit la lex electronica comme « *l'ensemble des normes juridiques informelles applicable dans le commerce électronique international* »[150].

Ainsi définies, les règles de la lex electronica seront des règles spontanées qui n'ont pas une origine étatique mais plutôt, ce sont les acteurs du commerce électronique qui vont les édicter. En effet, la directive 95/46/CE incite les Etats membres de la Commission Européenne à encourager l'élaboration de code de conduite, [151]ce qui aboutirait à une autorégulation.

Dans le même contexte, l'ancien premier ministre français Lionel Jospin a déclaré le 25 août 1997 qu' « *il appartient d'abord aux acteurs d'Internet de prendre en charge eux-mêmes ce qui peut relever d'une régulation préventive du réseau. Celle-ci, en s'appuyant sur des règles de conduite et une déontologie, doit concilier la lutte nécessaire contre le dévoiement auquel Internet peut donner lieu et le respect de la liberté de communiquer qui fait sa richesse* »[152].

Parmi les procédures qui dégagent des règles de lex electronica, il y'a l'arbitrage en matière de commerce électronique. Toutefois, il est difficile d'y recourir lorsqu'il s'agit d'un cyber-litige.

---

148 T.VERBIEST, article précité, p.10.

149 W.CAPELLER, article précité, p.180.

150 V.GAUTRAIS, « Y'a t-il une lex electronica ? », Disponible sur : http://www.bureau.qc.ca/journal/frameset.asp?article=/journal/vol30/no21/lex.html.

151 Voir art. 27 de la directive 95/46/CE.

152 M-A.MAURY, Faculté Jean Monnet-Université Paris- sud, La lex electronica, D.E.S.S de droit informatique et technologies nouvelles, 1997-1998, p. 16. Disponible sur : http://perso.wanadoo.fr/mam/these 4. htm.

Section 2- La difficulté du recours à l'arbitrage

L'article premier du code de l'arbitrage (C.A.) définit l'arbitrage comme étant « *un procédé privé de règlement de certaines catégories de contestations par un tribunal arbitral auquel les parties confient la mission de les juger en vertu d'une convention d'arbitrage* ».

Le caractère technique du commerce électronique peut être un argument pour l'adoption de l'arbitrage. Les parties peuvent designer parmi les arbitres des experts en commerce électronique.

Cela ne cache pas la difficulté du recours à ce procédé, voire son inadaptation au commerce électronique d'une part, et la méfiance à l'égard de l'arbitrage en ligne d'autre part.

A-Inadaptation du procès arbitral ordinaire

L'inadaptation du procès arbitral ordinaire est due d'une part, au caractère délocalisé du litige en matière de commerce électronique, d'autre part, à la question de la preuve de la convention d'arbitrage.

Il est évident de rappeler que dans les litiges naissants sur le net, les parties appartiennent souvent à des Etats différents. D'autant plus qu'en cas de recours à l'arbitrage, le lieu du procès peut être situé dans un Etat autre que celui des parties. On en déduit qu'il s'agit ici d'un arbitrage international[153]. Or, on voit mal comment un arbitre localisé dans un Etat peut statuer sur un cyber-litige délocalisé. Le problème se complique davantage lorsqu'il s'agit d'une atteinte aux D.C.P.

---

153 L'art 48 C.A dispose que « l'arbitrage est international dans l'un des cas suivants :
…b-Si l'un des lieux si après indiqués est situé hors de l'Etat dans lequel les parties ont leur établissement :
1- Le lieu de l'arbitrage, s'il est stipulé dans la convention d'arbitrage ou déterminé en vertu de cette convention… ».

Cette délocalisation du litige pose le problème de la loi que va appliquer l'arbitre. L'article 73 C.A. dispose que « *Le tribunal arbitral tranche les différends conformément à la loi désignée par les parties. A défaut d'une telle désignation, le tribunal arbitral applique la loi qu'il estime appropriée…* ».

L'expression "phare" de cet article est "la loi qu'il estime appropriée". Cette expression nous ramène au même problème que rencontre le juge étatique.

Il s'y ajoute la difficulté que rencontreront les parties pour exercer les voies de recours. Faut-il rappeler qu'en matière d'arbitrage international, le seul recours possible est le recours en annulation de la sentence arbitrale devant la cour d'appel de Tunis et dans des cas précisés par l'article 78 C.A.

Il est évident que pour être efficace, la sentence arbitrale doit être exécutée. Or, l'exécution d'une sentence en matière de protection des D.C.P. dans le commerce électronique paraît délicate. L'article 80 alinéa premier C.A. dispose que « *La sentence arbitrale, quel que soit le pays où elle a été rendue, a l'autorité de la chose jugée prévue à l'article 32 du présent code. Elle est exécutée sur requête écrite adressée à la Cour d'appel de Tunis…* » .

Cet article exige, pour avoir l'exequatur, d'adresser une requête écrite à la cour d'appel de Tunis. Or, lors d'une atteinte aux D.C.P. dans le commerce électronique, la sentence nécessiterait un exequatur dans tous les Etats où est survenu le dommage. Par exemple, si l'arbitre décide que le site doit effacer des données qui concernent une personne, cet effacement doit être universel. Pour voir cette sentence s'exécuter, la victime, malheureuse, devra avoir l'exequatur partout où le site est disponible, ce qui est très pénible. La tâche de la victime se complique davantage lorsque ses D.C.P. sont diffusées par plusieurs sites.

A tout cela s'ajoute le problème de la preuve de la convention d'arbitrage.

La convention d'arbitrage peut revêtir la forme d'une clause compromissoire [154] ou la forme d'un compromis [155]. Cependant, en matière délictuelle, il y a place souvent aux compromis plutôt qu'aux clauses compromissoires étant donné que l'atteinte est imprévisible.

L'art 6 C.A. dispose que « *La convention d'arbitrage ne peut être établie que par écrit, soit par acte authentique ou sous seing privé, soit par procès-verbal adressé auprès du tribunal arbitral choisi.*

La convention d'arbitrage est réputée établie par écrit lorsqu'elle est consignée dans un document signé par les parties ou dans un échange de lettres, de communication télex, de télégrammes ou de tout autre moyen de communication qui en atteste l'existence, ou encore, dans l'échange de conclusions en demande et de conclusion en défense, dans lesquelles l'existence d'une convention d'arbitrage est alléguée par une partie et n'est pas contestée par l'autre ».

L'alinéa premier exige que la convention d'arbitrage soit établie soit par acte authentique soit par acte sous seing privé. Or, dans une relation de commerce électronique, les parties résidents souvent dans deux Etats différents, seront dans l'impossibilité de rédiger un tel écrit. Seul un échange d'e-mail ou un document électronique[156] peut témoigner de la convention d'arbitrage.

L'alinéa 2 permet aux parties d'établir la convention d'arbitrage par « *tout autre moyen de communication qui en atteste l'existence* ».

---

154 « La clause compromissoire est l'engagement des parties à un contrat, de soumettre à l'arbitrage, les contestations qui pourraient naître de ce contrat ». art. 3 C.A.

155 « Le compromis est l'engagement par lequel les parties à une contestation déjà née, soumettent cette contestation à un tribunal arbitral ». art. 4 C.A.

156 L'art 453 bis C.O.C. dispose que « Le document électronique est l'écrit composé d'un ensemble de lettres et chiffres ou autres signes numériques y compris celui qui est échangé par les moyens de communication à condition qu'il soit d'un contenu intelligible, et archivé sur un support électronique qui garantit sa lecture et sa consultation en cas de besoin ».

Cela permet de considérer que l'écrit électronique pourrait être admis en tant que procédé de preuve après la réforme de juin 2000[157] attribuant à l'écrit électronique la valeur probante d'un acte sous seing privé.

Mais l'effort du législateur tunisien se heurte à l'article 80 C.A. En effet, si le législateur a reconnu la signature électronique et a donné au document électronique la force probante d'un acte sous seing privé, il ne semble pas avoir pensé aux effets de cette reconnaissance. L'alinéa 2 de l'article 80 C.A. dispose que « *La partie qui invoque une sentence arbitrale ou qui en demande l'exécution doit en produire l'original dûment authentifié ou une copie certifiée conforme, ainsi que l'original de la convention d'arbitrage…ou une copie certifiée conforme…* ».

Cet article exige l'original de la sentence d'arbitrage pour obtenir l'exequatur. Or, qu'est-ce qu'un original et qu'est-ce qu'une copie dans le commerce électronique ? Si le même document est enregistré sur trois disques durs, à savoir ceux de l'arbitre et des parties, comment distinguer l'original d'une copie ?

Tout en admettant qu'il est impossible de transposer cette condition à L'environnement électronique[158], la doctrine propose deux approches pour concilier les textes[159]. La première est historique, selon laquelle « *Si la fonction de l'original se comprenait bien autrefois, conformément aux standards de sécurité en vigueur et conformément à l'utilisation du papier, elle a perdu de sa pertinence dès lors que l'on souhaite la transposition à la situation d'aujourd'hui* »[160].

La deuxième est fonctionnaliste, et selon laquelle « On tente d'identifier les fonctions de l'original apportait au papier et on vérifie après si la technique permet

---

157 Loi n°2000-57 du 13 juin 2000.

158 E.A.CAPRIOLI, « Contribution à la définition d'un régime juridique pour la conservation des documents : du papier au message électronique », D.I.T. 1993, n°3, p.5.

159 V.GAUTRAIS, K.BENYEKHLEF et P.TRUDEL, « Les limites apprivoisées de l'arbitrage cybernétique : l'analyse de ces question à travers l'exemple du Cybertribinal », Rev.jur.Thèmis.,1999, p.578, disponible sur : http://www.themis.umontreal.ca.

160 *Ibidem*, loc.cit.

au document électronique de remplir les mêmes fonctions »[161]. C'est cette approche que l'article 8 de la loi type C.N.U.D.C.I. sur le commerce électronique a adopté. Le législateur tunisien a manqué l'occasion de l'intervention de juin 2000 pour adopter cette solution.

Ces problèmes que rencontre l'arbitrage s'accentuent lorsqu'il s'agit d'un arbitrage en ligne.

B-Méfiance à l'égard de l'arbitrage en ligne

La méfiance à l'égard de l'arbitrage en ligne s'explique par deux facteurs. D'une part, un élément de droit qui est l'inadaptation des textes à ce mode de règlement des litiges. D'autre part, un élément de fait qui est le manque de confiance en ce mode.

Bien que, techniquement, on peut envisager un arbitrage en ligne, juridiquement, il faut qu'un tel arbitrage soit compatible avec les textes en vigueur. Or, ceci n'est pas évident. Des problèmes de fond et de forme se posent.

En fait, l'exigence de la capacité dans l'article 8 C.A. est difficile à vérifier dans le cadre du commerce électronique où les parties peuvent simuler leur âge réel, d'autant plus que l'âge de la capacité diffère d'un Etat à un autre.

Le problème de l'écrit dans le cadre de l'arbitrage en ligne se pose d'une façon cruciale[162]. En effet, outre l'exigence de l'écrit lors de la conclusion de la convention d'arbitrage et lors de l'exequatur, l'écrit est exigé aussi lors du déroulement de l'instance et lors du prononcé de la sentence. Lors du déroulement de l'instance, les pièces versées aux débats doivent être par écrit telles que le rapport de l'expert ou la notification. En ce qui concerne la forme de la sentence, l'article 75 C.A. dispose que « *La sentence arbitrale est rendue par écrit et signée*

161 Ibidem, loc.cit.
162 Ibidem, p.111.

par l'arbitre ou les arbitres… ». Cette exigence est inadaptée à l'arbitrage en ligne dans lequel, la sentence sera enregistrée sur un support électronique. Le règlement du Cybertribunal prévoit que la sentence est exposée sur le site de l'affaire en cours et qu'une signification en est aussi tôt adressée aux parties par l'arbitre. Il est fort probable donc que cette signification soit par courrier électronique, avec, éventuellement, accusé de réception.

L'arbitrage en ligne est loin d'avoir des traditions. Les deux plus célèbres Cours d'arbitrage électronique sont le Virtual Magistrate[163] et le Cybertribunal[164].

Le Virtual Magistrate est un projet américain qui a débuté en 1996 et qui émet des sentences "en ligne" pour toute personne qui accepte de se soumettre à ce forum. En fait, la violation de la vie privée fait partie des litiges que le Virtual Magistrate peut trancher. Pour rendre sa décision, le Virtual Magistrate n'applique pas systématiquement un droit d'une juridiction spécifique. Il statue en équité. Les parties doivent s'engager à respecter la décision de l'arbitre et il n'y a pas d'appel possible[165].

Il faut noter que le fait de priver les parties d'un appel éventuel est une cause sérieuse de manque de confiance en ce procédé.

En ce qui concerne le Cybertribunal, c'est un projet du Centre de Recherche en Droit Public de Montréal. Etabli en 1996, le Cybertribunal est encore en stade expérimental. Il se distingue du Virtual Magistrate par un champ de compétence plus large qui comporte le commerce électronique, la liberté d'expression, la vie privée…[166]

Actuellement, le Cybertribunal offre des services d'arbitrage gratuitement, et malgré cela, aucune demande n'a encore été introduite, ce qui prouve que la cause

---

163 Voir : http://vmag.law.vill.edu:8080

164 Voir : http://www.cybertribunal.org

165 V.TILMAN, article précité, p. 52.

166 E.A.CAPRIOLI, « Arbitrage et médiation dans le commerce électronique (L'expérience du Cyber Tribunal) », R.A.,1999, n°2, p. 231.

de la négligence de l'arbitrage en ligne n'est pas d'ordre pécuniaire. L'absence de saisine est due à un manque de confiance. En effet, monsieur Vincent Tilman avoue que « *La procédure d'arbitrage recèle aux yeux des internautes un certain danger* »[167]. Il ajoute que « *Cette procédure souffre dans le cyberespace, d'un manque de confiance qui remet en question les projets actuels. Les petits surfeurs ne veulent pas utiliser une procédure inconnue alors que les grands préfèrent recourir au système judiciaire qui leur assure la légitimité de la décision* »[168]. On peut donc rejoindre la doctrine qui affirme qu'il s'agit essentiellement de manque de confiance qui a retardé le développement de l'arbitrage en ligne

La création d'un tribunal spécial pour traiter du droit de l'Internet est une voie longue semée d'embûches[169]. Confronté à ce risque, l'internaute reste hésitant et perdu entre un arbitrage en ligne qui souffre encore des douleurs de la naissance, et une procédure de médiation qui risque d'échouer.

Devant cette polémique, l'intervention des moyens techniques et administratifs paraît plus que nécessaire pour assurer à l'internaute une protection effective et efficace de ses D.C.P.

---

167 V.TILMAN, article précité, p. 9.
168 *Ibid.*, loc.cit.
169 *Ibid.*, p. 61.