Première partie :

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.

A- Le droit à l'information

On entend par le droit à l'information le droit que possède la personne concernée dans une opération quelconque (par exemple opération de commerce électronique) d'obtenir du traitant des données (par exp le cyber 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 de l'opération. 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, 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) ainsi que les mesures de sécurité garantissant l'authenticité du site, l'intégrité et la confidentialité des informations transmises sur le réseau.

Il s'ajoute à tout cela **les modalités d'information**. L'information doit être fournie d'une façon pratique et efficace. L'article 31 insiste 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, 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.

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 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.

Toutefois, 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 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.

L'exercice du Droit d'opposition : Le droit d'opposition devra s'exercer d'une manière aisée et gratuite. En pratique, la personne exprime son opposition soit en marquant "la case à cocher" soit en décochant cette case.

Le droit d'opposition, consacré aussi par la directive 95/46/CE66 qui a été abrogé et remplacé par le RGDP le 25-05-2018, 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.

On peut se demander si le droit d'opposition peut jouer lorsque les données n'ont pas été collectées directement. On se demande aussi 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 ? Le droit d'accès et de communication nous donnera une réponse à ces demandes.

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 ».

On considère que le droit d'accès constitue la pierre angulaire de la protection des données 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.

Les procédures d'exercice du droit d'accès : 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.

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. Cependant, ce droit "peut être utilisé pour protéger des intérêts patrimoniaux".

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 ».

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. On peut se demander si la demande d'accès une fois par semaine est excessive ?

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…».

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.

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". 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 sont des « petits programmes espions » 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 ». Les cookies permettent alors, d'assurer la traçabilité de la navigation et transforment, dès lors, la souris en véritable "bracelet électronique".

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 », 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 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 par exemple ?

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. Le ministre a répondu à travers un exemple qui se rapporte au domaine médical 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, 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 consiste en « la diffusion généralisée de messages non sollicitées à un grand nombre d'utilisateurs de l'Internet ».

Devant les inconvénients du spamming, 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 ». Ce système est fondé sur le principe 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. 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 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, 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 cybercommerçant 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", ce qui réduit l'efficacité et la portée du principe de finalité.

C-La sécurité des données

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 18 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[1], l'article 34 de la loi Informatique et Liberté et l'article 7 de la convention 108.

[1] Il est à noter que cette directive 95/46/CE (règlement général sur la protection des données) a été abrogée par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif

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". Le droit à l'oubli est le droit de voir les données oubliées après un certain temps.

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. 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 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'article 24 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 prend les mesures appropriées pour la destruction.

à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

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.

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 et doivent être détruites.

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 pour ses clients constitue un traitement, 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 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. ».

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».

Le consentement doit aussi être **spécifique**, il « doit porter sur des traitements précisément définis et non sur des objets généraux ».

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 ».

Ensuite, si la personne est incapable ou interdite ou incapable de signer, le consentement est régi par les règles générales de droit. 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 ».

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. Ces données acquièrent "une valeur marchande" qui séduit ces sociétés à les commercialiser et incite même leur titulaire à les vendre ; ainsi, la doctrine s'est posée la question si "nous allons devoir vendre nos données personnelles ?" 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 «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[2] nécessite des clarifications. C'est ainsi que l'article 51 de la loi 2004 précise que le caractère adéquat est « apprécié

[2] 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 ».

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, 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, offrent une protection adéquate aux données transférées vers elles ? Devant ce problème, la négociation entre la commission européenne et le ministère américain de commerce a engendré l'adoption de la sphère de sécurité dite "le safe harbor".

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.