http://www.droit-technologie.org

présente :

L'informatique et la protection de la vie privée

Luc GOLVERS

Ingénieur Civil
Consultant et expert en informatique auprès des Tribunaux
Président du Club de la Sécurité Informatique belge
golvers@compuserve.com

11 janvier 2001

Remarque liminaire : les vues exprimées dans ce document représentent celles de l'auteur et n'engagent en rien la Commission de la Protection de la Vie Privée.

Ce texte a pour objet de présenter les risques particuliers que l'usage de l'informatique peut faire naître au regard de la vie privée, ainsi que des mesures de protection qui peuvent être envisagées.

On observera d'emblée que la notion de vie privée paraît être un concept si bien compris que personne ne peut le définir. En effet, ni la législation belge ni celle des autres pays ayant légiféré en la matière ne présentent de définition de la notion de vie privée. Il s'agit apparemment de ce « cocon » immatériel que l'on ne peut violer sans choquer ce que nous ressentons être du ressort de notre intimité. La notion de vie privée est perçue différemment de pays en pays. Dans certains pays, le revenu imposable de chaque citoyen est public. Chez nous, il est considéré comme confidentiel. La notion de vie privée évolue également dans le temps, au même titre que ce que l'on considère comme films interdits aux enfants. Autres temps autres mœurs.

La loi du 8 décembre 1992, modifiée par celle du 11 décembre 1998, transposant la directive 95/46/CE du 24 octobre 1995 du Parlement Européen et du Conseil, ne traite pas de la protection de la vie privée en général mais bien de la protection de la vie privée à l'égard des traitements de données à caractère personnel. Elle concerne aussi bien des traitements, automatisés en tout ou en partie, que des traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Avant d'aborder cette matière, il convient de définir certaines notions de base. L'**information** est immatérielle. C'est une augmentation de notre savoir ou une réduction de notre incertitude. Nous pouvons être informés de quelque chose parce que nous l'observons. Il en va ainsi lorsque nous assistons personnellement à un événement. Souvent, notre savoir ne provient pas de l'observation directe mais bien de ce que faisons usage d'un système d'information, tel que la presse, un livre ou un système informatique. Notre information provient alors de notre interprétation des **données** que nous recevons. Ces données ont une existence matérielle dans la mesure où elles font l'objet d'une inscription sur un support. Les inscriptions et, partant, les données, peuvent être traitées, copiées, détruites. Diverses **technologies** de traitement de données existent qui varient par le système de codification et le support utilisés. Les **systèmes de codification** font en sorte que la même information peut être représentée de diverses manières. Un montant peut être représenté sous forme de chiffres romains ou de chiffres arabes, sous forme de texte en toutes lettres ou sous forme binaire pour traitement par un ordinateur. Les divers **supports** font que ce même montant peut se trouver imprimé sur papier, apparaître sous forme de scintillement sur un écran cathodique, sous forme d'impulsions sur un câble téléphonique, sous forme de bits magnétisés sur une disquette.

La loi du 8 décembre 1992, modifiée par celle du 11 décembre 1998, concerne effectivement le traitement des données à caractère personnel, qui sont matérielles et non de l'information, qui est immatérielle.

Un fichier est un ensemble de données. Celles-ci peuvent être du texte, des données numériques, des graphiques, des images, des sons, des enregistrements vidéos,…

La loi du 8 décembre 1992 parlait de manière fort malheureuse de traitements automatisés et de fichiers manuels. Il s'agissait d'une confusion de concepts et d'une terminologie non appropriée. En effet, des données peuvent être lisibles par l'homme ou par une machine. Une disquette est illisible par l'être humain. Pour que nous puissions prendre connaissance des données qu'elle contient, nous devons nécessairement l'introduire dans une machine qui la décodera et nous fera apparaître son contenu sur écran ou sur papier sous forme de symboles que nous pourrons comprendre.

Ce sont en revanche les traitements qui peuvent être manuels ou automatisés. La loi du 8 décembre 1992 aurait dès lors dû plutôt utiliser la qualification de « fichiers lisibles par l'homme » ou de dossiers « papier » plutôt que de « fichiers manuels ». Par ailleurs, la distinction faite par la loi de 1992 est devenue obsolète au regard des progrès réalisés dans les techniques de « scanning » et de reconnaissance optique de caractères. Les anciens fichiers dits « manuels » peuvent facilement être digitalisés et enregistrés dans un ordinateur, ce qui permet leur traitement automatisé.

L'application de la loi du 8 décembre 1992 a donné lieu à de futiles discussions importées de la jurisprudence française et relatives à la nécessité d'établir une distinction entre la notion de fichier et de dossier, pour notamment éviter une application de la loi aux fichiers manuels. Cette distinction est aussi subtile qu'impraticable. Il est en outre évident que certains fichiers dits « manuels » dans le texte de cette première loi peuvent présenter des risques importants d'atteinte à la vie privée, ne fût ce qu'en raison de leur difficile tenue à jour qui fait que souvent ils contiennent des données inexactes sur base desquelles des décisions préjudiciables peuvent être prises.

La nouvelle loi du 11 décembre 1998, transposant la directive européenne 95/46/CE, a fort heureusement clarifié la situation et introduit des définitions claires et cohérentes des concepts utilisés. C'est ainsi que cette loi entend pour son application :

- Par « données à caractère personnel », toute information concernant une personne physique identifiée ou identifiable ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;

  Ainsi des identifiants de personnes physiques tels que n° de carte d'identité, n° de carte de crédit, n° de compte bancaire, n° de sécurité sociale, n° de carte Proton, etc., sont à considérer comme des données à caractère personnel. Il en va de même d'informations codées pour lesquelles le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent, parce qu'il ne possède pas les clefs nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne ;

- Par « traitement », la loi entend toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel ;

- Par « fichier », la loi entend tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

La question se pose de savoir si ce sont les fichiers ou les traitements qui présentent un danger pour la vie privée. La loi française est principalement orientée « fichiers ». La loi belge est orientée « traitements ». Ces deux notions sont indissociables. En effet, un fichier sur lequel ne serait effectué aucun traitement ne présente aucun risque. Inversement, un traitement n'exploitant pas de fichier est inoffensif. Un traitement fait donc nécessairement usage de fichiers et le danger vient de l'existence conjointe de ces deux notions.

Quels sont les risques particuliers que l'informatique a fait naître en matière d'atteinte à la vie privée ? Les causes sont multiples :

- **fichage aisé grâce à la saisie automatisée de données**

  Nombre d'opérations de la vie courante laissent des traces dans des systèmes informatiques : les appels téléphoniques et l'emploi de cartes de paiement sont mémorisés aux fins de facturation; l'utilisation d'un badge protégeant l'accès à des locaux permet de suivre les déplacements de son détenteur;

  Le « shopping » électronique via les autoroutes de l'information se développe à un rythme accéléré; nos thèmes d'intérêt dans les catalogues que nous feuilletons, ainsi que les articles et les ouvrages littéraires que nous commandons peuvent être enregistrés; ces informations peuvent donner de sérieuses indications quant à notre personnalité profonde; elles intéressent au premier plan les fournisseurs pour étudier le comportement des consommateurs et de leurs clients; le risque existe qu'elles puissent être détournées à d'autres usages.

- **possibilité de gérer des fichiers colossaux**

  Les autorités publiques, des entreprises et des organisations privées gèrent des fichiers de données à caractère personnel concernant des populations énormes; les progrès technologiques ont permis la constitution de bases de données colossales; l'Eglise des Mormons s'est engagée dans un projet de fichage de la population mondiale, y compris celle de nos ancêtres; on peut aisément imaginer les risques liés au rapprochement de cette base de données avec les données génétiques des individus; le temps n'est plus éloigné où nos scientifiques auront achevé de dresser l'entièreté de la carte génétique de l'être humain;

  La concentration de l'information dans une seule base de données crée des risques qui n'existaient que dans une proportion beaucoup plus faible avec les fichiers « papier » ; il en est ainsi des risques d'accès non autorisé ou de copiage intégral;

- **surveillance permanente et généralisée rendue possible**

  Les autorités publiques multiplient les systèmes de vidéo-surveillance; nos villes et nos routes sont parsemées de caméras; les progrès enregistrés en traitement et reconnaissance d'images font que bientôt il sera bientôt possible de « montrer » la photo d'un individu à un système informatique de surveillance et de demander aux

diverses caméras de le rechercher et de le suivre; ce système peut être très utile pour faciliter la détection de personnes se présentant sous de fausses identités mais les dérives d'utilisation sont réelles;

La reconnaissance automatisée des caractères d'une plaque d'immatriculation permet semblablement de suivre à la trace les déplacements d'un véhicule; l'inclusion de micro-émetteurs, suggérée par d'aucuns comme moyen de lutte contre le vol des véhicules, présente des dangers encore plus préoccupants.

- **sélection sur base de critères discriminants**

Nombreuses sont les bases de données contenant des données sensibles relatives à l'ethnie, les convictions philosophiques, religieuses et politiques ou à l'état de santé psychique ou physique des personnes; certes, les législations en matière de protection de la vie privée prévoient des dispositions interdisant ou réglementant strictement le fichage de pareilles données;

Si, dans un régime démocratique, nanti de moyens efficaces de contrôle du respect de la réglementation, les risques sont limités mais réels, il n'en serait plus de même si ces outils tombaient aux mains d'un régime totalitaire; la seconde guerre mondiale a montré combien l'exploitation de fichiers pouvait avoir de conséquences désastreuses; la multiplication des bases de données publiques et privées, ainsi que de leurs copies de sauvegarde, fait que l'on peut raisonnablement douter que celles-ci ne puissent être toutes détruites en cas d'invasion ou de prise de pouvoir par un régime non démocratique.

Les techniques de profilage sur base de critères discriminants ont montré leur redoutable efficacité dans la traque aux criminels et aux terroristes. Les services de police allemands ont exploité avec succès cette stratégie dans leur lutte contre les terroristes de la « Rote Armee Fraktion ». Ils ont dressé le profil-type du terroriste et notamment son comportement au niveau de déménagements d'habitation, de paiement de notes de gaz, d'électricité, de téléphone,… Les policiers ont ensuite effectué des recherches dans les ordinateurs de compagnies de gaz, électricité, téléphone,… Au terme de fusions de fichiers et d'extractions sur base de leurs critères de recherche, ils ont abouti à une liste suffisamment courte de personnes qui ont pu être mises sous surveillance. A leur plus grande surprise, ainsi qu'à celle de celui qu'ils ont appréhendé, ils ont ainsi pu procéder à l'arrestation d'un terroriste qui ne se croyait pas menacé car il n'était pas fiché par les services de police et sa photo n'était pas affichée dans tous les lieux publics avec celles des autres membres de la bande « Bader-Meinhof ».

- **rapprochement de fichiers**

Voici un scénario fictif : M. DUPONT habite à Wavre; il quitte son domicile et chemin faisant prend de l'essence à la station de Wetteren; il paie au moyen de sa carte électronique; "Bing" fait le système informatique ! L'ordinateur de l'entreprise de M. DUPONT dit que celui-ci était inscrit à un séminaire à Namur; peu de temps après, il réserve une chambre double et une table deux couverts dans un restaurant romantique au bord des canaux de Bruges; il utilise sa carte de crédit pour confirmer la réservation à l'hôtel; "Bing" refait le système informatique ! L'ordinateur de l'hôpital signale que Mme DUPONT vient d'être admise en observation; peu de temps après,

M. DUPONT utilise à nouveau sa carte de crédit pour payer l'achat d'un chemisier en soie, taille 38; "Bing" refait le système informatique ! L'ordinateur constate que Mme DUPONT à une taille 42.

Pure science-fiction bien sûr…ou avez-vous un doute quant au fait que ceci pourrait appartenir au domaine du possible ?

En fait, chacun des gestes accomplis par M. DUPONT fait partie de nos actes quotidiens; pris individuellement, ils ne posent pas problèmes; c'est le rapprochement des divers morceaux du puzzle qui permet d'aboutir à la conclusion à laquelle vous n'aurez pas manqué d'aboutir et qui concerne pleinement la vie privée de M. DUPONT.

L'étude des relevés de cartes de crédit et de paiement appartient désormais aux contrôles de routines effectués par les services judiciaires pour reconstituer l'emploi du temps de suspects.

- **cession de fichiers**

  La facilité avec laquelle on peut copier des fichiers a créé un risque nouveau, à savoir la communication de fichiers à des tiers qui peuvent les utiliser pour des finalités différentes de celles pour lesquelles le fichier initial fut constitué;

  Exemple : vous commandez des vêtements à une société de vente par correspondance; vous vous situez dans les grandes tailles; peu de temps après, vous recevez dans votre boîte aux lettres une publicité personnalisée émanant d'une société proposant des cures d'amaigrissement.

  En France, la Commission « Informatique et Libertés » a lancé le slogan *« Adresse cédée = adresse informée »*, qui a pour but que toute personne reprise dans un fichier soit informée lorsque ce fichier est cédé à un tiers et puisse ainsi éventuellement s'y opposer.

  La nouvelle loi du 11 décembre 1998 prévoit également une protection en ce sens. Elle confère à la personne concernée un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de marketing direct. La personne concernée doit être informée avant que les données ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de marketing direct.

- **automatisation de la prise de décisions**

  Le recours aux systèmes experts et d'intelligence artificielle ne cesse de se développer : évaluation de la solvabilité lors de demandes de cartes de crédit, acceptation de risques d'assurances, …; le danger existe que l'être humain ne fasse dans ces circonstances l'objet de décisions qui seraient prises par un système informatique. Le permis de conduire à points en est un exemple potentiel.

  La loi du 11 décembre 1998 comble une lacune de la loi du 8 décembre 1992. Elle prévoit en effet qu'« *une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul*

fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité ». Cette disposition peut s'appliquer à des aspects tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc. La loi prévoit cependant que cette interdiction ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance, c'est à dire dans la quasi-totalité des cas des décisions automatisées.

- **puissance d'impression**

  Les techniques de marketing direct sont un sujet d'insatisfaction pour toute une frange de la population; la vente par correspondance vient depuis plusieurs années en tête des plaintes reçues par la Commission Française "Informatique et Libertés" (CNIL). Ceci n'eût pas été possible sans l'apparition d'imprimantes à très haute performance.

  La loi du 8 décembre 1992 ne prévoyait pas de protection réellement efficace pour se défendre contre les agissements parfois indélicats de certaines sociétés de marketing direct. L'Association Belge du Marketing Direct (ABMD) avait cependant mis sur pied un système appelé « ROBINSON List » auxquels tous les membres de l'ABMD devaient se conformer. Tout annonceur, membre de l'ABMD, s'engageait ainsi à ne plus adresser de courrier aux consommateurs qui avaient demandé à figurer sur la « Robinson List ». Cette initiative a permis de donner satisfaction aux personnes qui se sentaient importunées par les courriers des annonceurs. Bien entendu, la « Robinson List » ne permettait pas de stopper les courriers adressés par des annonceurs non-membres de l'ABMD.

  La loi du 11 décembre 1998 prévoit que *« lorsque les données à caractère personnel sont collectées à des fins de marketing direct, la personne concernée peut s'opposer, gratuitement et sans aucune justification, au traitement projeté de données à caractère personnel la concernant. »*

- **automates d'appel**

  Ces appareils permettent de composer des numéros de téléphone présélectionnés et de diffuser des messages publicitaires préenregistrés.

- **erreurs de conception et d'utilisation**

  Les erreurs de conception et d'utilisation des systèmes informatiques gérant des données à caractère personnel peuvent avoir pour effet que des personnes fassent l'objet de décisions ou de traitements sur base de données erronées. Un pourcentage non négligeable des centaines de plaintes reçues par la Commission belge de la Protection de la Vie Privée en matière de crédit à la consommation n'a pour autre cause que des erreurs sur l'identité de la personne concernée. Des manquements aux procédures de contrôle, notamment en matière d'homonymie, font que des personnes sont indûment fichées comme mauvais payeurs.

Que faut-il en fait entendre par données à caractère personnel ? L'article 2 de loi du 11 décembre 1998 précise qu'il s'agit de *« toute information concernant une personne physique identifiée ou identifiable ».* L'identification de la personne peut être directe ou

indirecte. Elle est possible par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Lorsqu'il est fait usage d'un identifiant, celui-ci peut être propre au traitement (p.ex. un numéro de client) ou un identifiant unique, tel que le numéro de Registre National.

La banalisation d'un identifiant unique fait manifestement peser de graves menaces en matière de protection de la vie privée car il rend beaucoup plus facile le rapprochement de fichiers. C'est pourquoi le législateur a soumis la consultation du Registre National, ainsi que l'utilisation du numéro de Registre National à un système d'autorisation par arrêté royal après avis préalable de la Commission de la Protection de la Vie Privée. On peut néanmoins regretter qu'il n'y ait pas encore eu de réflexion globale qui conduirait à édicter des principes généraux définissant dans quelles circonstances on peut consulter le Registre National ou utiliser le numéro de Registre National comme identifiant dans un traitement. Actuellement, à défaut de ce texte général, il existe plus d'une centaine d'arrêtés royaux dont l'analyse fait apparaître si pas des contradictions à tout le moins un manque de cohérence. Dans plusieurs cas, des autorisations d'utilisation du numéro de Registre National ont été accordées à des institutions publiques, là où il eût été parfaitement possible d'atteindre les objectifs recherchés sans avoir à le faire. La banalisation de cet identifiant doit manifestement être un sujet de préoccupation.

L'identification indirecte des personnes concerne les situations où la personne peut être identifiée par un biais, tel que son numéro de téléphone (centraux téléphoniques de l'opérateur public, d'entreprises, d'hôtels, téléphonie mobile,...), sa plaque d'immatriculation, son numéro de carte de crédit, des cartes à puces diverses (p.ex. dossiers médicaux portables), des badges (p.ex. horaire variable, contrôle d'accès). On constate ainsi qu'il s'agit souvent de situations où l'information est saisie à l'insu de la personne concernée. D'autre part, on réalise des progrès très importants en matière d'authentification sur base de caractéristiques biométriques (p.ex. reconnaissance vocale, analyse d'images de portraits, empreintes digitales,…). La nouvelle loi du 11 décembre 1998 ne souffre pas d'ambiguïté quant au fait que la possibilité d'une identification indirecte fait automatiquement tomber les données à caractère personnel correspondantes sous le couvert de la protection de la loi.

La loi du 11 décembre 1998, modifiant celle du 8 décembre 1992 en vue de se conformer à la directive européenne du 24 octobre 1995, a consacré un certain nombre de principes essentiels en matière de protection de données à caractère personnel :

- Les données doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et règlementaires applicables* »;

  Les cessions de fichiers font courir le risque que les données cédées soient utilisées à des fins différentes de celles pour lesquelles elles furent initialement collectées;

  La Commission de la Protection de la Vie Privée a eu à traiter de cas de détournements de fichiers :

- détournements de fichiers utilisés à des fins électorales;
- prospection commerciale sur base de fichiers non prévus à cette fin;
- exploitation des bénéficiaires des ordres de virements bancaires (une banque belge a analysé les ordres de virement destinés à des paiements d'assurance pour adresser aux donneurs d'ordre de la publicité concernant ses propres produits d'assurances)

Un problème se pose lorsqu'une organisation poursuit des finalités différentes (p.ex. une même organisation a des activités de mutuelle, de banque et d'assurances; les données de la mutuelle contiennent des informations sur l'état de santé des personnes qui pourraient être utilisées par la branche assurance du groupe pour l'acceptation d'assurances "vie"; la branche banque connaît la situation financière de ses clients et peut ainsi sélectionner pour la branche d'assurances les prospects intéressants).

La loi du 11 décembre 1998 introduit fort à propos les notions de « tiers » et de « destinataire ». L'article 13 impose au responsable du traitement d'informer la personne concernée des destinataires ou des catégories de destinataires des données.

- Les données doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement* »;

  Les cas sont fréquents où des données excédentaires par rapport aux finalités sont collectées.

- Les données doivent être « *exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que des données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées »;*

  Ceci impose aux responsables des traitements de données à caractère personnel de faire preuve de diligence et de prudence en prenant les dispositions appropriées pour assurer la qualité des données gérées et traitées.

- Les données doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. Le Roi prévoit, après avis de la Commission de la protection de la vie privée, des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.* »

  Ceci concerne à titre d'exemple des situations telles que :

  - la pérennisation des échecs scolaires;
  - la conservation d'incidents de paiement au-delà de durées raisonnables;
  - la réinsertion de populations à problèmes.

- Le traitement de données « sensibles » est interdit, sauf dans certains cas énumérés de manière restrictive (il n'y en a pas moins d'une douzaine…); ceci concerne « *les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement de données relatives à la vie sexuelle* ». Il en va de même des données relatives à la santé;

- Dans le cas particulier de données personnelles utilisées exclusivement à des fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations ont été prévues par la loi, de manière à maintenir l'équilibre entre la garantie de la liberté d'expression, d'une part, et la protection du droit au respect de la vie privée, d'autre part.

- La loi du 11 décembre 1998 prévoit l'obligation de fournir à la personne concernée, au plus tard au moment où ces données sont obtenues ou, si une communication à des tiers est envisagée, au plus tard au moment de la première communication de données, une série de renseignements tels que :

  - le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant;
  - les finalités du traitement;
  - l'existence du droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de direct marketing ;
  - les destinataires ou les catégories de destinataires des données;
  - le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse ;
  - l'existence d'un droit d'accès et de rectification des données la concernant ;
  - d'autres informations déterminées par le Roi en fonction du caractère spécifique du traitement, après avis de la Commission de la protection de la vie privée.

  Il existe en effet de nombreux cas où des données sont collectées à l'insu de la personne concernée ou utilisées pour des finalités non précisées :
  - sondages et enquêtes dont les buts et les bénéficiaires sont inconnus;
  - examens médicaux réalisés à l'insu de la personne;
  - annonces d'emploi "bidon" pour obtenir le curriculum vitae détaillé des postulants;
  - suivi de l'audience par des capteurs interactifs placés sur les réseaux de télédistribution;
  - destination, conservation et communication de tests psychologiques.

  Des exceptions et limitations sont prévues notamment lorsque les données concernent la sûreté de l'Etat, la défense, la sécurité publique, les infractions pénales,…

  On peut toutefois souligner que certains pays, dont la France, ont oeuvré pour une plus grande exactitude et transparence des fichiers de police et de sûreté d'Etat. Il est en effet permis d'exprimer des inquiétudes en la matière. Existe-t-il des procédures fiables par lesquelles la qualification de « suspect » est rectifiée lorsqu'au

terme d'une enquête ou d'un jugement une personne est lavée de tout soupçon ? Les informations mémorisées font-elles l'objet d'une procédure de contrôle de qualité ? Procède-t-on à des adaptations en cas de grâce ou d'amnistie ?

- La loi du 11 décembre 1998 reconnaît, dans certaines limites, à la personne concernée un droit d'opposition à ce que des données le concernant soient traitées;

  En dehors du droit déjà mentionné de s'opposer au traitement de données à des fins de direct marketing, la loi précise que *« toute personne a en outre le droit de s'opposer, pour des raisons sérieuses et légitimes tenant à une situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf lorsque la licéité du traitement est basée sur les motifs visés à l'article 5, b) et c). »*

- En ce qui concerne les transferts de données à caractère personnel vers les pays tiers, le principe est d'éviter que les règles de l'Union européenne ne puissent être contournées par des transferts vers des pays n'appartenant pas à l'Union européenne. Au sein de l'Union européenne, le principe d'une protection équivalente est bien entendu assuré par la directive.

- La directive européenne prévoit l'existence dans les Etats Membres d'une autorité de contrôle chargée de surveiller sur son territoire l'application des dispositions adoptées en application de la directive. Ce rôle est joué en Belgique par la Commission de la Protection de la Vie Privée, déjà instaurée par la loi du 8 décembre 1992. Elle comporte 16 membres. Son seul membre à temps plein est le Président, qui est un haut magistrat. Les autres membres, aux spécialités très diverses, ont été notamment choisis pour leur connaissances professionnelles et leur expérience des secteurs publics et privés. On y trouve des magistrats, des professeurs d'université, des fonctionnaires et des indépendants, des juristes, des informaticiens, …

  La Commission a plusieurs rôles :

  - elle émet soit d'initiative, soit sur demande du Gouvernement, des Chambres législatives, des Exécutifs communautaires ou régionaux, des Conseils de communauté ou régionaux,… des avis sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée;

    la loi prévoit que l'avis de la Commission est requis dans un certain nombre des situations; l'avis de la Commission est dans ce cas publié au Moniteur en même temps que l'acte réglementaire auquel il se rapporte.

  - la Commission peut également émettre des recommandations sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée;

  - la Commission examine les plaintes qui lui sont adressées, ce qui peut l'amener à effectuer des examens sur place; les membres de la Commissions disposent en ces circonstances des mêmes pouvoirs d'investigation que les agents de la police judiciaire;

- la Commission exerce une autorité de tutelle sur les comités de surveillance et de contrôle spécialisés dans des matières bien définies, telles que les banques de données sociales et les banques de données du secteur du crédit.

Dans le traitement des plaintes, la Commission privilégie la recherche de solutions de conciliation entre parties permettant de mettre fin à la violation de la loi. En l'absence de conciliation, la Commission peut émettre un avis sur le caractère fondé de la plainte, avis qui peut être accompagné de recommandations à l'intention du maître de fichier. Sauf si la loi en dispose autrement, la Commission peut dénoncer au Procureur du Roi les infractions dont elle a connaissance.

- La directive européenne encourage l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions adoptées par les Etats membres en matière de protection de la vie privée.

  Depuis sa création, la Commission de la Protection de la Vie Privée a poursuivi une politique d'ouverture et de dialogue avec les secteurs et les associations professionnelles en vue de s'informer des problèmes particuliers posés par l'application de la loi, de rechercher des solutions adéquates et d'encourager des initiatives sectorielles en vue d'une meilleure protection de la vie privée.

- La loi du 11 décembre 1998 consacre le principe, déjà présent dans la loi du 8 décembre 1992, d'une déclaration des traitements à l'autorité de contrôle, en l'occurrence la Commission de la Protection de la Vie Privée. Un régime de déclaration simplifiée et de dérogation est permis sous certaines conditions notamment pour certaines catégories de traitement *« lorque, compte tenu des données traitées, il n'y a manifestement pas de risque d'atteinte aux droits et libertés des personnes concernées… ».* Divers arrêtés royaux ont exploité cette disposition. Ils définissent de nombreux traitements pour lesquels une notification à la Commission n'est pas requise. Cette approche a le mérite d'éliminer une bureaucratie considérable et coûteuse qui n'aurait que peu contribué à l'amélioration de la protection de la vie privée. Il est désormais possible de concentrer tous les efforts sur les traitements où les risques d'atteinte potentiels sont manifestes. Ces traitements doivent être déclarés à la Commission, qui les insère dans un registre publiquement accessible.

- Enfin, nous soulignerons les importantes dispositions que la loi du 11 décembre 1998 impose en matière d'intégrité, de confidentialité et de sécurité des traitements de données à caractère personnel : *« Le responsable du traitement ou, le cas échéant, son représentant en Belgique, doit :*

  - *Faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues en méconnaissance des articles 4 à 8 ;*
  - *Veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limitées à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service ;*

- *Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, la perte accidentelle, ainsi que la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.*

Ces mesures doivent assurer un niveau de protection adéquat, compte tenu de l'état de la technique en la matière et des coûts qu'entraîne l'application de ces mesures et d'autre part, de la nature des données à protéger et des risques potentiels ».

Les risques liés à l'usage de l'informatique concernent donc la disponibilité, l'intégrité et la confidentialité.

Ces risques trouvent leurs **origines** dans :

- les causes accidentelles
- les erreurs
- la malveillance.

Parmi les **causes accidentelles,** il convient de mentionner :

- les accidents physiques (feu, eau, foudre, fumée, ...)
- les pannes
- les pertes de services essentiels (électricité, télécommunications,...)

Les **erreurs** concernent tant les erreurs d'utilisation (p.ex. introduction de paramètres incorrects pour un traitement, erreur sur le destinataire d'une télétransmission, erreur de fichier traité,...) que les erreurs de conception et de réalisation de systèmes.

Enfin, la troisième cause fort préoccupante d'incidents est la **malveillance**. Lorsque le CLUSIF (Club de la Sécurité Informatique Français) entama vers 1984 la collecte de données statistiques, la malveillance était à l'origine d'environ un tiers des pertes consécutives à des sinistres informatiques en France. Aujourd'hui, cette partie représente près de 60 % des pertes. Elle inclut le vol sous ses diverses formes (matériel, logiciel, données,...), le sabotage physique des équipements, les attaques logiques (virus, bombes logiques, Cheval de Troie, vers,...), la divulgation d'éléments confidentiels, la fraude,...

Les **conséquences** des incidents se traduisent par des pertes directes (p.ex. obligation de remplacer des composants détruits, endommagés, volés,...) et des pertes indirectes, telles que les frais supplémentaires (p.ex. heures supplémentaires prestées pour récupérer la situation, location de matériel de secours, de personnel intérimaire,...) et les pertes d'exploitation (pertes de marché, manque à gagner,...). Les pertes sont matérielles (pertes de biens et de fonds) ou immatérielles (atteinte à la capacité concurrentielle, détérioration de l'image de marque, sabotage du fonctionnement de l'organisation,...). La responsabilité civile vis-à-vis de tiers peut être d'envergure (p.ex. divulgation de données confidentielles telles que violation du secret médical ou communication de données financières sensibles, retards, inexécution ou erreurs dans des traitements accomplis pour compte de tiers).

Une saine gestion des risques implique que l'on établisse la distinction entre risques majeurs et mineurs.

Les **risques majeurs** sont des risques de vie ou de mort pour l'organisation. Ils ont généralement un taux de fréquence extrêmement bas mais leurs conséquences sont catastrophiques. Leurs conséquences sont totalement inacceptables. L'assurance est inadéquate pour se protéger contre pareils risques. Plus de la moitié des entreprises dont les bâtiments ont été totalement détruits par un incendie n'existent plus trois ans après le sinistre. Elles sont tout simplement *« out of business »*. Ceci n'est pas dû au fait qu'elles n'étaient pas ou mal assurées mais bien parce qu'elles ne disposaient pas d'un plan de survie. L'assureur donne une indemnisation mais il ne peut restituer à l'entreprise les données et programmes perdus.

Les **risques mineurs** ont une probabilité de survenance plus élevée mais leurs conséquences sont moindres. Elles sont temporairement acceptables. En cette matière, une approche d'amortissement économique est envisageable. Que coûte la prévention ou l'assurance vis-à-vis de la non-protection ? Les très nombreux incidents que l'on rencontre au quotidien sans même qu'ils ne soient répertoriés dans les statistiques vu leur fréquence sont à ranger dans cette catégorie.

Sous peine de mal orienter ses efforts et ressources, toute approche de la sécurité doit nécessairement débuter par l'identification des risques potentiels et de leurs conséquences.

Il conviendra de se poser les questions suivantes qui ont trait aux aspects fondamentaux de disponibilité, intégrité et confidentialité :

- quelles seraient les conséquences pour l'organisation si telle application était indisponible pendant une période de quelques secondes, minutes, heures, jours, semaines, mois, ...? Si le centre de traitement ou un serveur sont neutralisés, ce sont bien entendu toutes les applications qui en dépendent qui seront neutralisées !
- quel est le risque encouru en cas d'atteinte à l'intégrité ? Quelles seraient les conséquences maximales d'une erreur ou d'une fraude dans telle application ?
- quelles seraient les conséquences d'une divulgation à des tiers des données ou des programmes de telle application ? Ou encore des données relatives au système de sécurité protégeant l'application ?

La stratégie à suivre pour gérer les risques identifiés comprend les volets suivants:

- la **prévention**, qui vise à réduire la probabilité de survenance;
- la **protection**, qui a pour objet de limiter les conséquences d'un incident préjudiciable;
- la **détection**, qui veillera à détecter les incidents aussi rapidement que possible en évitant les fausses alarmes (trop sensible) et la non-détection (trop peu sensible);
- la **gestion de l'après sinistre** qui a pour effet de permettre à l'organisation de continuer à assumer ses fonctions vitales dans les meilleurs délais après un sinistre;

- le **transfert à l'assurance** qui, dans une philosophie de gestion de risques, ne sert qu'à financer le plan de survie et à prendre en charge ce qui dépasse la capacité financière propre à l'organisation;
- la **répression** en cas d'agissements malveillants.

Une neutralisation de courte ou de longue durée peut entraîner des conséquences dommageables pour le responsable du traitement mais également pour les personnes concernées par ces traitements. Le préjudice croît rapidement avec la durée d'indisponibilité. La perte irrécupérable des données est évidemment un risque majeur, qui n'a malheureusement rien d'improbable. Un important établissement hospitalier belge a récemment perdu l'entièreté de ses données comptables et de celles relatives aux visites des patients, ce qui inclut l'historique du dossier médical informatisé et les données de facturation.

Afin d'assurer un taux de **disponibilité** élevé, toutes les solutions reposeront nécessairement sur la **redondance** des composants de telle sorte que la défaillance de l'un d'entre eux ne conduise pas à une neutralisation du système. Les systèmes de réservation de places d'avion ou de paiements électroniques font largement usage de ce principe. Le terme « composant » est à prendre au sens large car il convient d'y inclure tous les éléments indispensables au fonctionnement du système d'information (matériels, logiciels, données, télécommunications, conditionnement d'air, personnel, énergie,...).

Il conviendra de ne pas réunir les composants redondants dans un même espace, où ils pourraient tous être neutralisés simultanément, par exemple suite à un incendie ou une grève. Il faudra donc les placer en des lieux suffisamment séparés, parfois de plusieurs kilomètres (p.ex. des bâtiments trop contigus pourraient être touchés par un même sinistre tel qu'une chute d'avion).

Lorsque, pour des raisons organisationnelles ou financières, une organisation ne peut envisager pareille solution, elle devra néanmoins mettre en oeuvre un **plan de survie** et cela quels que soient les moyens de prévention qu'elle aura déployés. L'éventualité d'un sinistre catastrophique ne peut en effet jamais être écartée. Diverses solutions existent telles que centre de calcul mobile (camion équipé), centre de calcul transportable (analogue aux salles de tennis « gonflables »), contrat de back up avec une société de services spécialisée,... Chacune des solutions entraînera des frais supplémentaires importants qu'un contrat d'assurance approprié pourra utilement financer.

Les atteintes à l'**intégrité** concernent les incidents qui ont pour effet que le système ne fonctionne plus selon les spécifications normales. On ne peut plus avoir confiance en les résultats qu'il produit car ceux-ci peuvent être erronés ou frauduleux.

En ce qui concerne les traitements de données à caractère personnel, il faudra notamment se protéger contre des incidents tels que :

- l'erreur sur la personne (p.ex. dangers en cas d'homonymie):
- la saisie de données erronées;
- les mises à jour non effectuées;
- les programmes produisant des résultats incorrects;

- les altérations frauduleuses de données;
- les erreurs de transmission;
- etc…

Les atteintes à la **confidentialité** peuvent se muer en risque majeur. Nombre de systèmes gèrent en effet des données au caractère très sensible, dont la divulgation à des tiers peut causer des dommages importants. Les exemples abondent dans les domaine médical, financier, judiciaire, …

Une stratégie de défense contre l'accès non autorisé aux informations se contruira autour d'un ensemble de mesures et moyens :

- tous les accès feront l'objet d'un contrôle qui devra permettre **l'identification** et **l'authentification** de ceux qui se connectent au système; en fonction du degré de sécurité recherché, le contrôle d'accès portera sur les utilisateurs, leur ligne téléphonique, leur numéro d'appel, leur terminal ou PC, les programmes utilisés,... ; chacun des composants devra dès lors pouvoir être authentifié (comment être sûr que tel composant est bien celui qu'il prétend être ?);
- chaque connexion sera enregistrée dans un **journal des accès**, qui prendra toute son importance lors de l'investigation d'incidents de sécurité; ce journal sera systématiquement analysé pour déceler d'éventuels profils de comportement suspects;
- une **classification** des informations en fonction de leur degré de confidentialité devra être établie. Certaines données pourront donner naissance à des risques de :
  - ◊ pressions ou chantage;
  - ◊ atteinte aux biens (p.ex. vols de fichiers de détenteurs d'objets précieux dans une compagnie d'assurances);
  - ◊ atteinte aux personnes (enlèvement, assassinat,…)
- une **politique d'autorisation** définira quels utilisateurs peuvent avoir accès à quelles informations;
- enfin, on étudiera l'opportunité de **chiffrer** les données sensibles, particulièrement lorsque celles-ci seront transmises sur les réseaux extérieurs; néanmoins, le risque est également présent au sein des organisations; un hôpital belge fut particulièrement embarrassé par le vol d'un de ses PC's; celui-ci contenait des données relatives à plusieurs milliers de patients et à leurs traitements; l'information n'était pas chiffrée et pouvait donc être lue par les voleurs.

  Le chiffrement soulève cependant d'autres questions, qui font l'objet de chauds débats à l'échelle mondiale. En effet, l'utilisation de techniques de chiffrement sûres, ç'est à dire difficiles à casser, pose manifestement problème aux services de police et de sûreté d'Etat, dans leurs opérations d'écoute et de surveillance. Des organisations terroristes ou criminelles peuvent ainsi communiquer en toute confidentialité.

  Plusieurs pays ont déjà pris des dispositions réglementant la fabrication, la commercialisation et l'usage de systèmes de chiffrement. Certains Etats tirent

totalement la couverture vers eux en créant des systèmes de licences, en réglementant l'exportation de ces technologies, en imposant l'utilisation de systèmes « faibles » qu'ils sont capables de casser facilement, en instaurant des régimes de dépôt de clefs auprès d'un tiers « de confiance » auxquels ils ont accès dans certaines conditions,... D'autres Etats sont partisans d'une liberté totale.

En Belgique, dans l'état actuel de la législation, l'usage d'outils de cryptographie est libre. Seule l'exportation fait l'objet de réglementations.

Il est bien entendu illusoire de vouloir donner en un espace aussi court un aperçu complet des diverses mesures de sécurité à mettre en oeuvre pour protéger les données à caractère personnel. Les risques diffèrent d'un environnement à l'autre. Les protections devront y être adaptées de manière proportionnée. On notera qu'il importe d'intégrer la sécurité dès la conception des applications car rien n'est plus difficile que de sécuriser des applications existantes. Une attention devra être portée à la cohérence des mesures. Souvent, des dépenses disproportionnées sont consenties pour se prémunir contre certains risques alors qu'il existe des vulnérabilités conséquentes dans d'autres domaines. La sécurité devra aussi faire l'objet de réévaluations périodiques car les dangers ne cessent d'évoluer.

En tout état de cause, la sécurité n'est pas qu'affaire de technologie et de spécialistes. La mise en place d'une structure de contrôle interne efficace est indispensable. La responsabilité de chacun dans l'organisation en matière de sécurité doit être correctement définie. Des efforts de sensibilisation pour rendre le personnel « security minded » sont indispensables. A défaut, l'être humain risque bien de demeurer le maillon le plus faible de la chaîne.

Remarque finale : au moment de clôturer la rédaction de ce texte, les arrêtés de mise en application de la loi du 11 décembre 1998 n'avaient toujours pas été pris.

* * *