Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La loi de protection des données personnelles en Belgique

de Terwangne , Cécile

Publication date:
2002

Document Version
Première version, également connu sous le nom de pré-print

Link to publication

Citation for pulished version (HARVARD):
de Terwangne , C 2002, *La loi de protection des données personnelles en Belgique*..

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 16. Apr. 2024

LA PROTECTION DES DONNÉES PERSONNELLES EN BELGIQUE

Cécile de Terwangne

Le développement spectaculaire des technologies de l'information et de la communication offre de grandes possibilités et de nombreux avantages. Le recours à l'ordinateur et aux réseaux de télécommunication (Internet) accroît l'efficacité des services et facilite souvent la vie. L'utilisation de ces technologies présente toutefois aussi de nouveaux dangers pour la vie privée et les libertés de chacun.

Dans un grand nombre de cas l'information qui circule se rapporte à des personnes. Des bases de données ou des fichiers reprenant des informations personnelles sont constitués, utilisés, communiqués, vendus. Il est désormais difficile de savoir qui sait quoi sur soi et qui en fait quoi. L'individu a perdu la maîtrise de l'information qui le concerne. De ce fait, le risque d'abus ne cesse de grandir.

Depuis 1992, une loi assure, en Belgique, la protection des individus face à l'utilisation de leurs données personnelles. La loi instaure un devoir de transparence concernant l'utilisation de données personnelles : il faut prévenir les personnes quand on traite des informations sur elles, annoncer qui l'on est et pourquoi on traite ces informations. La loi fixe aussi les règles d'utilisation des données personnelles : ce que l'on peut et ce que l'on doit faire avec les données recueillies. La loi instaure également de nouveaux droits pour les personnes fichées dans des registres ou des banques de données : droit d'accès aux données enregistrées, de rectification, d'opposition, …

Le 24 octobre 1995, une directive (norme législative) européenne a été adoptée pour harmoniser les règles de protection des données personnelles sur tout le territoire de l'Union européenne. Comme tous les autres Etats membres, la Belgique devait transposer dans son droit interne les principes contenus dans la directive. La loi du 8 décembre 1992 a en conséquence été fortement modifiée.

Cette brochure présente les nouvelles règles de protection en vigueur en Belgique à partir du 1er septembre 2001. Cette présentation n'est pas exhaustive et il demeure nécessaire de se rapporter aux textes légaux pour une information complète.

QUELQUES DÉFINITIONS UTILES

Qu'est-ce qu'une donnée à caractère personnel ?

C'est toute information qui concerne une personne physique identifiée ou identifiable (appelée « personne concernée »).

Il peut s'agir du nom d'une personne, d'une photographie, d'un numéro de téléphone (même professionnel), d'un code, d'un numéro de compte en banque, d'une adresse e-mail, d'une empreinte digitale, etc.

La notion ne se limite pas aux informations relatives à la vie privée des personnes. Même les informations qui se rapportent à la vie professionnelle ou publique de quelqu'un sont considérées comme des « données à caractère personnel ».

Seules les informations portant sur des personnes physiques sont prises en compte, non celles concernant une personne morale ou une association.

Qui est la « personne concernée » ?

Chacun de nous est une personne concernée. Dès que l'on remplit un formulaire, que l'on passe une commande, réserve une place à un concert ou un billet de train, utilise une carte de crédit, s'inscrit à un cours ou à un club sportif, se fait hospitaliser, emprunte un livre à la bibliothèque publique ou une cassette vidéo à la vidéothèque, on livre des données personnelles.

La loi ne fait aucune différence entre Belges et non Belges.

Qu'est-ce qu'un traitement de données ?

C'est toute opération ou ensemble d'opérations appliquées à des données personnelles. Les opérations dont il s'agit sont particulièrement variées et comprennent la collecte de données, leur conservation, l'utilisation, la modification, la communication, etc. Chaque fois que l'on est invité à remplir un talon réponse, cela correspond donc à un traitement de données pour celui qui va les recueillir. De même, l'hôtel qui offre la possibilité de faire une réservation via Internet fait un traitement de données lorsqu'il enregistre le nom du client, les dates de son séjour et le numéro de sa carte de crédit. La commune qui transmet les noms des demandeurs

de permis de bâtir à un entrepreneur qui désire leur envoyer sa publicité fait également un traitement de données personnelles.

La loi s'applique dès que les opérations effectuées sur des données personnelles se réalisent, ne fût-ce qu'en partie, par des moyens automatisés. Les moyens automatisés englobent toutes les technologies de l'information : informatique, télématique, réseaux de télécommunication (Internet). La loi s'applique donc, par exemple, à une base de données informatique où sont enregistrés les clients ou les fournisseurs d'une société, au registre des immatriculations automobiles tenu par l'administration, à la liste électronique des opérations effectuées sur un compte en banque, au fichier informatisé du personnel d'une entreprise ou des enfants inscrits dans une école, etc. Mais la loi s'applique aussi dès qu'une seule opération fait intervenir des moyens automatisés. Ainsi, l'agence de placement qui conserve les curriculum vitae des candidats sur papier mais qui les envoie par fax aux offreurs d'emploi devra respecter les prescrits de la loi pour tout ce qu'elle fait avec les curriculum vitae reçus (les conserver, les classer, les transmettre).

Celui qui place des caméras vidéo à l'entrée d'un bâtiment ou sur un lieu de travail réalise aussi un traitement à partir du moment où les images des personnes qui passent sont enregistrées, conservées.

Quand les opérations sur les données se font sans le moindre recours à des procédés automatisés (sur papier ou microfiches, notamment), il faut tout de même respecter la loi si les données figurent ou sont destinées à figurer dans un fichier manuel, c'est-à-dire un ensemble dans lequel les données sont accessibles selon des critères spécifiques (par exemple un classement sur la base des noms des personnes, par ordre alphabétique).

Qui est le responsable d'un traitement ?

Il est très important de savoir qui, aux yeux de la loi, est considéré comme le « responsable du traitement ». C'est en effet sur cette personne que repose la charge de presque toutes les obligations imposées par la loi pour assurer la protection des données traitées. C'est donc lui qui sera tenu responsable si un problème survient. C'est aussi le responsable du traitement qui est l'interlocuteur principal des personnes concernées.

La loi désigne comme responsable du traitement la personne qui détermine les objectifs et les moyens de ce traitement de données. Il peut s'agir d'une personne physique ou morale, d'une association de fait ou d'une administration publique.

Lorsque les objectifs et les moyens du traitement sont déterminés par une loi, un décret ou une ordonnance, le responsable du traitement est la personne physique ou morale, l'association de fait ou l'administration publique désignée comme tel par le texte en question.

Cas où la loi sur la protection des données ne s'applique pas

La loi ne s'applique pas lorsque les données personnelles sont traitées dans le cadre d'*activités exclusivement personnelles ou domestiques*. C'est le cas, par exemple, d'un fichier d'adresses privé ou d'un agenda personnel électronique. Ce genre de fichier peut être tenu sans se préoccuper de la loi de protection des données.

Dans certains autres cas, il est prévu une application seulement partielle de la loi. C'est le cas pour les traitements de données à caractère personnel effectués aux seules fins de *journalisme* ou d'*expression artistique ou littéraire*. Une série de dispositions peuvent ne pas être appliquées à ces traitements, afin de garantir un équilibre avec la protection de la liberté d'expression.

Les traitements effectués à des fins de sécurité publique (par la Sûreté de l'Etat, …) bénéficient, eux aussi, d'exceptions partielles.

FORMALITÉ PRÉALABLE

La déclaration des traitements et le registre public

Avant de mettre en œuvre un traitement entièrement ou partiellement automatisé (par exemple avant de se mettre à récolter des données personnelles), le responsable du traitement doit déclarer le traitement auprès de la Commission de la protection de la vie privée. On peut obtenir auprès de cette Commission un formulaire type (sur papier ou sur disquette) permettant d'effectuer la déclaration. Une contribution est à verser à chaque déclaration : 25 euros (1008 francs) si la déclaration est présentée sur disquette, 125 euros (5042 francs) si la déclaration est présentée sur papier.

Tous les renseignements transmis dans la déclaration sont repris dans un registre public. Ce registre peut être librement consulté par quiconque, soit sur place, dans les locaux de la Commission de la protection de la vie privée, soit à distance, via Internet. On peut également demander à recevoir un extrait du registre.

Contenu de la déclaration

La déclaration comporte une description des caractéristiques du traitement. Doivent y figurer, notamment :

- les finalités du traitement
- les catégories de données traitées (pas les données elles-mêmes)
- les catégories de destinataires à qui les données peuvent être fournies
- les garanties entourant la communication de données à des tiers
- les moyens par lesquels les personnes à propos desquelles des données sont traitées en seront informées
- les mesures prises pour faciliter l'exercice du droit d'accès
- les catégories de données destinées à être transmises à l'étranger et les pays de destination
- la période au-delà de laquelle les données ne peuvent plus être gardées, utilisées ou diffusées

Exceptions à l'obligation de déclaration

Outre le fait qu'il ne faut pas déclarer les traitements manuels (sur papier ou microfiches), une série de traitements automatisés de données sont dispensés de l'obligation de déclaration. Il s'agit notamment :

- du traitement réalisé par une société pour gérer son personnel
- du traitement pour gérer les salaires du personnel
- des traitements qui se rapportent à la comptabilité

- des traitements qui visent la gestion de la clientèle ou des fournisseurs
- des traitements effectués par une fondation ou une A.S.B.L. concernant ses membres, ses bienfaiteurs et les personnes avec qui le responsable entretient des contacts réguliers
- des traitements effectués par les écoles et les établissements d'enseignement concernant leurs élèves et étudiants.

Si le responsable de ces traitements est dispensé de la formalité de déclaration, il doit tout de même tenir à la disposition de toute personne qui en fait la demande les mêmes renseignements que ceux contenus dans la déclaration. Cet exercice n'est certes pas vain ; il contribue à une bonne gestion interne des ressources informationnelles.

LA COLLECTE DES DONNÉES

Que doit-on faire si l'on veut collecter des données personnelles ?

La collecte doit être *loyale*. Cela signifie que l'on doit agir de manière transparente : celui qui collecte des informations doit indiquer pourquoi il veut obtenir des données personnelles. Il ne peut faire croire qu'il poursuit un but alors qu'il a l'intention de faire autre chose avec les informations recueillies. On ne peut pas non plus agir à l'insu des personnes (en plaçant des caméras vidéo sans prévenir ceux qui sont filmés, par exemple).

Il faut *fournir des informations* aux personnes auprès desquelles on recueille des données, à moins que ces personnes soient déjà informées. Outre ce qui vient d'être dit sur l'indication des objectifs de la collecte, il faut signaler :

- Le nom et l'adresse du responsable du traitement et, éventuellement, de son représentant,
- Les destinataires ou les catégories de destinataires des données (personnes à qui les données seront communiquées),
- Le caractère obligatoire ou non de la réponse, ainsi que les conséquences éventuelles d'un défaut de réponse,
- L'existence pour chacun d'un droit d'accès aux données qui le concernent et d'un droit de rectification de celles-ci,
- Si les données seront traitées à des fins de marketing direct (démarches publicitaires), il faut signaler aux personnes concernées qu'elles disposent du droit de s'opposer gratuitement à un tel traitement.

Celui qui ne fournit pas ces informations lorsqu'il collecte des données s'expose à une amende allant de 20.000 francs à 20 millions de francs (… euros).

Quelles données peut-on collecter ?

On ne peut collecter que les données qui sont *pertinentes, nécessaires* au vu de l'objectif annoncé. Par exemple :

- Un commerçant peut demander le nom et l'adresse de ses clients dans le but de leur envoyer les factures ou de les informer de ses activités commerciales. Mais il n'a pas de raison de demander la date de naissance de ses clients, ni leur profession.
- Il n'est pas nécessaire pour une école de demander la catégorie de revenus des parents.

- Il n'est pas non plus nécessaire de demander l'état civil d'une personne pour lui ouvrir une ligne téléphonique, ni pour l'inscrire à la bibliothèque publique, ni pour lui fournir un abonnement au câble.
- Le service de guidance psycho-sociale rattaché à une école ne peut récolter systématiquement auprès de tous les parents des classes dans lesquelles il effectue un suivi, des informations sur l'état de santé et l'histoire médicale de tous les membres de chaque famille.

On n'a pas le droit de collecter certaines *données qui sont par nature sensibles*. Ce sont les données relatives à la race, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la santé, à la vie sexuelle, à des suspicions, des poursuites ou des condamnations pénales ou administratives. Il est en principe interdit de récolter ces données. Certaines exceptions sont toutefois admises (voy. « Les données sensibles »).

Celui qui demande des données non nécessaires ou des données interdites s'expose à une amende allant de 20.000 francs à 20 millions de francs (….euros).

Peut-on se fournir en données auprès de tiers ?

On n'est pas toujours obligé de s'adresser aux personnes concernées pour obtenir des données sur elles. On peut recevoir les données d'un tiers (un médecin généraliste envoie des données sur son patient à un médecin spécialiste, par exemple) ou s'adresser à des organismes ou des sociétés disposant de bases de données qu'ils peuvent communiquer (on peut, par exemple, demander à une société de travail intérimaire une liste des curriculum vitae des personnes correspondant à un profil professionnel souhaité).

Dans ce cas, il faut *informer les personnes concernées*, à moins qu'elles ne le soient déjà :

- du nom et de l'adresse du nouveau responsable du traitement (celui qui a obtenu les données) et, éventuellement, de son représentant,
- des objectifs du traitement des données,
- des catégories de données en cause,
- des destinataires ou des catégories de destinataires des données (personnes à qui les données seront communiquées),
- de l'existence pour chacun d'un droit d'accès aux données qui le concernent et d'un droit de rectification de celles-ci,
- Si les données seront traitées à des fins de marketing direct (démarches publicitaires), il faut informer les personnes concernées de ce qu'elles disposent du droit de s'opposer gratuitement à un tel traitement.

On est toutefois *dispensé de cette obligation* si la démarche d'information s'avère impossible ou extrêmement difficile. Mais si une prise de contact s'établit (plus tard) avec une ou plusieurs personnes concernées, il faudra à ce moment fournir les informations énumérées.

Celui qui invoque l'impossibilité ou les efforts disproportionnés qu'impliquerait pour lui le fait d'informer les personnes concernées doit se justifier auprès de la Commission de la protection de la vie privée. Il rajoute cette justification dans la déclaration qu'il doit faire avant de démarrer son traitement (voir « Formalité préalable »).

A QUELLES CONDITIONS PEUT-ON TRAITER DES DONNÉES PERSONNELLES ?

Pour pouvoir traiter des données personnelles (c'est-à-dire les collecter, les utiliser, les exploiter, les communiquer,… voir « Quelques définitions utiles »), on doit remplir deux conditions : il faut poursuivre un objectif particulier et légitime et se trouver dans une des six hypothèses énumérées ci-dessous.

A condition de poursuivre un objectif particulier et légitime…

Les données personnelles ne peuvent être recueillies qu'en vue d'un ou de plusieurs objectifs particuliers. Elles ne peuvent être utilisées que conformément à ce ou ces objectifs. Ce ou ces objectifs doivent en outre être légitimes.

Un ou des objectifs particuliers : on ne peut pas collecter des données personnelles et décider d'utiliser des données sans un but précis. C'est ce but décidé au départ qui va orienter toute la suite des opérations. C'est en fonction de l'objectif poursuivi que l'on saura quelles données on peut collecter, ce que l'on peut faire avec ces données, si on peut les communiquer et à qui, etc.

On ne peut faire que ce qui répond à ou aux objectifs poursuivis et ce qui est compatible avec ces objectifs. On considère comme compatible notamment ce qui est prévu par la loi et ce que la personne concernée peut raisonnablement prévoir.

Celui qui ne respecte pas l'objectif annoncé au départ et qui se sert des données à d'autres fins, incompatibles avec cet objectif, commet un détournement de finalité et est passible d'une amende de 20.000 francs à 20 millions de francs (..euros). C'est le cas, par exemple :

- du bourgmestre d'une commune qui, en tant que président du conseil d'administration des crèches et des maisons de repos communales, a accès aux listes des inscrits dans ces institutions, et qui utilise ces listes pour sa campagne électorale (en précisant dans ses envois « Je suis sensible à la qualité d'accueil de la petite enfance » ou « Une de mes priorités est la situation des personnes âgées », selon qu'il utilise l'une ou l'autre liste)
- du club de fitness qui vend son registre d'adhérents à une société qui propose des cures d'amaigrissement

- de l'oculiste qui communique le nom de ses patients à une société spécialisée dans la vente de lentilles de contact (par contre, il peut communiquer ses dossiers à un confrère duquel il veut avoir l'avis)
- de la grande surface qui vend son fichier où sont enregistrés tous les achats de chaque client détenteur d'une carte destinée à accorder des points liés à la fidélité, à une société de marketing qui désire connaître pour chaque personne enregistrée ses préférences en matière d'alimentation, de boisson, d'hygiène, les quantités achetées, les marques des produits choisis.

Un objectif légitime : pour être admis, l'objectif que l'on poursuit en traitant des données personnelles doit être légitime. C'est-à-dire qu'un équilibre doit exister entre l'intérêt du responsable du traitement et les intérêts des personnes sur qui portent les données traitées. On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux personnes concernées.

- Par exemple, la mise en place d'une caméra de surveillance enregistrant les allées et venues à l'entrée d'un immeuble à appartements porte une grave atteinte à la vie privée des habitants et visiteurs de l'immeuble (on sait qui est entré, qui est sorti, à quelle heure et en quelle compagnie). Il s'agit d'un traitement de données personnelles qui ne peut se justifier (être considéré comme légitime) que si de véritables impératifs de sécurité l'imposent. Ce serait le cas si l'immeuble avait été régulièrement la cible d'effractions, ou si des actes de vandalisme y avaient été perpétré à plusieurs reprises.

- On ne peut pas non plus considérer comme légitime le fait de constituer un fichier des personnes proches de la soixantaine pour leur envoyer le jour de leur 60ème anniversaire une documentation sur une assurance pour subvenir aux frais d'un enterrement ou d'une crémation, « car il devient temps d'y songer ». L'atteinte portée aux personnes est sans aucun doute supérieure à l'intérêt commercial du ficheur.

… Et à condition de se trouver dans une des hypothèses suivantes

Des données personnelles ne peuvent être traitées que :

- si la personne concernée a sans ambiguïté donné son CONSENTEMENT. Le consentement n'est valable que s'il est libre (c'est-à-dire s'il a été émis sans pression), spécifique (le consentement doit porter sur un traitement précis) et

informé (la personne a reçu toute l'information utile sur le traitement envisagé). Le consentement ne doit pas nécessairement être donné par écrit.

- ou si le traitement des données est nécessaire à l'exécution d'un CONTRAT ou à l'exécution de mesures précontractuelles sollicitées par la personne concernée. C'est le cas de l'enregistrement de données pour permettre la facturation d'un service ou pour octroyer un crédit ou pour établir un contrat d'assurance, etc.
- ou si le traitement est exigé par une LOI, un décret ou une ordonnance. Entre par exemple dans cette hypothèse l'obligation imposée à l'employeur de communiquer certaines données concernant son personnel aux organismes de la sécurité sociale.
- ou si le traitement est nécessaire pour sauvegarder un INTÉRÊT VITAL de la personne concernée. C'est le cas de l'accidenté inconscient, à propos duquel on rassemble des données médicales (résultats de tests sanguins, notamment) afin de le soigner.
- ou si le traitement des données est nécessaire pour exécuter une MISSION D'INTÉRÊT PUBLIC ou une mission relevant de l'exercice de l'autorité publique. A ce titre, la SNCB est en droit de tenir un registre des titulaires d'abonnements de train, et la Poste est autorisée à créer un fichier des changements d'adresses pour lui permettre de faire suivre le courrier en cas de déménagement.
- ou, enfin, si le traitement des données est nécessaire pour réaliser un INTÉRÊT LÉGITIME du responsable ou d'un tiers, à condition que l'intérêt ou les droits de la personne concernée ne prévalent pas. Des traitements sont admis si l'intérêt du ficheur à traiter les données est supérieur à l'intérêt du fiché à ce que ses données ne soient pas traitées.

LES INFORMATIONS SENSIBLES

Quelles informations ?

Certaines informations personnelles sont par nature beaucoup plus sensibles que d'autres. Alors que le nom et l'adresse de quelqu'un sont des informations somme toute anodines, il n'en est pas de même des convictions politiques de cette personne, de ses préférences sexuelles ou de son passé judiciaire. La loi règle de manière beaucoup plus stricte l'enregistrement et l'utilisation de ces informations sensibles.

Les données visées sont : les données relatives à la race, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la santé, à la vie sexuelle, à des suspicions, des poursuites ou des condamnations pénales ou administratives.

Des données interdites…

Il est en principe interdit de collecter, d'enregistrer ou de demander communication de données telles que celles énumérées ci-dessus. Celui qui le fait s'expose à une amende de 20.000 francs à 20 millions de francs (…euros) et, en cas de récidive, à un emprisonnement de 3 mois à 2 ans.

… sauf dans des cas très spécifiques

On peut tout de même traiter ces données dans certains cas bien déterminés.

Les cas admis :

A l'exception des données relatives à des suspicions, des poursuites et des condamnations, les données sensibles peuvent être traitées avec le consentement *écrit* de la personne concernée. Cette exception n'est toutefois pas valable lorsque le responsable du traitement est l'employeur présent ou potentiel de la personne concernée ou lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement l'empêchant de refuser librement son consentement. Dans une telle situation, le consentement écrit est tout de même admis s'il permet d'octroyer un avantage à la personne concernée.

On peut également traiter ces données si cela est nécessaire pour l'administration de soins (le traitement doit alors se faire sous la surveillance d'un professionnel des soins de santé) ; si le traitement est exigé par la législation sur le travail ; s'il porte sur des données manifestement rendues publiques par la personne concernée (l'appartenance politique d'une personne ayant mené une campagne électorale, par exemple) ; si le traitement est nécessaire à des recherches scientifiques, etc.

Les partis politiques, congrégations, syndicats, mutuelles ou autres organismes peuvent bien sûr enregistrer et utiliser des données sur leurs membres. Ils ne peuvent toutefois pas communiquer ces données à des tiers sans le consentement des personnes concernées.

Les données relatives aux suspicions, poursuites et condamnations peuvent être traitées par une autorité publique si cela est nécessaire à l'exercice de ses tâches ; par un avocat pour la défense de ses clients ; par quiconque pour la gestion de son propre contentieux ; ou si c'est nécessaire à la réalisation de finalités fixées par la loi.

Les précautions supplémentaires :

Pour toutes ces hypothèses, des garanties supplémentaires sont à respecter, notamment :

- le responsable du traitement doit désigner les catégories de personnes ayant accès aux données et décrire de manière précise leur fonction par rapport au traitement des données. Cela n'oblige pas le responsable du traitement à désigner les personnes par leur nom mais plutôt à établir des profils d'accès (les médecins et infirmières de l'hôpital, par exemple).
- Lors de l'information de la personne concernée (voir « La collecte »), le responsable du traitement doit mentionner la base légale ou réglementaire autorisant le traitement des données. Cela permet de contrôler sur quoi il se base pour traiter des données en principe interdites.
- Enfin, lorsqu'on se fonde sur le consentement écrit d'une personne pour traiter ses données sensibles, il faut signaler à cette personne les motifs pour lesquels ces données sont traitées et lui communiquer la liste des catégories de personnes ayant accès aux données.

QUE DOIT-ON FAIRE AVEC LES DONNÉES RECUEILLIES ?

Veiller à la qualité des données

Les données que l'on traite doivent être exactes et, si c'est nécessaire, mises à jour. Le responsable du traitement doit prendre toutes les mesures raisonnables pour corriger ou effacer les données qui sont inexactes ou incomplètes. S'il ne le fait pas, il risque une amende de 20.000 francs à 20 millions de francs (…euros).

Veiller à la confidentialité des données

Le responsable du traitement doit veiller à ce que les personnes travaillant sous son autorité n'aient accès et ne puissent utiliser que les données dont elles ont besoin pour exercer leurs fonctions. Il n'est pas question de permettre aux membres du personnel d'avoir accès à des données qui ne leur sont pas nécessaires.

Le responsable doit en outre mettre son personnel au courant des prescrits de la loi sur la protection des données. Il doit expliquer les principes de protection qui doivent désormais être respectés.

Veiller à la sécurité des données

Il est important de protéger les données contre une curiosité malsaine venant de l'intérieur ou de l'extérieur ou contre des manipulations non autorisées. Les risques de fuites et d'atteintes à l'intégrité des données est trop réel de nos jours. Ces atteintes peuvent être accidentelles ou malintentionnées. Il est essentiel de prendre des mesures de sécurité pour protéger les données.

Ces mesures de sécurité sont de deux ordres : des mesures organisationnelles (limiter le nombre de personnes ayant accès aux données, utiliser des mots de passe, fermer les locaux où sont localisés les ordinateurs et les fichiers, etc.) et des mesures techniques.

Plus les données en cause sont sensibles et les risques pour la personne concernée grands, plus importantes seront les précautions à prendre. Par exemple, des données relatives à la santé d'une personne, utilisées en dehors d'un contexte médical (par une compagnie d'assurance pour octroyer une assurance-vie, par exemple), devront être encadrées de mesures de sécurité sévères.

Effacer les données

Les données personnelles ne doivent pas être conservées sous une forme qui permet d'identifier les personnes plus longtemps qu'il n'est nécessaire par rapport à l'objectif poursuivi. Il convient alors de les effacer ou de les rendre anonymes. A défaut de quoi, on s'expose à une amende de 20.000 francs à 20 millions de francs (… euros).

LES DROITS DES PERSONNES CONCERNÉES

Toute personne, quel que soit son âge, son domicile ou sa nationalité, se voit reconnaître des droits vis-à-vis des personnes qui traitent des données sur elle :

Le droit à l'information

On ne peut pas traiter des données personnelles à l'insu des sujets. A partir du moment où l'on recueille des données sur des personnes, on doit mettre ces personnes au courant de ce que l'on compte en faire. La loi indique quelles informations doivent être communiquées. Cette formalité doit être accomplie que les données soient obtenues de la personne concernée elle-même ou de manière indirecte. Voir « La collecte des données »

Le droit à la curiosité

Chacun a le droit d'interroger tout responsable de traitement pour savoir s'il détient ou non des données sur lui. Le responsable interrogé doit confirmer ou non s'il détient des données et, si c'est le cas, il doit préciser dans quel but il détient les données, de quelles catégories de données il s'agit et quels sont les destinataires de ces données.

Le droit d'accès direct

A quoi a-t-on accès?

Chacun a le droit de recevoir, sous une forme intelligible, une copie des données faisant l'objet d'un traitement ainsi que toute information disponible sur l'origine des données. Le droit de connaître la provenance des données utilisées est particulièrement important car c'est souvent la question de la source des informations qui préoccupe les personnes concernées.

Il arrive qu'une décision affectant de manière significative une personne soit prise sur le seul fondement d'un traitement automatisé (cela peut être le cas pour l'octroi d'un prêt ou la souscription d'une assurance, par exemple). Dans ce cas, la personne en cause doit pouvoir avoir aussi accès à la logique qui sous-tend le traitement automatisé en question.

Comment exercer son droit d'accès?

Pour exercer son droit d'accès, il faut adresser une demande au responsable du traitement en faisant la preuve de son identité (en joignant la photocopie de sa carte d'identité, par exemple). La demande peut être envoyée par la poste ou par tout moyen de télécommunication (par fax ; par courrier électronique avec apposition d'une signature électronique).

Le responsable doit répondre sans délai et au plus tard dans les quarante-cinq jours de la réception de la demande. S'il ne le fait pas, il s'expose à une amende de 20.000 francs à 20 millions de francs (… euros). On peut en outre dénoncer ce comportement à la Commission de la protection de la vie privée, voire porter plainte auprès du juge (voir ci-dessous « Recours »). Il en est de même si le responsable du traitement a donné des renseignements inexacts ou incomplets.

Le droit d'accès indirect

En deux circonstances, c'est un accès indirect de la personne concernée à ses données qui est prévu.

L'accès aux *données relatives à sa santé* peut s'effectuer soit directement par la personne sur qui portent les données, soit par l'intermédiaire d'un professionnel des soins de santé choisi par cette personne, si le responsable du traitement ou la personne elle-même demande l'intervention d'un intermédiaire.

Pour les *données traitées à des fins de sûreté de l'Etat, de sécurité publique, de défense nationale, de prévention ou de répression des infractions*, c'est également un accès indirect qui est mis en place. Dans ces cas, il faut s'adresser à la Commission de la protection de la vie privée en apportant la preuve de son identité et en lui demandant d'effectuer la démarche d'accès. La Commission effectue les vérifications utiles, fait procéder aux modifications nécessaires et spécifie à l'intéressé qu'il a été procédé aux vérifications.

Le droit de rectification

Chacun peut, sans frais, faire rectifier les données inexactes qui se rapportent à lui et faire effacer ou interdire d'utilisation les données incomplètes, non pertinentes ou interdites.

Le responsable du traitement doit répondre dans le mois à celui qui a demandé les corrections. Il doit indiquer les rectifications ou effacements qu'il a effectués. S'il ne le fait pas, on peut s'adresser à la Commission de la protection de la vie privée en dénonçant son comportement. On peut également porter plainte devant le juge (voir ci-dessous « Recours »).

Si des données inexactes, incomplètes, non pertinentes ou interdites ont été transmises à des tiers, le responsable doit, dans le mois, signaler les corrections ou effacements à effectuer aux personnes à qui ces données ont été communiquées, à moins que cela ne s'avère impossible ou extrêmement difficile.

Le droit d'opposition

Chacun a le droit de s'opposer à ce que les données le concernant fassent l'objet d'un traitement, mais il doit invoquer des raisons sérieuses et légitimes.

Limites du droit d'opposition : le droit d'opposition n'est pas admis pour les traitements nécessaires à la conclusion ou à l'exécution d'un contrat ; les personnes concernées ne peuvent pas non plus s'opposer au traitement de leurs données imposé par une obligation légale ou réglementaire.

Lorsque les données sont collectées *à des fins de marketing direct* (pour des démarches publicitaires), la personne concernée peut s'opposer gratuitement et sans aucune justification au traitement de ses données. Ainsi, lorsque l'on est invité à remplir un talon-réponse, si celui qui récolte les données a l'intention de les transmettre à des sociétés de marketing direct, il doit le mentionner sur le talon et on a le droit de s'opposer sans justification à ces transmissions. De même, celui qui est importuné par des propositions téléphoniques pour découvrir des salons de cuir ou déguster des vins, peut exiger d'être radié de la liste de celui qui téléphone.

Le droit de ne pas être soumis à une décision automatisée

Il n'est pas souhaitable qu'une décision qui s'impose à un homme dépende des seules conclusions d'une machine. Aussi, la loi interdit qu'une décision affectant une personne de manière significative soit prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité.

Toutefois, cette interdiction ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat (pour l'octroi d'un prêt ou la souscription d'une assurance, par exemple) ou est fondée sur une disposition légale ou réglementaire. Le contrat ou la

disposition en question doivent contenir des mesures garantissant la sauvegarde des intérêts de l'intéressé. A tout le moins, celui-ci doit avoir le droit de faire valoir *utilement* son point de vue.

Recours en cas de difficulté à faire respecter ses droits

Auprès de la Commission de la protection de la vie privée

En cas de difficultés rencontrées dans l'exercice des droits consacrés par la loi ou en cas de non-respect d'obligations découlant de la loi, la personne concernée peut adresser une plainte à la Commission de la protection de la vie privée. Cette Commission intervient pour amener le responsable du traitement à respecter les obligations que lui impose la loi. Elle s'efforce de résoudre les litiges à l'amiable. En cas d'insuccès, la Commission émet un avis sur le caractère fondé de la plainte. Si elle constate une infraction, elle la dénonce au procureur du Roi. Elle peut aussi soumettre le litige au président du tribunal de première instance.

Auprès du tribunal

Celui qui n'est pas satisfait peut également porter plainte auprès du président du tribunal de première instance de son domicile.

TRANSFERTS DE DONNÉES VERS L'ÉTRANGER

Transfert de données personnelles vers un Etat membre de l'Union européenne

Les transferts de données personnelles entre pays membres de l'Union européenne sont désormais libres. Une personne établie en Belgique peut donc librement envoyer des données personnelles dans un autre pays de l'Union européenne si cet envoi est légitime aux yeux de la loi belge (si cet envoi s'impose pour réaliser le but annoncé du traitement des données ou s'il est compatible avec ce but – voir « A quelles conditions peut-on traiter des données personnelles ? »).

Par exemple, une banque peut envoyer les données relatives à un de ses clients pour effectuer un paiement en France, un hôpital belge peut communiquer à un organisme de sécurité sociale italien les données concernant les frais d'hospitalisation d'un membre de cet organisme, une agence de voyage peut envoyer à la compagnie aérienne néerlandaise et à l'hôtel espagnol réservés par son client les données de celui-ci, une entreprise peut transférer le fichier de son personnel dans un autre Etat de l'Union.

Transfert de données personnelles hors de l'Union européenne

En dehors de l'Union européenne, on ne peut transférer des données personnelles que vers des pays qui assurent une protection des données correspondante à celle assurée sur le territoire de l'Union européenne. En l'absence d'une telle règle, la forte protection garantie à l'intérieur de l'Union européenne serait rapidement vide de sens étant donné la facilité de circulation des données grâce aux nouvelles technologies.

Tout responsable de traitement qui souhaite exporter des données personnelles hors de l'Union européenne doit d'abord se demander si le pays destinataire assure un *niveau de protection adéquat* pour de telles données. Il faut retrouver les mêmes principes de protection que ceux établis sur le territoire européen. Pour évaluer la qualité de la protection offerte, il faut tenir compte de la législation du pays en question, des règles déontologiques appliquées, etc. En cas de doute, on peut s'adresser à la Commission de la protection de la vie privée pour savoir si un pays particulier offre une protection adéquate et si les transferts de données vers ce pays sont autorisés.

Dans certains cas, on peut tout de même transférer des données vers des pays qui n'offrent *pas un niveau de protection adéquat*. C'est notamment le cas si les personnes concernées donnent leur consentement indubitable au transfert de leurs données vers un tel pays, ou lorsque le transfert est nécessaire pour exécuter un contrat avec la personne concernée, ou lorsque les données proviennent d'un registre public destiné à l'information du public (annuaire téléphonique, registre du commerce, par exemple).

Le responsable du traitement peut également offrir lui-même, par la voie contractuelle, une protection appropriée. La protection peut ainsi être assurée au moyen d'un contrat liant celui qui envoie les données et celui qui les reçoit et contenant des garanties suffisantes au regard de la protection des données. Un modèle de contrat offrant des garanties suffisantes est proposé par la Commission européenne. Il est disponible sur le site Internet de la Commission.