Bureau de dépôt Vilvoorde 1
KE DOCUMENTA

Manuel des Services de Police

Actualités en bref **N° 206** **30 août 1995**

Publication bimensuelle, contient 14 feuillets (28 pages), ne paraît pas en juillet

Vous pourrez lire, ci-dessous, un texte très intéressant sur le traitement des données à caractère personnel par les services de police.
Nous l'avons jugé suffisamment intéressant pour y consacrer un numéro spécial des Actualités en bref. Un texte plus détaillé sera publié prochainement sur le sujet dans le Postal-Mémorialis.

LES BASES DE DONNEES POLICIERES
ET LA LOI SUR LA VIE PRIVEE 206/1

Introduction

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel a été publiée au Moniteur belge du 18 mars 1993. Ses arrêtés d'exécution sont parus récemment. La loi impose à l'enregistrement des données

à caractère personnel des conditions strictes et a pour objectif de prévenir les abus. Elle comprend diverses dispositions importantes dans le cadre des bases de données policières. Cet article traite de certains aspects de la loi sur la protection de la vie privée très importants pour les services de police. Un article plus détaillé sera bientôt publié à ce sujet dans Postal-Mémorialis.

1. Que trouve-t-on dans la loi sur la vie privée ?

La loi sur la vie privée comprend les lignes directrices en matière de traitement des données à caractère personnel et décrit également les exceptions à ces lignes directrices (e.a. les données destinées à une utilisation policière).
Dans ce cadre, le législateur a tenté d'atteindre l'équilibre entre les exigences de la protection de la vie privée des enregistrés d'une part et les exigences du système administratif, économique et social d'autre part.
Cette loi élabore également le cadre de fonctionnement et de compétence de la Commission de la protection de la vie privée (art. 23-26). Enfin, elle contient aussi une longue série de dispositions pénales (art. 37-43) relatives à pratiquement toutes les obligations qui découlent de la loi. Par analogie aux législations financière, économique et environnementale, des amendes élevées sont prévues pour lutter efficacement contre les infractions à la protection de la liberté fondamentale des personnes physiques.

2. Quelques notions importantes

Données à caractère personnel

Les données à caractère personnel sont les données relatives à une personne physique identifiée ou identifiable.
La possibilité d'identification doit être interprétée largement : le numéro de la carte d'identité ou

du passeport, un numéro de plaque minéralogique, un numéro de téléphone, l'adresse et la fonction de la personne ou encore la combinaison de ses caractéristiques physiques (taille, poids, empreintes digitales, ...) qui permettent d'identifier une personne directement ou indirectement doivent être considérés comme des données à caractère personnel.

Personnes physiques

Il convient de remarquer que la loi vise uniquement la protection des "personnes physiques" et exclut les personnes morales et les associations de fait.

Traitement

On pense souvent que les lois sur la vie privée relatives aux données à caractère personnel ne concernent que les bases de données ou les fichiers automatisés. Ce n'est pas le cas.
La notion de traitement y occupe une place centrale. La loi est en effet d'application sur tout "traitement" de données à caractère personnel. Non seulement, le traitement par ordinateur, mais aussi ce que l'on appelle la tenue d'un fichier manuel (art. 1er, § 1er loi sur la vie privée).

Un "traitement automatisé" de données à caractère personnel est tout un ensemble d'opérations, à savoir l'enregistrement, la conservation, la modification, l'effacement, la consultation ou la diffusion de données à caractère personnel, réalisées en tout ou en partie à l'aide de procédés automatisés (art. 1er, § 3 loi sur la vie privée).
Les traitements mis en oeuvre de manière automatisée comprennent non seulement les exécutions soutenues par ordinateur, mais aussi par toutes les autres techniques dans lesquelles une ou plusieurs opérations ne sont pas dirigées directement par la main de l'homme. Il ne doit pas être nécessairement question d'un fichier automatisé.

Il y a traitement dès que des données à caractère personnel sont susceptibles d'être enregistrées de manière automatisée, avec ou sans structure logique, et qu'elles peuvent être consultées de manière systématique à l'aide d'un petit programme informatique.
Si le législateur avait conservé l'exigence d'un fichier ou d'une structure logique, la loi n'aurait pas été, de manière injustifiée, d'application sur de nombreux traitements automatisés.

Tenue d'un fichier manuel

Par contre, l'exigence de fichier s'impose quand les données à caractère personnel sont traitées de manière non automatisée.
La "tenue" de données à caractère personnel dans un "fichier manuel" tombe sous l'application de la loi.
La "tenue d'un fichier manuel" est l'enregistrement, la conservation, la modification, l'effacement, la consultation ou la diffusion de données à caractère personnel sous la forme d'un fichier sur un support non automatisé (art. 1er, § 4 loi sur la vie privée).
Le législateur a voulu éviter qu'un gribouillage isolé sur un concitoyen dans un carnet de notes ne tombe sous l'application de la loi sur la vie privée. Seule la collecte systématique de données à caractère personnel sans ordinateur est donc visée par la loi.
Pour le travail sur les données à caractère personnel sans ordinateur, il est donc extrêmement important de savoir dans quelles conditions il est question de "fichier".

Fichier

Pour établir la limite, la définition que donne la loi de la notion de "fichier" est très importante.
Au sens de la loi, un fichier est un ensemble de données à caractère personnel constitué et conservé suivant une structure logique devant permettre une consultation systématique (art. 1er, § 2 loi sur la vie privée).

L'ensemble des données à caractère personnel, conservé dans un ordre purement alphabétique ou chronologique, ne constitue pas un fichier. Un dossier non plus. Un dossier n'est d'ailleurs rien de plus qu'un ensemble de données, sans structure interne, qui doit systématiquement être entièrement repris pour retrouver une donnée précise.
Il ressort de l'exposé des motifs qu'une série de dossiers classés par ordre alphabétique ou numérique ne tombe pas sous l'application de la loi.

La lecture attentive des définitions proposées par la loi fait ressortir que l'enregistrement et la conservation de données à caractère personnel, indépendamment de toute utilisation réelle de ces données, suffisent pour tomber dans le champ d'application de la loi et devoir satisfaire à ses exigences et que les données passives ne sont pas exclues de son champ d'application.

Il ressort aussi de ces définitions que la simple "collecte" des données à caractère personnel ne constitue pas un "traitement" au sens de la loi.
L'observation d'un concitoyen fournit sans aucun doute des données à caractère personnel, mais ne constitue pas pour autant un traitement de données à caractère personnel au sens de la loi.

Maître du fichier

La majorité des obligations qui découlent de la loi doivent être respectées par le maître du fichier.
Conformément à l'article 1er, § 6 de la loi sur la vie privée, on entend par "maître du fichier", la personne physique ou morale ou l'association de fait compétente pour décider de la finalité du traitement ou des catégories de données devant y figurer. Le pouvoir de décision occupe donc une place centrale dans la détermination du maître de fichier par la loi.
Le maître du fichier est la personne qui possède un réel pouvoir de décision. Autrement dit : la personne qui

décide de traiter les données dans une finalité déterminée doit être considérée comme le maître du fichier. Cela signifie que les techniciens qui décident des données devant être traitées pour aboutir à la finalité fixée ne peuvent pas être considérés comme les maîtres du fichier.

Lorsqu'il s'agit d'un traitement lié à la gestion du personnel, le maître du fichier est l'employeur.
Au niveau de la police communale, cela signifie que la commune est responsable de son fichier personnel.

Une difficulté peut survenir lorsqu'au sein d'une personne morale, un organe décide de la finalité du traitement et une autre organe décide de son contenu. Dans ce cas, la personne morale est considérée comme le maître du fichier, sans qu'aucune distinction ne soit faite entre ses différents services.

Si le maître du fichier n'a pas de domicile en Belgique, il doit élire domicile en Belgique, ou, dans le cas des personnes morales ou des associations de fait, désigner un représentant dans notre pays.

Gestionnaire du traitement

Le maître du fichier ne peut pas être confondu avec le gestionnaire du traitement.
Conformément à l'article 1er, § 7 de la loi sur la vie privée, la personne a qui sont confiées, in concreto, l'organisation et l'exécution du traitement est appelée "gestionnaire du fichier" de données à caractère personnel. Il ne s'agit pas des membres du personnel du "maître du fichier", chargés, in concreto, de la mise en oeuvre des traitements par le maître du fichier. Il s'agit plutôt des personnes ou institutions extérieures à l'entreprise ou aux services publics - par exemple un secrétariat social dans le cadre du calcul ou du paiement du salaire du personnel.

3. Maîtres et gestionnaires du fichier dans quelques services de police

Il est important de déterminer qui est le maître du fichier sur la base des définitions légales qui précèdent.

Ce n'est pas simple, surtout au niveau de la police communale.
Le Procureur, le bourgmestre et le chef de corps peuvent tous trois être "maître du fichier".
Les Pays-Bas ont opté pour un responsable désigné par la loi : le bourgmestre est toujours le chef de la police communale (art. 1er loi sur les registres de police).
La loi belge a opté pour le système de la responsabilité réelle, ce qui revient à dire que le maître du fichier doit être déterminé cas par cas et est en fait la personne qui possède le pouvoir de décision.
La loi fait toutefois une exception : lorsque la finalité du traitement ou les catégories de données devant y figurer sont déterminées par la loi, le maître du fichier est la personne physique ou morale déterminée par la loi pour tenir le fichier (art. 1er, § 6, al.2 loi sur la vie privée).

A la gendarmerie, les choses sont plus simples.
La gendarmerie dispose d'un ordinateur central et, étant donné qu'elle n'est pas une personne morale, le maître du fichier est donc la personne physique responsable.
En principe, il s'agit de la plus haute autorité du corps, à savoir le lieutenant-général.

Au niveau de la police communale, ainsi que nous l'avons déjà signalé, les choses sont plus complexes.
Le bourgmestre est en principe considéré comme le maître du fichier, étant donné que c'est lui qui est investi de la responsabilité finale en matière de police.
Dans la mesure où le chef de corps a plus de pouvoir sur la finalité du traitement et sur les données traitées, c'est lui qui devient le maître du fichier.

Lorsque des agents sont investis de la plus grande autonomie au niveau de la collecte des données dans des bases de données (auxiliaires) ou documents personnels, qui peuvent être considérés comme des fichiers manuels, ce sont eux qui sont les "maîtres du fichier".
Dans les autres cas, ils agissent sous la responsabilité de leur supérieur.

Ce critère fonctionnel du pouvoir de décision doit également être appliqué lorsque plusieurs communes exploitent une base de données commune. Lorsque le système informatique national (PIP) est utilisé, un régime de responsabilité plus simple peut être utilisé pour la police communale. On constate que le régime de la responsabilité réelle est plus complexe que le système utilisé aux Pays-Bas. La loi ne permet pas non plus d'y déroger par arrêté royal et toute dérogation nécessite une loi.

4. Comment satisfaire à la loi ?

La structure de la loi

- Le **chapitre 1er** de la loi reprend une série de définitions et délimite son champ d'application.

- Le **chapitre 2** comprend cinq dispositions diverses. Trois dispositions élaborent un régime particulièrement sévère sur les données sensibles ou conditionnelles (e.a. le sexe et la couleur politique d'un individu, les données médicales et judiciaires). Le traitement de ces données n'est autorisé que dans certains cas exceptionnels. Ce chapitre comprend également une disposition conférant à quiconque un droit d'information lorsque des données sont rassemblées à son sujet et comprend l'article-principe 5 sur lequel nous allons revenir.

- Le **chapitre 3** règle le droit d'information, d'accès et de rectification. Tous ceux impliqués dans un traitement ont un droit d'accès. Ce droit pour

quiconque d'avoir accès à toutes les données recueillies sur sa personne est un droit fondamental. Tout individu jouit en principe d'un droit d'information (art. 4 et 9) et d'un droit de communication et de rectification gratuites des données qui le concerne (art. 10 et 12). L'effacement ou l'interdiction d'utilisation des données dont le traitement est interdit ou qui ont été conservées au-delà de la période autorisée peuvent également être exigés. Le président du tribunal de première instance prend connaissance de toutes les demandes à ce sujet (art. 14). Des poursuites pénales sont prévues en cas de non-respect de ces dispositions.

- Le **chapitre 4** de la loi stipule les obligations imposées au maître du fichier qui doit, e.a., établir un état reprenant toute une série de données exigées par la loi.

- Le **chapitre 5** réglemente la déclaration préalable à la Commission de la protection de la vie privée.

- Le **chapitre 6** contient quelques dispositions relativement peu concrètes sur l'interconnexion des fichiers et les flux transfrontaliers de données.

- Le **chapitre 7** réglemente tout ce qui concerne la Commission de la protection de la vie privée (art. 23-36). La Commission de la protection de la vie privée fonctionnait déjà avant cette loi dans le cadre de l'application de la loi sur le Registre national et de la loi sur la Banque-carrefour de la sécurité sociale. Cette Commission est d'ailleurs titulaire d'un "pouvoir de contrôle général sur les fichiers et les traitements de données". Elle peut, à tout moment, consulter les données des déclarations et exiger d'autres éléments d'information (art. 17, § 4). En vue d'obtenir de plus amples informations, elle peut également ordonner une enquête (art. 32) et adresser des recommandations motivées (art. 30). Cette

Commission est l'organe de contrôle des bases de données policières. Les citoyens qui ont des plaintes ou des demandes relatives aux bases de données policières à formuler doivent s'y adresser (art. 31). Elle est dotée d'un pouvoir d'investigation autonome et peut se faire assister par des experts (art. 32, § 1er). Elle doit dénoncer au parquet les infractions dont elle a connaissance (art. 32, § 2). Son président doit porter devant le tribunal de première instance tout litige concernant l'application de la loi et de ses arrêtés d'exécution (art. 32, § 3).

- Le **chapitre 8** contient les dispositions pénales. C'est ainsi qu'un membre d'un service de police qui empêche la Commission de la protection de la vie privée ou un de ses experts de vérifier une base de données est punissable d'une amende de cent francs à cent mille francs (art. 39 loi sur la vie privée).

- Le **chapitre 9** comprend les diverses compétences du Roi, ainsi que d'autres dispositions finales.

Les bases de données policières et l'interdiction de base imposée par l'article 5 de la loi sur la vie privée

La loi est sans aucun doute d'application aux traitements automatisés et les fichiers manuels de données à caractère personnel mis en oeuvre et/ou constitués par la police.
La police ne peut recueillir que des données à caractère personnel, pertinentes et non excessives, dans le cadre de ses missions (art. 5 loi sur la vie privée). Elle n'est pas autorisée à traiter des données à caractère personnel sans finalité déterminée.
Les finalités doivent être clairement définies, légitimes et connues dès le départ.
Enfin, les données recueillies ne peuvent pas être utilisées de manière incompatible avec leur finalité (art. 5 loi sur la vie privée).
Dans le rapport au Roi de l'arrêté royal n° 8, le Ministre de la justice fait remarquer que, même si un

traitement de données policières est autorisé, il doit respecter toutes les obligations qui lui sont imposées, tout particulièrement celles énumérées dans l'article 5 de la loi sur la vie privée.
"Les principes du respect des finalités légitimes et déterminées et de la qualité des données traitées devront notamment guider les maîtres de fichier dans le traitement de données judiciaires et para-judiciaires".

Bases de données policières et contrôle

Lorsque la collecte des données est organisée par la police administrative ou judiciaire, l'intéressé ne doit pas être informé de ses raisons (art. 4, § 1er in fine loi sur la vie privée).
La justice et la police ne doivent pas, en d'autres termes, informer l'enregistré du traitement de "ses" données. A ce niveau la loi déroge à la règle stipulant que tout maître de fichier doit informer les enregistrés. La justice et la police ne sont pas soumises à l'obligation d'information, étant donné qu'il est logique que la personne impliquée ne soit pas informée que la police judiciaire mène une enquête à son sujet ou qu'elle est soupçonnée d'avoir commis une infraction.

La règle permettant l'accès aux bases de données à tout un chacun n'est pas toujours imposée. Pour une série de données, le droit d'accès ne peut être exercé qu'indirectement. C'est ainsi, par exemple, que les données médicales ne sont communiquées à l'intéressé que via le médecin qu'il a choisi (art. 10, § 3).
La majorité des cas d'accès indirect se situe dans le domaine de la justice et de la police.
L'accès aux données gérées par la police administrative et judiciaire (infra), la Sûreté de l'Etat du Ministère de la justice et le Service Général du Renseignement et de la sécurité de la Défense nationale est toujours indirect. Il est gratuit et passe par l'intermédiaire de la Commission de la protection de la vie privée (cf. art. 13 loi sur la vie privée).

Après vérification, la Commission de la protection de la vie privée informe l'intéressé uniquement du fait que les vérifications nécessaires ont été effectuées, mais ne communique jamais directement de données. Intentionnellement, aucun délai d'intervention de la Commission n'a été prévu. La raison de l'absence de ce délai réside dans le fait que la consultation des fichiers de tiers exige toujours un certain temps, ceci d'autant plus s'il s'agit de données délicates. Si l'absence d'un délai d'intervention devait poser de gros problèmes, un arrêté royal pourrait toujours en introduire un.

La procédure indirecte est gratuite, étant donné que l'intéressé ne peut obtenir d'informations que sur le fait de savoir si les services ont agi ou non conformément à la loi et s'il s'agit de données importantes.

Les services suivants de la justice et de la police sont exemptés de l'obligation d'information et d'accès :

- les services publics chargés de missions de police judiciaire;
- les services de police mentionnés à l'article 3 de la loi réglementant la surveillance des services de police et de renseignement en vue de l'exercice de leur mission de police administrative : la police communale, la police judiciaire près des parquets, la gendarmerie, les services qui ressortent aux autorités publiques et les organismes d'utilité publique dont les membres sont revêtus de la qualité d'agent ou d'officier de police judiciaire;
- la cellule de traitement des informations financières (cf. loi 11 janvier 1993 sur le blanchiment de captaux);
- les deux services de renseignement (cf. infra);
- l'inspection sociale et éventuellement les autres services publics investis de missions de police judiciaire et désignés par arrêté royal.

Les services d'inspection sociale ont été exemptés de l'obligation d'information et d'accès par l'arrêté royal du 12 août 1993 (M.B., 03 08 1993).
En fait, il s'agit de douze services rassemblés sous le Ministère de l'emploi et du travail, l'Office National de l'Emploi, le Ministère de la prévoyance sociale, l'Office National de Sécurité Sociale, l'Office National des Vacances Annuelles, l'Office National des Pensions, l'Institut National d'Assurance Maladie Invalidité, l'Office National d'Allocations Familiales pour Travailleurs Salariés, l'Office National des Administrations Provinciales et Locales, le Fonds des Accidents du travail, le Fonds des Maladies professionnelles et l'Office de Contrôle des fonds des maladies et des Mutualités des fonds des maladies.

Outre le droit d'information et d'accès, les enregistrés disposent également d'un droit de rectification, d'effacement et d'interdiction d'utilisation de certaines données.
Conformément à l'article 12 de la loi sur la vie privée, toute personne a également le droit d'obtenir, sans frais, l'effacement ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant, qui, compte tenu du but du traitement, est incomplète ou non pertinente, ou dont l'enregistrement, la communication et la conservation sont interdits ou encore dont le délai de conservation a été dépassé. Encore une fois, ces droits ne peuvent être exercés qu'indirectement via l'intervention de la Commission de la protection de la vie privée, lorsqu'il s'agit de données gérées par la police administrative et judiciaire, la Sûreté de l'Etat du Ministère de la justice et le Service Général du Renseignement et de la sécurité de la Défense nationale (art. 13). Ici aussi, la Commission de la protection de la vie privée ne communique que l'exécution des contrôles nécessaires, la procédure est gratuite et aucun délai d'intervention n'est prévu.

Il convient également de remarquer que les bases de données policières qui ne soutiennent aucune tâche de

police administrative ou judiciaire, mais traitent par exemple de données relatives au personnel, ne sont pas exemptées. Ces fichiers sont soumis au régime des traitements automatisés "normaux". Tout agent a un droit d'information et peut exercer son droit d'accès, de rectification, d'effacement et d'interdiction d'utilisation pour les données reprises dans l'ordinateur personnel de son corps.

Les bases de données policières doivent être déclarées

Avant qu'un traitement automatisé ne puisse démarrer, il doit être déclaré auprès de la Commission de la protection de la vie privée (art. 17, § 3 loi sur la vie privée).
La déclaration doit mentionner e.a. le fondement légal qui a justifié son instauration ainsi que la finalité du traitement automatisé. Lorsque les données traitées, même occasionnellement, sont destinées à être communiquées à l'étranger, le pays de destination doit être mentionné et ceci pour chaque catégorie de données (art. 1er, § 6). La Commission de la protection de la vie privée tient un registre des traitements déclarés. Quiconque peut donc être informé de n'importe quel traitement automatisé par le registre auquel l'accès est entièrement libre (art. 18). Dès que la déclaration est faite, le traitement peut être lancé et les bases de données existantes peuvent continuer. Le traitement non automatisé ne tombe pas sous l'obligation de déclaration.
L'arrêté royal n° 12 de la loi sur la vie privée fournit les informations nécessaires sur le mode de déclaration et son coût (M.B., 14 03 1995).
La déclaration peut se faire sur un formulaire écrit à la main ou sur un formulaire pré-imprimé de la Commission de la protection de la vie privée ou encore sur une disquette qui représente le formulaire sur support électronique.
Pour la déclaration des bases de données policières et judiciaires, les services et instances concernés sont tenus de payer la somme de 10 000 francs lorsqu'il

s'agit d'une déclaration "libre" et de 3 000 francs lorsqu'il s'agit d'une déclaration sur le formulaire pré-imprimé et de 1 500 francs pour la déclaration sur disquette. Les déclarations de modifications de la déclaration initiale coûtent 800 francs; les avis de suppression de traitements automatisés sont gratuits. Pour les déclarations d'une base de données de gestion du personnel effectuées par un service de police ou une autorité communale les frais sont fixés à respectivement 10 000, 6 000 et 5 000 francs.

Toute déclaration ne peut se rapporter qu'à une seule finalité. Le même maître du fichier peut (bien sûr) faire plusieurs déclarations.
Lorsqu'une commune veut mettre sur pied un casier judiciaire communal et autorise sa police à mettre sur pied une base de données automatisée sur la police administrative et judiciaire et une base de données relative aux frais du personnel de son service de police, en supposant qu'elle fasse ses déclarations uniquement sur support électronique, les frais s'élèveront à 1 500 francs pour les trois premiers traitements et à de 5 000 pour le dernier.

La première partie de la déclaration est destinée à recueillir des informations sur le maître du fichier. Il s'agit de la personne physique ou morale autorisées à décider de la finalité du traitement ou des catégories de données qui doivent y figurer.

La deuxième partie de la déclaration doit comprendre e.a. les données suivantes :

- la dénomination du traitement automatisé;
- le fondement légal de ce traitement;
- la finalité du traitement;
- les catégories de données qui y sont traitées;
- les catégories de personnes autorisées à obtenir les données;
- les délais de conservation des données;

- les pays de destination si des données doivent être envoyées (même à titre occasionnel) à l'étranger.

En ce qui concerne les finalités du traitement et les catégories de données, l'arrêté royal contient deux annexes utiles avec des exemples.

Reprenons l'idée de base de la loi sur la vie privée. Un particulier ou un service public qui veut mettre sur pied une base de données.
Il ou elle doit faire une déclaration dans laquelle figurent la finalité et les catégories de données à traiter.
Les exemples fournis par les annexes de l'arrêté royal n° 12 peuvent être utilisés, mais le sujet peut aussi choisir librement la finalité du traitement et les catégories de données à traiter. La Commission de la protection de la vie privée et le juge exercent post factum une surveillance sur la compatibilité avec la loi sur la vie privée et son article 5 plus particulièrement : sa finalité est-elle légitime, les catégories de données sont-elles nécessaires et légitimes, etc.
La loi est plus stricte pour une série de catégories. Pour ces données, un service public ou un sujet de droit ne peut pas *personnellement* choisir la finalité du traitement ou les catégories de données à traiter.
Seules les finalités fixées par ou en vertu d'une loi sont envisageables. Si cette finalité ne peut être invoquée, le traitement de cette catégorie particulière de données n'est en principe pas autorisé.

Les données dites interdites

Comme on l'a déjà dit, il s'agit de trois catégories de données.
C'est le cas de l'article 7 relatif à la collecte et à la diffusion des données médicales.
Les données médicales sont toutes les données à caractère personnel dont on peut déduire une information sur

l'état antérieur, actuel ou futur de la santé physique ou psychique d'une personne physique (art. 7, al. 1er loi sur la vie privée).
En principe les données médicales ne peuvent pas être traitées. Ces données ne peuvent être traitées que sous la surveillance et la responsabilité d'un praticien de l'art de guérir, à moins qu'il n'y ait urgence, que l'intéressé n'ait donné un consentement spécifique par écrit, ou qu'une loi ou un arrêté royal permette de communiquer ces données à des tiers. Seuls une loi ou un arrêté royal peut permettre à la police de traiter les données médicales.
Les dispositions légales sur la fonction de police qui chargent la police de la surveillance des malades mentaux en est un exemple.

En principe les données sensibles ne peuvent pas être traitées

L'article 6 de la loi sur la vie privée interdit, en principe, le traitement des données à caractère personnel relatives aux origines raciales ou ethniques, à la vie sexuelle, aux opinions ou activités politiques, philosophiques ou religieuses, aux appartenances syndicales ou mutualistes. Ces traitements ne sont autorisés qu'à des fins déterminées par/ou en vertu de la loi. C'est ainsi par exemple que le tribunal et la police peuvent traiter des données à caractère personnel relatives à la vie sexuelle d'un individu dans le cadre de recherches (voir infra), lorsque ces données se rapportent à des infractions dont l'individu est soupçonné, auxquelles il a participé ou pour lesquelles il est jugé.

L'article 6 et le cadre dans lequel le traitement de cette catégorie de données est possible sont élaborés plus en détail dans l'arrêté royal du 7 février 1995 (M.B., 28 02 1995).
Conformément à cet arrêté royal, tout traitement des données énumérées dans l'article 6 doit tenir compte des mesures suivantes :

1. les personnes autorisées à traiter les données doivent être désignées nominativement par le maître du fichier qui doit tenir la liste des personnes ainsi désignées à la disposition de la personne concernée et de la Commission de la protection de la vie privée;

2. ces personnes doivent être soumises légalement, déontologiquement, statutairement et contractuellement à l'obligation de confidentialité;

3. la déclaration à la Commission de la protection de la vie privée par le maître du fichier doit porter la mention du fondement légal ou réglementaire précis de l'autorisation du traitement des données reprises à l'article 6.

Les services de police qui traitent les données dont il est question ici, dans le cadre de l'exercice de leur mission, doivent veiller à ne pas perdre de vue ces conditions.

La police peut traiter des données policières et judiciaires (mais pas toutes)

L'article 8 est très important pour l'administration policière. Il définit avant tout seize domaines.

En résumé, il s'agit des domaines suivants :

- les litiges présentés devant les cours et les tribunaux;
- les infractions;
- les peines prononcées;
- les détentions et toutes les déchéances.

Pour simplifier l'analyse de cet article difficile, nous partirons du principe que l'article 8 de la loi sur la vie privée parle de seize catégories de données.

En d'autres termes, nous partirons du principe que chacun des seize domaines correspond à une catégorie de données.
Ces catégories (ou domaines) de données ne peuvent être traitées par la justice et la police que lorsque la finalité du traitement des données est fixée par une loi ou un arrêté royal.
Tous les services publics doivent, en ce qui concerne ces seize domaines, vérifier s'ils sont autorisés à les traiter par ou en vertu d'une loi. C'est ainsi qu'un service qui possède une compétence spécifique, par exemple l'inspection sociale, ne sera pas autorisé à enregistrer la déchéance de la puissance parentale (art. 8, § 1er, 8°). Conformément au Code judiciaire et au Code d'instruction criminelle, les cours et tribunaux sont autorisés à traiter les données relatives aux différends qui leur sont soumis (cf.art. 8, § 1er, 1°) en vue de l'organisation de leur mission générale.

La police et la justice peuvent traiter des données relatives aux infractions dont un individu est suspecté ou dans lesquelles il est impliqué (art. 8, § 1er, 2°), conformément à la mission de la police judiciaire (art. 8 C.I.Cr., art. 39 loi sur la fonction de police). L'article 8 ne parle pas de la police administrative : par conséquent, elle ne constitue pas un domaine protégé.
Les services de police visés par la loi sur la fonction de police peuvent en tout cas se rapporter, pour les fichiers de la police administrative, à l'article 39 de cette loi. Les autres domaines doivent être considérés séparément. La parcimonie est toutefois de règle.
La police des chemins de fer doit se limiter à la recherche et à la prévention des infractions relatives aux chemins de fer. Même si, dans certains cas exceptionnels, cela pouvait lui être utile, elle n'est pas autorisée à mettre sur pied d'un fichier, par exemple des "mauvais payeurs" auprès des autres services publics.

Nous avons dit que les catégories citées à l'article 8 peuvent être traitées à condition que la finalité du traitement des données soit fixée par une loi ou un arrêté royal.
Cette même disposition, à savoir l'article 8, énumère déjà quelques traitements autorisés. Les jugements, les peines, les détentions et mises à la disposition du gouvernement pour la répression du vagabondage et de la mendicité, les mesures d'internement et de mise à la disposition du gouvernement des anormaux et des délinquants d'habitude, etc. peuvent faire l'objet de traitements par le casier judiciaire central, tenu au Ministère de la justice; certaines de ces données peuvent aussi être traitées par les casiers judiciaires communaux (art. 8, § 4). Toutes les données policières et judiciaires énumérées dans l'article 8 peuvent également être traitées sous la surveillance et la responsabilité d'un avocat quand elles concernent le besoin de la défense des intérêts de ses clients, à condition que l'accès en soit réservé à l'avocat lui-même, à ses collaborateurs et à ses préposés, ainsi qu'à son remplaçant et son successeur (art. 8, § 6).

Enfin, les données énumérées à l'article 8 peuvent, moyennant avis préalable de la Commission de la protection de la vie privée et avis préalable donné par écrit à l'intéressé, faire l'objet d'un traitement par des personnes physiques ou morales, désignées par arrêtés royaux délibérés en Conseil des ministres (art. 8, § 5, al. 1er).

Les conditions relatives à la compétence de la justice et de la police doivent être également respectées

L'arrêté royal du 7 février 1995, à savoir l'arrêté royal n° 8 (M.B., 28 02 1995), détermine la compétence de la justice et de la police dans la mise sur pied des bases de données policières et judiciaires.

L'article 1er autorise les autorités et services chargés de missions policières à traiter les données judiciaires

et para-judiciaires. Elles sont définies en référence à l'article 11 de la loi du 8 décembre 1992.
Conformément au souhait exprimé par le Conseil d'Etat, l'article 1er définit que les finalités de cet article sont déterminées par rapport aux descriptions qui en sont données dans la loi du 5 août 1992 sur la fonction de police.
Afin de tenir compte de la spécificité de la finalité décrite dans l'article 11, cinquième alinéa, de la loi du 8 décembre 1992, cette disposition vaut également pour la loi du 11 janvier 1993, relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux.

1. Les personnes autorisées à traiter les données doivent être désignées nominativement par le maître du fichier qui doit tenir la liste des personnes ainsi désignées à la disposition de la personne concernée et de la Commission de la protection de la vie privée;

2. ces personnes doivent être soumises légalement, déontologiquement, statutairement ou contractuellement à l'obligation de confidentialité;

3. dans la déclaration visée à l'article 17, § 1er, de la loi du 8 décembre 1992, le fondement légal ou réglementaire précis de l'autorisation de traitement des données visé à l'article 8 de la loi précitée doit être mentionné.

La police peut échanger des données au niveau international

La loi sur la vie privée est également d'application sur le traitement automatisé de données à caractère personnel, lorsque les traitements sont effectués entièrement ou partiellement à l'étranger, pourvu que ce traitement soit directement accessible en Belgique par des moyens propres au traitement (art. 3, § 1er, 2°).

Le seul critère utilisé pour le traitement automatisé à l'étranger est l'accès direct du traitement par des moyens propres au traitement.
Il doit s'agir d'une forme de traitement dans lequel le gestionnaire peut avoir accès au système sans autre intervention humaine.
Le simple transit de données à caractère personnel en Belgique, sauf en cas d'accessibilité directe, ne tombe pas sous l'"application de la loi.
C'est ainsi par exemple que le traitement à l'étranger, dont le résultat est ensuite communiqué sur papier ou via transfert de fichier, en l'absence d'accès direct par les moyens propres au traitement, ne tombe pas dans le champ d'application de la loi.

La loi est également d'application pour la tenue d'un fichier manuel en Belgique (art. 3, § 1er, 1°).
Etant donné que la définition de "tenue d'un fichier manuel" est reprise dans l'article 1er, § 4 de la loi (voir plus haut), il suffit que l'une des opérations citées (enregistrement, conservation, modification, effacement, consultation ou diffusion de données à caractère personnel) ait lieu en Belgique, pour que la loi sur le fichier manuel soit d'application.

Nous retiendrons de ce qui précède qu'étant donné qu'elles sont interrogeables directement à partir de notre pays les bases de données Schengen et Interpol (toutes deux situées en France) tombent sous les normes de la loi belge sur la vie privée.

L'arrêté royal n° 8 contient des règles importantes dans le cadre de l'échange des données policières et judiciaires, entre les services de police et de justice à l'étranger.
L'article 1er, § 2, de cet arrêté est plus particulièrement consacré au flux transfrontalier des données visées dans l'article 8 de la loi. Les autorités publiques et les services de police belges peuvent communiquer des données énumérées à l'article 8 aux services de police étrangers sous certaines conditions.

P

L'échange est avant tout possible dans le cadre d'une convention internationale.
L'échange est égalementpossible dans le cadre d'une convention intergouvernementale ou par l'intervention d'une organisation internationale de coopération policière.

Etant donné que dans ces cas il n'existe aucune convention internationale, les conditions supplémentaires suivantes doivent également être respectées, lorsque l'Etat auquel les données sont destinées n'offre pas de garanties suffisantes en matière de protection des données policières et judiciaires :

- seules certaines données énumérées à l'article 8 de la loi peuvent être communiquées (cf. A.R.);
- la communication de données doit être nécessaire à l'accomplissement des missions policières des autorités publiques ou services belges, ou de missions équivalentes par les autorités et services étrangers. Cette mission "équivalente" doit se rapporter à un même type de mission dans le domaine de la prévention, de la recherche et de la sanction d'infractions similaires, si elles sont sanctionnées par le droit pénal belge, ceci à l'exception des crimes et délits politiques, les délits de presse et les délits d'opinion;
- la communication ne peut avoir lieu qu'en cas de danger grave et imminent ou dans un but de répression d'un crime ou d'un délit.

Un arrêté royal dressera la liste des Etats offrant une protection équivalente à celle de la loi belge.
Lorsque des informations sont échangées avec un service de police d'un pays qui ne figure pas sur cette liste, le bureau national, chargé de la coopération policière internationale, doit conserver pendant six mois le nom de la personne qui a demandé la communication et les raisons de cette demande (cf. art. 4 A.R. n° 8).

5. Sécurité, interconnexion, communication de données à des tiers

Nous n'entrerons pas ici dans le détail des dispositions légales en matière de sécurité, d'interconnexion, de communication de données à des tiers et des dispositions pénales et dispositions relatives aux compétences de la Commission. A ce sujet, veuillez vous référer à la brève synthèse des obligations qui découlent de la loi et à la bibliographie, toutes deux reprises en fin de cet article.

6. Les services de sécurité

L'Administration de la Sûreté de l'Etat du Ministère de la justice et le Service Général du Renseignement et de la Sécurité du Ministère de la défense nationale tombent, en ce qui concerne les données à caractère personnel nécessaires à l'exercice de leur mission, sous l'application de la loi sur la vie privée (art. 3, § 3). Elles sont toutefois exemptées de pratiquement toutes les obligations imposées au maître du fichier. A savoir les articles 4, 6 à 10, 12, 14, 15, 17, 18, 20 et 31 §§ 1er à 3 qui ne sont pas d'application sur leurs opérations.

Sont toutefois d'application :

- l'important article 5 qui met en place le principe de la finalité, de la proportionnalité et de la légitimité;
- l'article 13 qui autorise la Commission de la protection de la vie privée à garantir l'exercice du droit d'accès et de rectification des enregistrés;
- l'article 16 qui impose au maître du fichier d'établir un état du traitement automatisé et de respecter une série d'obligations en matière de gestion du traitement des données à caractère personnel;
- l'article 19 qui donne à la Commission de la protection de la vie privée un droit de contrôle sur les fichiers manuels;

- le chapitre VI de la loi relative aux interconnexions et flux transfrontaliers de données;
- le chapitre VII relatif à la Commission de la protection de la vie privée sauf les dispositions relatives au droit de plainte des individus;
- le chapitre VIII relatif aux dispositions pénales;
- le chapitre IX relatif à certaines compétences et autres dispositions finales.

7. Aperçu des obligations en matière de bases de données policières

- **Article 5 de la loi sur la vie privée** :
  les finalités de la collecte des données à caractère personnel doivent être préalablement communiquées (principe de la finalité).

- **Article 5 de la loi sur la vie privée et arrêté royal n° 8** :
  les données ne peuvent être recueillies que pour des finalités déterminées et légitimes (principe de la légitimité).

- **Article 5 de la loi sur la vie privée** :
  en règle générale, les données ne peuvent pas être utilisées pour une finalité autre que celle décrite (principe de l'utilisation limitée ou principe de conformité).

- **Articles 5, 6, 7 et 8 de la loi sur la vie privée** :
  les données policières doivent être obtenues et traitées de manière honnête et légitime (principe de l'honnêteté). Certaines données ne peuvent normalement pas être recueillies (principe de la collecte limitée).

- **Articles 5 et 16 de la loi sur la vie privée** :
  les données à caractère personnel des bases de données policières doivent être adéquates et non excessives, correctes et complètes et ne peuvent pas être conser-

vées plus longtemps que nécessaire (principe de la proportionnalité ou principe de la qualité des données et de leur limitation dans le temps).

- **Article 16 de la loi sur la vie privée** :
en principe, les données à caractère personnel ne sont pas accessibles aux tiers (principe de la limitation de la diffusion).

- **Article 18 de la loi sur la vie privée** :
tous ceux enregistrés dans la base de données de la police ont un droit d'information indirect. Ils sont mis au courant de l'existence des bases de données policières via le registre public tenu par la Commission de la protection de la vie privée (principe de la publicité et droit d'information).

- **Article 13 de la loi sur la vie privée** :
tous les enregistrés ont un droit d'accès indirect de rectification, et, dans certains cas, un droit d'effacement et d'interdiction d'utilisation (principe du droit d'intervention individuelle).

- **Article 5 sur la loi sur la vie privée** :
l'utilisation de profils dans l'évaluation des enregistrés est en principe interdite (interdiction de profil).

- **Article 16 de la loi sur la vie privée** :
il faut toujours désigner un responsable de la collecte des informations (principe de la responsabilité). Les données doivent être protégées techniquement (principe de la sécurité).

8. Brève bibliographie

- De Hert, P., "Persoonsgegevens", *Postal Memorialis*, à paraître.
- Boulanger, M.-H., De Terwagne, C. et Leonard, Th., "La protection de la vie privée à l'égard des traitements

de données à caractère personnel - La loi du 8 décembre 1992" *J.T.*, 1992-93, 370.
- De Schutter, B. et De Hert, P., "L'usage par la police d'informations : la loi sur la vie privée", *Politeia*, 1994, 6, 7-14.
- X, "Bescherming van het privé-leven. Opgepast mat uw bestanden", *Vbo Bulletin*, 1995, 1, 14-18.
- Lemmens, P., "De verwerking van persoonsgegevens door politiediensten et de eerbieding van de persoonlijke levensfeer", *Liber Amicorum Jules D'Haenens*, Gent, Mys et Breesch, 1993.
- Centrum voor Internationaal Strafrecht, "De Belgisch privacy-wetgeving, een eerste analyse", *R.W.*, 1992-93, 1145-1154.

Informations pratiques

Conformément à l'article 35 de la loi sur la vie privée, la Commission dispose d'un secrétariat dont le personnel est rattaché au Ministère de la justice.

Commission de la protection de la vie privée
Ministère de la justice
Rue de la Régence 61,
1000 Bruxelles
tél. : 02/542.72.00
fax : 02/542.72

A collaboré à ce numéro : Paul De Hert
Rédaction finale : C. Goffaux, F. Van Emelen

Editeur responsable : R. De Vries, Kouterveld 2, 1831 Diegem