APPROCHE DE LA NOTION DE VIE PRIVEE

par
Hugo VANDENBERGHE
Professeur à la K.U.L.

1. Je sais bien que la notion de "vie privée" n'a, ni chez les organisateurs ni - peut être - chez les participants, une place opérationnelle pour résoudre les problèmes posés par l'informatique. Et pourtant ce concept juridique est essentiel dans cette matière.
Une fois de plus, j'ai donc l'honneur de prêcher à l'heure de l'angelus devant une paroisse infidèle.
Commençons avec une définition classique de la vie privée : c'est l'espace nécessaire dans le sens littéral et figuratif du mot pour pouvoir mener librement une existence propre.

Pour ces raisons l'individu doit être protégé contre :
a) toute immixtion dans sa vie privée, familiale et domestique;
b) toute atteinte à son intégrité physique ou mentale ou à sa liberté morale ou intellectuelle;
c) toute atteinte à son honneur ou à sa réputation;
d) toute interprétation dommageable donnée à ses paroles ou à ses actes;
e) la divulgation hors de propos de faits gênants en rapport avec sa vie privée;
f) l'utilisation de son nom, de son identité ou de son image;
g) toute activité tendant à l'espionner, l'épier, le surveiller, et le harceler;
h) l'interception de sa correspondance;
i) l'utilisation malveillante de ses communications privées, écrites ou orales;
j) la divulgation de renseignements communiqués ou reçus par lui sous le sceau du secret professionnel.

C'est dans ce sens qu'il faut interpréter l'article 8 de la Convention Européenne des Droits de l'homme qui consacre le respect de la vie privée.
Les autres sources du droit au respect de la vie privée se trouvent dans les règles de droit interne. Elles concernent les atteintes à la personne, à l'intégrité physique ou mentale ou à la liberté morale ou intellectuelle; les activités tendant à l'espionner, surveiller ou harceler; les atteintes à l'honneur et à la réputation et les faits assimilés; l'utilisation du nom, de l'identité ou de l'image; la divulgation de renseignements couverts par le secret professionnel.
S'il est donc possible de conclure que la liberté de "s'enfermer chez soi" est généralement reconnue, il subsiste néanmoins la question délicate de savoir quelle est la forme et le contenu de la vie privée.
Si on exige une définition de la vie privée - more geometrico - alors on demande la probatio diabolica, la preuve diabolique. Le droit est en effet une science précise mais pas exacte. Et la notion "vie privée" est une notion qualitative.
D'abord, la terminologie dans le droit comparé est assez variée (vie privée, sphère intime, domaine personnel, allgemeines Persönlichkeitsrecht, privacy, etc...). Ensuite, des divergences assez importantes existent entre les différents systèmes juridiques, surtout entre la tradition anglosaxonne - le berceau de la "privacy" - et des pays européens comme la France ou l'Allemagne et leurs satellites. Les conclusions auxquelles ont abouti le Congrès des juristes des pays nordiques en mai 1967 et le 3ème colloque international sur la Convention Européenne des Droits de l'homme (Bruxelles, 1970) donnent une conception extensive du droit au respect de la vie privée qu'on pourrait alors identifier avec les droits de la personnalité.

En général, lit-on dans un rapport du Comité d'experts des Droits de l'homme du Conseil de l'Europe, le concept de vie privée recouvre toutes les valeurs qui se rapportent à l'individu et qui doivent être protégées contre les ingérences extérieures.
Mais cela est également vrai de la grande majorité d'autres droits fondamentaux qui sont des droits individuels ayant pour but de garantir à l'individu un domaine de liberté.
Toutefois les valeurs désignées par l'expression "vie privée" se rattachent à l'individu d'une manière particulièrement étroite.
Enfin, on souligne que la portée de la vie privée se modifie avec les circonstances de temps et les conditions de vie concrètes dans lesquelles on se trouve.

2. Mais quelle est donc la relation entre la "vie privée" et la protection des données personnelles enregistrées dans les banques de données ?
Pour comprendre cette question, il faut préalablement poser le problème dans son contexte social nouveau.
Notre société est devenue une "information based society", une société d'information. Des données de toute sorte et d'une ampleur exceptionnelle sont nécessaires pour pouvoir déterminer la politique à suivre aussi bien dans le secteur public que dans le secteur privé. D'où l'utilité de la collecte, du stockage et de la diffusion d'informations personnelles au moyen de banques de données (Data Bank Society).
La société du bien-être a évolué vers une société de type tutélaire et bureaucratique, l'homme y est plutôt un objet qu'un citoyen.
La distribution des biens et des services s'organise de manière de plus en plus réglementaire et autoritaire; l'apport de la créativité individuelle diminue. C'est pour cette raison que la société a besoin d'informations importantes sur le consommateur des biens sociaux.
Ainsi les banques de données peuvent devenir le centre d'un système de surveillance qui transformera notre société en un monde transparent dans lequel notre foyer, nos ressources financières ("le voyeurisme financier" est de mise), nos fréquentations, notre condition mentale et physique seront exposés à certains observateurs. Ils pourront obtenir un "bleu" de chaque individu; c'est l'installation de la "datacratie".
La doctrine souligne amplement que les systèmes modernes d'enregistrement fonctionnent sous le signe de "mass surveillance", la surveillance de la clientèle indivise et anonyme.
Et c'est ici que le privacy informationel se présente dans un tout autre contexte que dans le passé. La vie privée n'est plus essentiellement définie dans son aspect physique et spatial, ce n'est plus un soi-disant concept élitiste, ce restant de la civilisation victorienne, surtout utilisé par des personnages publics qui étaient les victimes de la publicité indésirée des "mas media". Non, la "vie privée" obtient une toute nouvelle dimension. La protection des données personnelles devient un problème indépendant où plusieurs aspects de la liberté personnelle s'affirment. Ce concept informationnel de privacy n'est plus basé sur l'idée que l'homme doit pouvoir se retirer dans sa sphère privée. La base juridique est beaucoup plus large, c'est le droit de la personne de conserver son autonomie et son identité, sa "self-destination".
Comme le dit Alan Westin, qui, en 1967, a donné pour la première fois un exposé convaincant sur le "fichage" de la personne comme menace

pour le privacy
groups or insti
what extent info
Et Miller : "Th
the individual'
relating to him
social relations
Mais des contac
et le privacy i
blème du stocka
sonnelles.
Le concept vie
double significa
to est significa
Et l'enregistrem
la vie privée s
vidu dans un syst

3. Tenant compte
ques de données
? Comment ? Pa
ments spécifique
part, l'applicat
comme la "protec
la personnalité"
se limiter à la
ques de sécurité
databanquier.
"A major theme of
and as an individ
(Personnal Privac
Protection Study
La complexité de
être une excuse p
Neuf pays sont a
entre l'informati
1973), les Etats-
Allemande (la loi
bourg, la France
triche (18 octobre
Parmi eux, sept pa
l'Allemagne Fédér
Danemark et l'Autr
soit au niveau du
province (Canada),
D'autres disposent
la Norvège. D'autr

4. Pour élaborer
nir quelles persor
morales ?
Dans l'ensemble de
vée" on parle tar
d'Allemagne, U.S.A
et morales" (Belgiq

pour le privacy, "the right of privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others".
Et Miller : "The basic attribute of an affective right of privacy is the individual's ability to control the circulation of information relating to him - a power that often is essential for maintaining social relationship and personal freedom".
Mais des contacts directs entre la notion classique de vie privée et le privacy informationnel demeurent. Je cite entre autres le problème du stockage et le problème de la combinaison des données personnelles.
Le concept vie privée, en relation avec l'informatique, a donc une double signification. La protection de la sphère privée sensu stricto est significative pour le problème des données sensibles.
Et l'enregistrement des autres données peut poser des problèmes pour la vie privée sensu stricto mais aussi pour la position de l'individu dans un système social donné.

3. Tenant compte de la spécificité des problèmes que posent les banques de données (quelles informations personnelles peut-on rassembler ? Comment ? Par qui ? Qui peut les utiliser ? etc...), des réglements spécifiques sont nécessaires (computer Bill of Rights). D'une part, l'application prétorienne d'une clausule juridique générale, comme la "protection de la vie privée" ou "le respect des droits de la personnalité" ne sauront suffire dans ce domaine. D'autre part, se limiter à la solution déontologique et à l'utilisation des techniques de sécurité, c'est affirmer et reconnaître les prérogatives du databanquier.
"A major theme of this report is that privacy, both as a social value and as an individual interest, does not and cannot exist in a vacuum. (Personnal Privacy in an Information Society", Report of the Privacy Protection Study Commission, 1977, 21).
La complexité de la démarche, l'absence de solutions simples ne peut être une excuse pour l'inertie législative.
Neuf pays sont actuellement dotés de lois réglementant les rapports entre l'informatique et la "vie privée" : la Suède (la loi du 11 mai 1973), les Etats-Unis (Privacy Act of 1974), la République Fédérale Allemande (la loi du 27 janvier 1977), le Canada, la Suisse, le Luxembourg, la France (7 janvier 1978), le Danemark (8 juin 1978) et l'Autriche (18 octobre 1978).
Parmi eux, sept pays possèdent une loi au niveau "national": la Suède, l'Allemagne Fédérale, les Etats-Unis, la France, le Luxembourg, le Danemark et l'Autriche. D'autres pays disposent d'un statut protecteur soit au niveau du Land (Hesse, Bavière, Rhémanie, en Allemagne), d'une province (Canada), soit du canton (Bâle-Ville, Vaud, Zürich).
D'autres disposent d'un projet de loi rédigé, tels la Belgique ou la Norvège. D'autres enfin disposent d'études avancées.

4. Pour élaborer ce "computer Bill of Rights", il faut d'abord définir quelles personnes sont concernées: les personnes physiques et/ou morales ?
Dans l'ensemble des textes relatifs à la protection de la "vie privée" on parle tantôt de "personnes physiques" (République Fédérale d'Allemagne, U.S.A., Suède, France), tantôt de "personnes physiques et morales" (Belgique).

La prolifération de fichiers nominatifs sur les personnes morales justifie pleinement une législation en la matière, mais il faut se demander si une identification totale avec les personnes physiques n'est pas contre-indiquée.

5. La défense de la liberté "informationnelle" implique le renforcement de la position juridique individuelle de la personne concernée.
Il faudra donner à l'individu la possibilité de savoir où, par qui, et quelles données sont stockées et qui peut les utiliser (droit de regard). Ensuite, faut-il prévoir un droit de correction ?
La plupart des textes législatifs prévoient la possibilité pour les personnes de connaître les données qui les concernent. La communication des données suppose, le plus souvent, une démarche explicite de l'intéressé à qui la réponse doit être fournie, mais elle peut être obligatoire sans qu'il y ait eu intervention préalable de cette demande explicite de l'intéressé, p.ex. lorsqu'il s'agit du "premier enregistrement" (Belgique, République Fédérale Allemande, Suède).
La loi américaine pousse les choses plus loin, puisqu'elle fait obligation aux agences de fournir aux intéressés, à leur demande, toute divulgation faite à une autre agence que l'agence collectrice ou à un individu autre que l'intéressé.
Le contenu de cette communication peut varier: ainsi l'individu pourrait avoir la possibilité de connaître non seulement les données de base mais aussi les données résultant d'un traitement ("l'information résultat"). La quasi-totalité des textes examinés prévoit la possibilité pour une personne de faire corriger certaines données erronées. Une procédure de recours interne à l'administration détentrice est d'abord envisagée, à l'exception du projet belge qui exige de passer par le pouvoir judiciaire.
Il faut aussi noter la publicité qui, dans certains pays (U.S.A., République Fédérale Allemande, Belgique), doit être donnée à l'existence de tel ou tel fichier, les buts des traitements, les avis des instances de contrôle, par l'obligation de tenir un registre public.

6. Un point capital dans cette matière est la question du stockage des données.
Peut-on stocker toute donnée ? Y a-t-il au contraire des restrictions pour les données sensibles ? Quoique la notion de sensibilité soit plus ou moins relative (la sensibilité d'une donnée dépend entre autres du contexte social) on ne peut cependant nier qu'un traitement différent suivant la nature des données est nécessaire.
Pour résoudre ce problème, le professeur Bing a fait une proposition intéressante. Il a essayé d'établir une liste complète des données personnelles, tenant compte de leur sensibilité pour la personne concernée ("sensivity grading").
Alors l'approche législative de ce problème dépendra du grade de sensibilité de l'information à stocker (information personnelle générale, information intime, information discréditante).
Plusieurs pays (p.ex. U.S.A., Suède, France, Belgique) ont exclu en principe, sauf dérogation, les données les plus intimes comme p.ex. l'opinion politique et religieuse. En outre, un statut spécial est prévu pour les données pénales et médicales.
Mais ce serait une erreur d'axer une réglementation juridique exclusivement sur les données sensibles.

Chaque donnée a
La possibilité
portante que la
Comme le disai
and compiling
is trivial in
cerned".
Ainsi, le numér
sensibilité dir
tère exceptionn
pour entrer dar
de naissance, le
La question se
uniforme est e
le rejettent.

7. Dans le con
tiative personn
recte.
C'est pour cett
prié au contrôle
Tous ces organi
que les différen
La différence l
la création, la
Les solutions pe
loi suédoise et
de contrôle un
vent être créés
les fichiers crée
De l'autre côté,
prié a essentiell
Un autre problèm
autres autorités
latif ou à l'Exéc
Il me semble, en
larges à cet ord
dant puisse être

8. Conclusions
Le grand danger
des données pers
"Data-Security" s
s'y trompe pas,
(protection de d
liberté pour l'in
mation personnell
dynamique propre.
envers le changem
est applicable: pl
L'informatique es
et donc marginalis
C'est la "semiocr
informatique.

Chaque donnée a, en effet, une valeur informative dérivée.
La possibilité de combiner une donnée avec les autres est aussi importante que la sensibilité.
Comme le disait la commission suédoise : "But even the collection and compiling of large quantities of information, each item of which is trivial in itself, may effect the privacy of the individuals concerned".
Ainsi, le numéro national pour chaque citoyen n'est pas d'une grande sensibilité directe, mais il a une valeur informative dérivée de caractère exceptionnel. D'autres "key data", c'est-à-dire des données-clé pour entrer dans les banques de données, existent: le nom, la date de naissance, le numéro bancaire ou de la sécurité sociale.
La question se pose de savoir si l'introduction générale d'un numéro uniforme est en soi acceptable. La plupart des pays démocratiques le rejettent.

7. Dans le contrôle de l'utilisation des banques de données, l'initiative personnelle n'aurait en tout cas qu'une signification indirecte.
C'est pour cette raison que les textes parlent d'un organisme approprié au contrôle des fichiers informatiques ("Commission Bancaire").
Tous ces organismes jouissent évidemment d'un pouvoir d'investigation que les différentes lois ne négligent pas de préciser.
La différence la plus nette vise leur pouvoir de décision quant à la création, la tenue, le fonctionnement ... des fichiers.
Les solutions peuvent ici se ranger en deux catégories. D'un côté la loi suédoise et le projet belge, qui visent à donner à l'organisme de contrôle un véritable pouvoir de décision : les fichiers ne peuvent être créés et tenus qu'avec autorisation (réserve faite pour les fichiers créés par le Parlement).
De l'autre côté, les législations pour lesquelles l'organisme approprié a essentiellement une fonction d'avis et de contrôle.
Un autre problème concerne la relation desdits organismes avec les autres autorités; l'organisme ad hoc doit-il être rattaché au Législatif ou à l'Exécutif ?
Il me semble, en tout cas, qu'il faut donner des pouvoirs assez larges à cet organisme pour que la garantie d'un contrôle indépendant puisse être réalisé.

8. Conclusions
Le grand danger que je perçois est l'opinion que l'enregistrement des données personnelles est un instrument politiquement neutre. Le "Data-Security" suffirait pour protéger le citoyen. Mais qu'on ne s'y trompe pas, cette notion signifie non pas la "Datensicherung" (protection de données), mais la "Datenschutz", c'est-à-dire la liberté pour l'individu ou pour les groupes de disposer de l'information personnelle. L'automatisation des données personnelles a une dynamique propre. Elle est "self contained", végétative et répressive envers le changement et le renouveau. Ici aussi la loi de Parkinson est applicable: plus on sait, plus on veut savoir.
L'informatique est réductrice. Certaines valeurs sont "indicibles" et donc marginalisées.
C'est la "semiocratie", l'art d'imposer les valeurs et le vocabulaire informatique.

Nous retrouvons ici la fable d'Orwell où "Big Brother" prenait le pouvoir en inventant Novlang, langage réservé au dominant, car rendant indicibles certaines aspirations.
Comme le disait Friedrich dans "Secrecy versus Privacy : the Democratic Dilemma", la démocratisation implique que la vie publique devient de plus en plus publique et la vie privée de plus en plus privée.
Là est la divergence essentielle avec les systèmes totalitaires. Dans ces systèmes, la vie politique se déroule dans l'obscurité tandis que la vie privée du citoyen doit être transparente.
Dans ce sens, la protection du domaine privé est une défense de la démocratie, car l'informatisation totale nous mène à l'état totalitaire.
En l'absence d'une réglementation juridique appropriée, l'Etat SS en civil est ante portas, devant la porte.