Principe de finalité

Les différents aspects du principe de finalité

Le principe de finalité est une composante fondamentale de la loi « Informatique et Libertés » du 6 janvier 1978 modifiée le 6 août 2004.
Les finalités d'un traitement de données à caractère personnel (DCP) sont déterminées par le responsable du traitement.

Les finalités d'un traitement de DCP doivent être déterminées, explicites et légitimes.

Les finalités étant précisées, les caractéristiques essentielles du traitement doivent être conformes à ces finalités.

1°) La qualité des données

La collecte et le traitement des données doit se faire de manière loyale et licite. Ces données doivent être adéquates, pertinentes et non excessives au regard des finalités ; elles doivent être exactes, complètes et, si nécessaire, mises à jour.

2°) La durée de conservation des données

Ces données ne doivent être conservées que pendant un temps qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles ont été collectées et traitées.

3°) Les destinataires des données

Seules les personnes ou les catégories de personnes dont le concours est indispensable à la réalisation des finalités du traitement, doivent avoir accès à ces données.

Quelques précisions de sens

Essayons, dans un premier temps, de préciser le sens des termes de la loi (mentionnés ci-dessus).

Les finalités doivent être précises, bien délimitées, formulées clairement, ne laissant aucun doute, fondées en droit.

Les données doivent être collectées et traitées de manière honnête, conforme à la loi, ou du moins non défendue par la loi. Elles doivent être adaptées à leur but, proportionnées à leur objet ; elles ne doivent pas être surabondantes ni dépasser la mesure souhaitable ou permise. Elles doivent en outre être correctes, non entachées d'erreur, exhaustives et actualisées. Les données inexactes ou incomplètes au regard des finalités pour lesquelles elles ont été collectées ou traitées doivent être effacées ou rectifiées.

La durée de conservation des données doit être prévue lors de la création du traitement (en conformité avec les finalités) ; ces données doivent ensuite être effacées ou rendues anonymes pour des traitements à des fins statistiques par exemple.

Les destinataires des données doivent être bien identifiés et précisés (en conformité avec les finalités) lors de la création du traitement ; des mesures techniques et organisationnelles visant à empêcher tout accès non autorisé, doivent être prévues et mise en place.

Le respect du principe de finalité

Une application correcte et non laxiste du principe de finalité par les responsables de traitements de DCP constitue une garantie essentielle de respect des dispositions de l'article 1er de la loi « I et L » qui dit que l'informatique « ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».
Cependant, les violations, plus ou moins graves, du principe de finalité sont monnaie courante. Voyons quelques exemples, que les débats et les réunions à venir pourront évidemment développer et compléter.

Peut-on parler de finalités déterminées, précises et bien délimitées pour :

- le STIC dans lequel sont enregistrées des comptes rendus d'enquêtes, issus des procédures pénales, à des fins de recherches criminelles, mais qui est aussi utilisé pour des enquêtes administratives ?
- le FNAEG qui, créé en 1998, a vu son champ d'application s'élargir considérablement en 2001 et en 2003 avec, aujourd'hui, une définition très large des infractions donnant lieu à l'enregistrement d'une empreinte génétique ?
- le projet de décret EDVIRSP (EDVIGE.2) qui ouvre un champ quasi illimité au fichage puisqu'il concerne toutes les personnes qui « peuvent porter atteinte à la sécurité publique » ainsi que « les personnes faisant l'objet d'enquêtes administratives » ?

Peut-on considérer que la qualité des données est respectée quand :

- dans le STIC, l'enquête rendue publique par la CNIL en janvier 2009 montre qu'il existe des taux d'erreur très importants concernant aussi bien la saisie des données que leur mise à jour ?
- dans JUDEX, les contrôles effectués par la CNIL en 2005 avaient fait apparaître des taux d'erreur sur les données importants, bien qu'inférieurs à ceux du STIC ?
- on constate le nombre et la diversité des données mentionnées dans le projet de décret EDVIRSP ?
- on sait que le nombre de personnes fichées dans le FNAEG a cru de façon exponentielle ces dernières années, pour atteindre plus de 800 000 profils génétiques au 1er octobre 2008 ? A quand un contrôle de ce fichier ?

La durée de conservation des données fait apparaître une double nécessité :

1- effacer les données à l'expiration du délai prévu ; les résultats des contrôles effectués par la CNIL dans le STIC et dans JUDEX montrent que cette obligation n'est pas respectée.
2- prévoir une durée de conservation des données qui ne soit pas excessive par rapport aux finalités du traitement ; les durées de conservation, pour certaines catégories de personnes, prévues dans le STIC, le FNAEG, EDVIRSP, par exemple, posent manifestement problème.

Concernant les destinataires des données, le principe de finalité est-il toujours respecté ?

Non, si l'on en croit le rapport de la CNIL sur le STIC.
L'étude des dispositions relatives aux destinataires dans le projet EDVIRSP nous conduit à la même conclusion.

Fiche rédigée par Félix Paoletti
CREIS-Terminal (Centre de coordination des Recherches et Enseignements en Informatique et Société)

CREIS : http://www.creis.sgdg.org/

TERMINAL : http://www.terminal.sgdg.org/