Zeitschrift: Vermessung, Photogrammetrie, Kulturtechnik : VPK = Mensuration, photogrammétrie, génie rural

Herausgeber: Schweizerischer Verein für Vermessung und Kulturtechnik (SVVK) = Société suisse des mensurations et améliorations foncières (SSMAF)

Band: 95 (1997)

Heft: 1

Artikel: La protection des données personnelles lors de l'utilisation d'informations spatiales

Autor: Walter, J.-P.

DOI: https://doi.org/10.5169/seals-235304

La protection des données personnelles lors de l'utilisation d'informations spatiales

Les systèmes d'informations géographiques font partie intégrante de la structure informationnelle et sont un instrument de gestion important non seulement dans le secteur public, mais également dans le secteur privé. Les SIG permettent également le traitement de données personnelles. Ce traitement est soumis aux dispositions du droit de la protection des données. En particulier, les SIG doivent respecter les principes fondamentaux de licéité, de proportionnalité, de finalité, de bonne foi, d'exactitude et de sécurité.

Die geographischen Informationssysteme bilden heute einen integrierenden Bestandteil der Informationsstruktur und sind ein wichtiges Verwaltungsinstrument nicht nur im öffentlichen Sektor sondern auch in der Privatwirtschaft. Die GIS ermöglichen ebenfalls die Behandlung von persönlichen Daten. Diese Behandlung unterliegt den Bestimmungen über den Datenschutz. Im besonderen müssen die GIS die fundamentalen Prinzipien der Berechtigung, der Proportionalität, der Zweckbestimmung, von Treu und Glauben, der Wahrheit und der Sicherheit beachten.

I sistemi d'informazione geografica sono parte integrante della struttura informativa e costituiscono un importante sistema di gestione, non solo nell'ambito pubblico ma anche in quello privato. I SIG permettono anche il trattamento di dati personali, sottostante alle disposizioni del diritto della protezione dei dati. In particolare, i SIG devono rispettare i principi fondamentali di liceità, proporzionalità, finalità, buona fede, esattezza e sicurezza.

J.-Ph. Walter

1. Système d'information géographique, instrument performant de traitement des données personnelles?

1.1 Système d'information

Cette fin de siècle est marquée par l'avènement de la société d'informations et l'explosion des technologies téléinformatiques. Ces technologies bouleversent et vont continuer de bouleverser profondément notre environnement social et nos manières de penser et d'agir. L'information est ainsi appelée à jouer un rôle fondamental dans le monde de demain. La quantité d'informations à disposition ne sera pas déterminante. Toutefois, de la qualité de l'information à disposition, de notre capacité et de nos possibilités d'accès aux informations pertinentes dépendront nos décisions individuelles, sociales, professionnelles, politiques, culturelles ou économiques. Parmi, ces technologies d'informations, les systèmes d'informations géographiques ont un rôle important à jouer et font partie intégrante de l'infrastructure informationelle. S'ils étaient traditionnellement essentiellement réservés à certains domaines d'activités de nos administrations publiques (et je pense en particulier à la statistique, à l'environnement, à l'aménagement du territoire ou encore au registre foncier et mensurations cadastrales), ils deviennent aujourd'hui un instrument important non seulement dans le secteur public, mais également dans le secteur privé (et je pense notamment au domaine des assurances, du marketing, du renseignement de crédit, du tourisme). Les systèmes d'informations géographiques ont un impact technologique et informationnel immense qui confèrent à leurs concepteurs et à leurs utilisateurs une lourde responsabilité sociale. Au côté des aspects positifs de ces systèmes, qu'en tant qu'utilisateurs vous connaissez et sur lesquels je n'ai pas besoin de m'attarder, nous devons également prendre en compte les aspects négatifs du recours à de tels systèmes pour essayer, non d'empêcher l'utilisation de ces techniques, mais d'éliminer ou de diminuer ces effets négatifs. L'un de ces effets négatifs – et c'est le seul sur lequel je vais m'arrêter – a trait aux risques d'atteinte à la personnalité et aux droits et libertés fondamentaux des personnes.

Lorsque l'on aborde le problème des systèmes d'information géographique, nous ne pensons pas au premier abord que cela puisse toucher la protection des données. Pour le commun des mortels, un système d'information géographique est lié au territoire, à l'espace et à l'environnement. Son contenu ne doit vraisemblablement pas contenir d'informations liées à la personne et ses finalités relèvent de la planification, de la recherche, de la statistique, de l'aménagement du territoire, de l'environnement, du registre foncier et des mensurations cadastrales. Alors pourquoi aborder la question de la protection des données personnelles lors de l'utilisation d'informations spatiales ?

Si nous examinons les choses d'un peu plus près, nous nous apercevons que le système d'information géographique, en recourant à l'utilisation de banques de données relationnelles, permet la saisie à la fois des données géométriques (données géocodées, position, coordonnées) et des données de fait (caractéristiques, attributs) et de lier ces données dans un rapport complexe et logique tant au niveau du contenu que de l'espace. Nous constatons que parmi ces données de fait, figurent également des données personnelles. Le SIG couplé aux techniques de télédétection, notamment par satellite, permet aisément et précisément de repérer sur une carte des phénomènes qui sont difficilement relevables par une observation sur place, par exemple maladies de

végétaux ou pollution marine, et ainsi d'intervenir rapidement. Il permet également d'identifier des personnes physiques ou morales en relation avec un lieu et/ou un objet/immeuble: repérage d'un véhicule, localisation d'un immeuble, surveillance de l'utilisation de subventions agricoles, contrôle des sinistres, etc. Les SIG sont ainsi des outils très performants comme technologie d'intégration des données. Il est en particulier possible d'intégrer les données en les connectant à leur localisation géographique (procédure de géocodage). Dans un secteur comme celui du marketing ou des assurances, cette technique est très prometteuse et offre des possibilités insoupçonnées d'assemblage ou de compilation des données à partir de différentes sources d'informations touchant aussi bien les ménages, les individus que les entreprises. Le SIG devient ainsi un instrument performant dans l'analyse et le traitement des données personnelles. Grâce à leur puissance d'intégration des données et leur capacité d'analyse et grâce au fait que les données ont un caractère local ou spatial, ces systèmes ont un potentiel d'intrusion dans la vie privée que d'autres systèmes d'informations ne connaissent pas.

1.2 Données personnelles

Le SIG n'est concerné par la protection des données que dans la mesure où il intègre des données personnelles, c'est-à-dire des informations se rapportant à une personne identifiée ou identifiable (art. 3, let. a, LPD). Une personne est identifiée lorsqu'il ressort directement des informations qui sont traitées qu'il s'agit d'une personne déterminée et d'elle seule. Tel est le cas lorsque les données sont nominatives, à savoir que le nom, le prénom et généralement l'adresse de la personne sont connues et traitées. Une personne est identifiable lorsque les données traitées permettent d'identifier la personne, notamment par corrélation indirecte d'informations tirées des circonstances ou du contexte (par exemple, lorsqu'à partir de données foncières, on peut remonter au propriétaire d'un immeuble donné). Une personne ne sera pas identifiable si son identification nécessite des moyens disproportionnés (délai, activité) que, selon le cours ordinaire des choses, aucun intéressé ne mettrait en oeuvre. Dans un tel cas, les données sont alors anonymes. Les moyens techniques actuels, notamment dans le cadre des SIG, rendent la notion d'anonymat très relative.

1.3 But de la protection des données

Dès le moment où le SIG contient des données personnelles, il est soumis au droit de la protection des données. Le but général du droit de la protection des données n'est pas de protéger les données personnelles, – cela relève notamment de la sécurité des données ou du droit de la propriété intellectuelle –, mais de protéger la personnalité des personnes physiques ou morales et de garantir le respect des droits et libertés fondamentaux lors du traitement de données personnelles par des personnes privées ou des organes étatiques. Par traitement, il faut comprendre l'ensemble des opérations, effectuées ou non à l'aide de procédés automatisés, relatives à des données personnelles et notamment la collecte, l'enregistrement, la conservation, l'exploitation, l'adaptation, la modification, la consultation, la communication, la publication, le rapprochement ou l'interconnexion, l'archivage ou la destruction des données (art. 3, let e et f, LPD).

Le développement actuel des technologies de l'information qui se caractérise par un décloisonnement et une interpénétration croissante des systèmes d'information – les SIG en sont une illustration –, tend à banaliser le traitement des données personnelles et place les personnes au sujet desquelles des données sont traitées dans une position inconfortable: à son insu, l'individu devient transparent face à la société. L'individu perd de plus en plus la vue d'ensemble sur les traitements qui le concernent et dès lors la maîtrise sur ses propres informations. Il n'est souvent plus en mesure de savoir qui connaît quelque chose sur lui, où se trouvent ses propres données, dans quels buts elles sont traitées ou à qui elles sont communiquées. Le traitement de données personnelles diminue la capacité de jugement, d'opinion, d'action et de décision de l'individu principalement lorsqu'il n'est pas à même d'influencer le processus de traitement, d'adapter son comportement et de déterminer quelles données le concernant peuvent être traitées. Or, en s'appuyant sur le respect de la personnalité et des droits et libertés fondamentaux de la personne, toute personne doit pouvoir exercer une certaine maîtrise sur ses informations et pouvoir interdire ou restreindre leur traitement par des tiers. Il doit pouvoir déterminer ou du moins influencer la connaissance et l'image, que son environnement proche ou lointain a de lui.

Pour permettre aux personnes d'exercer leur droit à la maîtrise des informations qui les concernent (droit à l'autodétermination individuelle en matière d'informations), il est nécessaire de définir certaines règles de conduite pour le traitement de données personnelles. Il ne s'agit pas par là d'empêcher le traitement de données personnelles, notamment dans les systèmes d'informations géographiques, mais de concilier les intérêts publics ou privés pouvant légitimer ces traitements avec le respect de la personnalité et des droits fondamentaux de la personne.

2. La législation fédérale sur la protection des données

J'aborde ainsi les dispositions de la protection des données applicables au traitement de données personnelles dans le cadre des systèmes d'informations géographiques. Je me limite ici à invoquer les dispositions du droit fédéral et je laisse de côté les règles du droit cantonal. Toutefois, les principes que je vais évoquer, se retrouvent également dans la plupart des législations cantonales. J'aborde tout d'abord les dispositions générales applicables aux SIG en matière de protection des données, avant d'examiner quelques règles spécifiques applicables au système

GEOSTAT de l'Office fédéral de la statistique.

2.1 But et champ d'application

La loi fédérale sur la protection des données a été adoptée le 16 juin 1992 et est entrée en vigueur le 1er juillet 1993. Cette loi tend à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données personnelles. Elle s'applique aux traitements de données personnelles effectués par des personnes privées et par des organes fédéraux. Elle ne s'applique en principe pas aux traitements effectués par des organes cantonaux. Elle ne s'applique également pas aux registres publics relatifs aux rapports juridiques de droit privé, tel que le registre foncier.

Cette loi repose sur quatre piliers, à savoir:

- l'énoncé de principes régissant le traitement de données à caractère personnel,
- les obligations des organes fédéraux et des personnes privées qui traitent des données personnelles,
- les droits des personnes concernées et en particulier le droit d'accès aux données les concernant contenues dans un fichier,
- la surveillance et en particulier l'institution d'un préposé fédéral à la protection des données.

2.2 Règles matérielles de la protection des données

Je m'arrête plus spécifiquement sur le premier pilier, à savoir les principes régissant le traitement de données à caractère personnel ou les règles matérielles de la protection des données.

La mise en place et l'exploitation d'un système d'information géographique par des organes fédéraux ou par des personnes privées doivent intervenir dans le respect des règles matérielles de la LPD, à savoir les principes généraux du traitement, les règles matérielles proprement dites et certaines dispositions sectorielles. Il s'agit par là d'éviter un traitement illimité et disproportionné, qui est en soi aisément réalisable vu la puissance des moyens technologiques en présence. Ces règles présupposent une constante mise en balance des intérêts de celui qui veut traiter des données (notamment par une clarification de ses besoins réels en fonction des tâches à accomplir) avec le droit des personnes à la maîtrise des informations qui les concernent.

2.2.1 Les principes généraux régissant le traitement de données personnelles

Les articles 4 à 7 de la LPD énoncent ainsi sept principes fondamentaux de la protection des données. Ces principes constituent en quelque sorte le noyau dur de la loi et régissent aussi bien les organes publics fédéraux que les personnes privées qui traitent des données personnelles. Ces principes qui sont des normes de comportement, sont les suivants:

La collecte de données doit être licite:

Ce principe (art. 4, 1er al. LPD) exprime le principe général de loyauté non seulement quant au droit de collecter des données, mais également quant au mode de collecte. Ce principe tend à éviter que dès le début, le traitement des données soit entaché d'irrégularité. Une telle collecte illicite résultera de l'obtention de renseignements par violation de domicile. Une observation par satellite pourrait être constitutive d'une telle violation. Constitue également une telle collecte illicite, la collecte de données par tromperie, par menace ou de manière dissimulée. Dans le secteur public, une collecte intervenant sans base légale, doit également être considérée comme illicite.

Principe de la bonne foi:

Le deuxième principe énoncé à l'article 4, 2e alinéa prévoit que le traitement des données doit être conforme au principe de la bonne foi. Ce principe définit l'attitude loyale que l'on est en droit d'attendre de toute personne ou organe intervenant dans la vie sociale. Avec le principe de licéité, il constitue un élément de la transparence et de la prévisibilité du traitement de données personnelles permettant aux personnes concernées d'adapter leur comportement. Il en découle en particulier qu'en règle générale la collecte de données doit avoir lieu auprès de la personne concernée ou du moins au su de celle-ci, et qu'elle ne doit en principe pas intervenir contre sa volonté. La transparence du traitement implique en particulier que la personne concernée soit informée des traitements soit directement, soit indirectement notamment par le biais du registre des fichiers. Il serait ainsi souhaitable qu'à l'instar du droit européen, la personne concernée soit, au moment de la collecte, informée de l'identité du responsable du traitement, des finalités du traitement, des catégories de données traitées, des destinataires des données et du caractère obligatoire ou facultatif de la collecte. Dans le secteur public, l'article 18, 1er alinéa, LPD prévoit une obligation d'information lorsque les données personnelles sont collectées systématiquement, notamment au moyen de questionnaires.

Proportionalité:

Le troisième principe est celui de la proportionnalité (art. 4, 2e al. LPD) selon lequel le traitement de données personnelles doit être propre et nécessaire à atteindre le but pour lequel des données doivent être traitées tout en préservant le plus possible les droits des personnes concernées. Le traitement de données personnelles suppose qu'il existe un rapport raisonnable entre le résultat recherché et le moyen utilisé. Ce principe touche au mode de traitement, ainsi qu'à l'étendue et aux catégories de données personnelles utilisées. Seules les données qui sont vraiment nécessaires doivent être collectées.

Finalité:

Le quatrième principe est celui de finalité. Il est énoncé à l'article 4, 3e alinéa de la LPD: «Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances». Ce principe comporte deux volets: l'obligation de déterminer une finalité préalable au traitement et l'obligation d'utiliser les données uniquement

en fonction de cette finalité ou du moins pour une finalité compatible avec la finalité initiale. Egalement élément de la transparence, il permet aux personnes concernées de savoir à quelles fins les données sont collectées et traitées. Cela exclut la collecte illimitée de données pour des finalités ou des applications indéterminées (collecte «en prévision de»). Ainsi, ce principe ne permet pas de communiquer et d'utiliser les données contenues dans un système d'information géographique en matière d'environnement ou d'aménagement du territoire pour des finalités d'assurance ou de marketing ou encore d'utiliser des données d'un SIG «statistique» aux fins de surveillance de l'utilisation de subventions agricoles.

Exactitude des données:
Le cinquième principe est celui de l'exactitude des données énoncée à l'article 5 LPD ou principe de qualité des données. Celui qui traite des données doit s'assurer que celles-ci sont correctes. Le non respect de ce principe peut avoir des conséquences graves pour la personne concernée, suivant le contexte et la finalité pour laquelle les données sont traitées. Par exemple une erreur de codage de l'information dans un SIG utilisé pour repérer les auteurs d'une atteinte à l'environnement pourrait entraîner l'inculpation d'une personne ou entreprise étrangère à l'infraction de pollution. Ce principe n'est cependant pas absolu et il doit être pondéré en fonction de la finalité et des circonstances concrètes du traitement de données personnelles.

Communication de données à l'étranger:
Le sixième principe a trait à la communication de données à l'étranger (art. 6, 1er al. LPD). La communication n'est possible que dans la mesure où elle n'entraîne pas une menace grave pour la personnalité des personnes concernées, notamment du fait que le destinataire des données n'est pas soumis à une protection des données équivalente à celle qui est garantie en Suisse. Ainsi, on devrait s'abstenir de communiquer des données personnelles vers des Etats qui n'ont pas de loi sur la protection des données, sauf si l'équivalence peut être garantie par d'autres dispositions légales, statutaires ou contractuelles.

Sécurité des données:
Le septième principe est celui de la sécurité des données selon lequel les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures techniques et organisationnelles appropriées (art. 7 LPD). La nécessité d'assurer la sécurité des données et des systèmes de traitement de l'information, notamment pour garantir leur confidentialité, leur disponibilité et leur intégrité est indispensable pour rendre effectives les autres exigences de la protection des données et éviter notamment que des personnes non autorisées aient accès aux informations, que les données soient diffusées de manière illicite ou utilisées pour des finalités non autorisées. Cela implique notamment que les systèmes soient conçus pour effectuer uniquement les traitements nécessaires à l'accomplissement des tâches pour lesquelles les données ont été collectées. Les mesures à prendre doivent être différenciées en fonction des finalités du traitement, de la nature des données traitées, de l'étendue du traitement et du risque encouru par les personnes concernées. On tiendra également compte du développement de la technique. Ces mesures touchent notamment le personnel, le matériel, l'accès aux locaux, le logiciel et l'organisation de l'entreprise.
Outre les principes généraux qui régissent l'ensemble des traitements de données personnelles et auxquels, sauf dispositions légales contraires ou existence d'un motif justificatif prépondérant, il ne peut être dérogé, le traitement de données personnelles ne peut intervenir que dans la mesure où certaines conditions préalables sont respectées. La LPD distingue ici entre le secteur privé et le secteur public.

2.2.2 Traitement de données personnelles par des personnes privées

Dans le secteur privé, l'utilisation d'un SIG contenant des données personnelles n'est possible que si le traitement ne porte pas une atteinte illicite à la personnalité des personnes concernées. Aux termes de l'article 13, 1er alinéa LPD, une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la personne concernée, par un intérêt prépondérant privé ou public, ou par la loi. Trois conditions pour que la violation de la loi soit consommée:

- un droit de la personnalité est en cause. Généralement le traitement de données personnelles met en jeu la personnalité des personnes concernées.
- Ensuite, il faut que ce droit de la personnalité soit atteint. Si nous admettons que tout traitement de données personnelles touche la personnalité des personnes concernées, il n'en résulte pas automatiquement et en tous les cas une atteinte. Cela dépendra en particulier de la nature des données traitées, des finalités et des circonstances du traitement, du domaine d'activité ou de l'organisation du système d'information. Ainsi la loi précise qu'en règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement (art. 12, 3e al. LPD). Dans un tel cas, il faut que ce soit la personne concernée elle-même qui rendent ses données accessibles, soit en les diffusant, soit en consentant à leur diffusion par des tiers. Ainsi, tel n'est pas le cas lors de la publication d'un annuaire, téléphonique ou autre, effectuée sans que la personne n'y ait consenti ou n'ait le droit de s'y opposer.
- Enfin, s'il y a atteinte, celle-ci doit être illicite. En principe toute atteinte est illicite sauf si elle est justifiée par le consentement de la personne concernée, par la loi ou par un intérêt public ou privé prépondérant.

La LPD définit, à titre exemplatif, trois cas dans lesquels le traitement de données personnelles porte une atteinte illicite à la personnalité des personnes concernées (art. 12, 2e al. LPD):

- Il s'agit des traitements de données personnelles qui interviennent en violation de l'un des principes fondamentaux définis aux articles 4 et suivants de la loi et que nous avons examinés auparavant;
- Il y a également atteinte illicite lorsque le traitement s'effectue contre la volonté expresse de la personne concernée;
- Il s'agit enfin de la communication à des tiers de données sensibles ou de profils de la personnalité. Par données sensibles (art. 3, let. c, LPD), il faut comprendre: les données personnelles relatives aux opinions ou aux activités religieuses, philosophiques, politiques ou syndicales, les données sur la santé, la sphère intime ou l'appartenance à une race, celles concernant les mesures d'aide sociale, ainsi que les poursuites ou les sanctions administratives. Par profil de la personnalité (art. 3, let. d, LPD), on entend un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique ou qui en donne une image complète.

Dans ces trois cas, l'illicéité de l'atteinte peut être levée si le responsable du traitement parvient à démontrer qu'il est au bénéfice d'un motif justifiant le traitement des données.

La loi énonce trois motifs généraux justifiant une atteinte à la personnalité (art. 13, 1er al. LPD): le consentement de la personne concernée, qui peut être exprès ou tacite, mais qui doit être libre, spécifique, éclairé et révocable, la loi ou l'intérêt public ou privé prépondérant. Selon la jurisprudence du Tribunal fédéral (ATF 97 II 97), seul un intérêt particulièrement important à traiter les données peut l'emporter sur le droit à la vie privée exempte de troubles. Il s'agit en fait de procéder à une pesée des intérêts en présence et d'apprécier de cas en cas si l'intérêt au traitement l'emporte sur l'intérêt de la personne concernée à conserver la maîtrise sur ses données et donc sur sa vie privée. La loi énonce également à titre exemplatif, six situations où, en principe, un intérêt prépondérant de celui qui traite des données entre en considération (art. 13, 2e al. LPD). Cela doit notamment permettre au juge de pondérer les intérêts en présence en cas de conflit. Parmi ces situations, une peut justifier le traitement de données personnelles dans le cadre d'un système d'information géographique par des personnes privées: lorsque ces données sont traitées à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique. Cela implique en particulier que les données personnelles ne sont pas utilisées pour prendre une décision relative à la personne concernée ou pour enrichir ou corriger des fichiers ou des systèmes d'informations dont les données personnelles sont traitées pour des finalités non statistiques. En outre, cela implique également que les données sont diffusées sous une forme qui ne permettent pas d'identifier les personnes concernées.

2.2.3 Traitement de données personnelles par des organes fédéraux

Dans le secteur public fédéral, un système d'information géographique ne peut être créé que s'il repose sur une base légale suffisante (art. 17, 1er alinéa LPD), c'est-à-dire répondant aux exigences de transparence et de prévisibilité des traitements de données personnelles. Par base légale, on entend non seulement une loi au sens formel, c.à.d. une loi fédérale ou un arrêté fédéral de portée générale sujet au référendum, mais aussi toute disposition de nature réglementaire (loi au sens matériel) basée sur une telle loi. Le degré de normativité, à savoir le choix entre une loi au sens formel ou une loi au sens matériel, ainsi que le degré de précision de la base légale dépendent de différents critères. On retiendra en particulier la gravité de l'atteinte, la nature des données traitées, le cercle des personnes concernées, l'organisation et la structure du système d'information, la finalité du traitement, le domaine d'activité ou encore le cercle et l'étendue des personnes concernées. La LPD exige en particulier que le traitement de données personnelles sensibles ou de profils de la personnalité soit en principe expressément prévu dans une loi au sens formel (art. 17, 2e al., LPD). En outre, si les données sont rendues accessibles par procédure d'appel, notamment les destinataires ont un accès en ligne aux informations du SIG (processus du self-service), alors l'accès doit être expressément prévu dans la base légale régissant le SIG (art. 19, 3e al., LPD). Cela implique notamment que les destinataires des données soient définis et que la finalité et l'étendue de l'accès soient précisées.

Dans la mesure où un SIG est utilisé par diverses entités administratives, fédérales et/ou cantonales, voire par des personnes privées, il devrait, à l'instar d'autres systèmes d'informations fédéraux, faire l'objet d'une réglementation spécifique définissant en particulier le but du système et des traitements de données qui en découlent, l'organisation et les compétences (déterminer l'organe responsable et le cas échéant les organes ou personnes participants à la gestion du système), les catégories de données traitées et leur provenance, les droits des utilisateurs du SIG (accès aux données et leur étendue), les communications de données, la conservation des données et les mesures techniques et organisationnelles.

2.2.4 Systèmes d'informations géographiques à des fins statistiques

Les SIG à des fins statistiques et en particulier le GEOSTAT de l'Office fédéral de la statistique peuvent également nécessiter l'utilisation de données personnelles issues d'un recensement de la population ou d'autres relevés statistiques. La loi fédérale sur la protection des données contient une disposition particulière, l'article 22, régissant le traitement de données à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique. Cette disposition vise à faciliter la collecte et le traitement des données pour ce type de finalité. Cela se justifie du fait que l'intérêt public n'est pas contesté et que d'autre part les risques pour la personnalité des personnes concernées sont

en principe moins élevés, car les finalités poursuivies ne se rapportent pas à des personnes et ne visent en particulier pas la prise de décisions ou de mesures relatives à une personne concernée. Les statistiques ne s'intéressent pas à la personne en tant que telle. Elles fournissent des informations synthétiques qualitatives et quantitatives, notamment sous forme de chiffres, de tableaux ou de cartes. Ces informations sont représentatives de l'état d'une population ou d'un phénomène de masse (connaissance de grands ensembles et analyse de phénomènes collectifs).

L'article 22 de la loi fédérale sur la protection des données ne crée pas la base légale des traitements ne se rapportant pas à la personne concernée et notamment pour le GEOSTAT. Celle-ci doit être recherchée dans la législation spécifique. Il allège cependant les exigences de la loi:

- le traitement de données sensibles ou de profils de la personnalité ne nécessite pas une loi au sens formel.
- la collecte et le traitement à des fins statistiques de données qui ont été collectées pour une autre finalité sont autorisés, même si la finalité statistique n'a pas été indiquée lors de la collecte initiale, n'est pas prévue dans la loi ou ne ressort pas des circonstances (fiction de finalité compatible).
- Enfin, les conditions de la communication des données sont assouplies.

Toutefois, ces allégements sont soumis au respect de quatre conditions cumulatives:

- Les données ne doivent être utilisées qu'à des fins ne se rapportant pas à des personnes;
- Les données personnelles doivent être rendues anonymes dès que le but du traitement le permet. Il s'agit ici d'appliquer le principe de proportionnalité. Si cela est d'emblée possible, on renoncera à collecter ou à communiquer des données sous forme nominative;
- Lorsque les données ont été communiquées à un tiers, le destinataire ne peut à son tour les communiquer qu'avec le consentement de l'organe fédéral qui lui les a transmises;
- Enfin, les résultats du traitement sont publiés sous une forme ne permettant pas d'identifier les personnes concernées. Cela implique notamment qu'un accès en ligne ou la communication sous forme informatique de données du GEOSTAT doivent avoir un niveau d'anonymisation et d'agrégation suffisant afin de ne pas permettre l'identification des personnes, notamment en connectant ces informations avec d'autres données.

Les bases légales actuelles du système GEOSTAT sont à rechercher dans la loi fédérale sur la statistique et l'ordonnance concernant l'exécution des relevés statistiques fédéraux. La loi sur la statistique règle en particulier l'organisation de la statistique fédérale, la collecte des données (collecte primaire directe ou indirecte, collecte secondaire ou mobilisation secondaire des données), les obligations des personnes concernées, l'utilisation des données et notamment le respect du secret statistique, ainsi que la conservation, la communication et la publication des données. Concrétisant le respect du principe de finalité énoncé à l'article 4, 3e alinéa de la LPD, l'article 14 de la loi fédérale sur la statistique prévoit que les données collectées à des fins statistiques ne peuvent être utilisées à d'autres fins, sauf si une loi fédérale autorise expressément une autre utilisation ou si la personne concernée y a consenti par écrit. Ainsi, l'utilisation de données de GEOSTAT à des fins non statistiques, c'est-à-dire à des fins se rapportant aux personnes concernées, si elle est envisagée, nécessiterait une autorisation expresse dans une loi au sens formel, sauf à pouvoir obtenir le consentement de toutes les personnes concernées, ce qui paraît illusoire!

Toutefois, une ouverture à des fins non statistiques constituerait une évolution dangereuse risquant d'entraîner une perte de maîtrise sur le flux des informations. Le respect du secret statistique et du principe de finalité qui en découle est un élément central de la protection des données et de la confiance en l'outil statistique. Toute brèche dans ce principe peut remettre en cause l'équilibre entre l'intérêt public à disposer de données statistiques fiables et le respect de la personnalité et des droits et libertés fondamentaux de la personne.

3. Conclusion

Le développement des SIG et la multiplicité des utilisations réelles ou potentielles des SIG tant dans le secteur public que dans le secteur privé doivent tenir compte des exigences d'un Etat de droit dans une société démocratique. Ils doivent en particulier respecter la personnalité et les droits fondamentaux et notamment le droit des individus à l'autodétermination en matière d'informations. Il est dès lors nécessaire d'entourer la mise en place de tels systèmes et leur utilisation d'un environnement légal approprié assurant la protection des données tout en tenant compte des intérêts publics ou privés prépondérants pouvant légitimer le traitement des données personnelles. Les lois générales de protection des données assurent un cadre adéquat dans la mesure où les principes fondamentaux que sont notamment les principes de licéité, de proportionnalité, de finalité, de bonne foi (transparence), d'exactitude et de sécurité des données sont respectés. Il convient néanmoins que tous les acteurs concernés par l'utilisation de SIG examinent la nécessité de compléter l'arsenal juridique par des dispositions sectorielles et par des mesures techniques et organisationnelles spécifiques. Cet examen qui ne peut s'arrêter aux seules frontières nationales et qui nécessite une concertation internationale, notamment au sein du Conseil de l'Europe et de l'Union européenne, ne doit pas absolument déboucher sur l'adoption de nouvelles lois. Ainsi, dans le secteur privé, des mesures d'autoréglementation pourraient utilement compléter les dispositions légales existantes. En particulier, il est important de garantir:

- La transparence des traitements de données personnelles dans un SIG. A cet effet, il faut que les personnes concernées puissent être informées sur les finalités du SIG, les catégories de

données traitées, les utilisateurs du SIG et les destinataires des informations et qu'elles puissent faire valoir leurs droits, notamment par le biais du droit d'accès.

- La ou les finalités du SIG doivent être déterminées et respectées. En particulier si les finalités du SIG ne se rapportent pas aux personnes concernées, notamment dans le cadre de la statistique, il faut en particulier veiller au respect du secret statistique et garantir l'anonymat lors de la publication ou de la diffusion.
- Le catalogue des données traitées doit être établi et seules les données nécessaires au but du SIG doivent être collectées et traitées.
- La qualité des données doit être garantie (exactitude, mise à jour, conservation limitée dans le temps)
- les communications de données et en particulier par procédure d'appel doivent être clairement réglées.
- Ce cadre juridique doit également être accompagné de mesures techniques et organisationnelles. Il conviendrait en particulier d'encourager le développement et le recours à des technologies dites de la vie privée.

Enfin, face aux pressions budgétaires, aux nécessités d'économie et de rationalisation, il convient de ne pas céder aux mesures de facilité allant au détriment du respect de la personnalité et des droits fondamentaux. Les organes publics se doivent en particulier de s'interroger sur leur mission et ne pas se faire les complices de violations de la vie privée en diffusant sans réserve les données qu'ils ont collectées pour une finalité publique déterminée.

Jean-Philippe Walter, dr en droit
Préposé fédéral suppléant à la protection des données
CH-3003 Berne