

LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES RENSEIGNEMENTS PERSONNELS OU SENSIBLES SUR LES CITOYENS : L'APPROCHE DES ORGANISMES STATISTIQUES GOUVERNEMENTAUX

Louise Bourque¹

RÉSUMÉ

Les organismes statistiques gouvernementaux de la plupart des pays au monde ont des pouvoirs de recueillir des informations sur les citoyens en vertu de lois. Ces organismes sont en conséquence de grands cueilleurs d'informations tant auprès des personnes que des entreprises, des institutions, etc. Les informations demandées portent sur des sujets très divers, et parfois sensibles : éducation, santé et bien-être, culture, activité commerciale, industrielle ou financière, travail et emploi, etc. Pour équilibrer les pouvoirs des organismes statistiques, les législateurs ont établi l'obligation juridique de protéger la confidentialité des renseignements détenus par ceux-ci. En conséquence, ces organisations se dotent de politiques, procédures, règles d'éthique, etc., qui visent à assurer la confidentialité et la sécurité des renseignements qu'ils détiennent. La conférence donnera un aperçu général des politiques et règles qui sont en vigueur en matière de confidentialité et sécurité des informations confidentielles détenues par les organismes statistiques gouvernementaux canadien, québécois, et européens.

Mots clés : Confidentialité, collecte, diffusion, encadrement légal, organismes statistiques gouvernementaux, sécurité, traitement.

ABSTRACT

In most countries, government statistical organizations have the legislated right to gather information on their citizens. In consequence, official statistical organizations have become major collectors of data on individuals, businesses, institutions, etc. The information they request concern subject matter that is diverse and often sensitive: education; health and welfare; culture; commercial, industrial or financial activity; work and employment, etc. To counterbalance the powers of statistical organizations, legislators have created laws to protect the confidentiality of this information. In consequence, the statistical organizations are bound by policies, procedures, ethical guidelines, etc., aimed at assuring the confidentiality and security of their data. This talk will give a general overview of the policies and regulations currently in effect to protect the confidentiality and security of data held by Canadian, Quebec and European government statistical organizations.

KEY WORDS: Collection; Confidentiality; Dissemination; Government statistical organizations; Legal framework; Processing; Security

1. CONTEXTE

➤ Les organismes statistiques (OS) et le secret statistique

- La plupart des pays se sont dotés d'entités gouvernementales (OS) qui ont pour mission de produire les statistiques officielles nationales. Elles ont en conséquence des pouvoirs, définis dans le cadre de leurs lois constitutives, de recueillir des informations sur les citoyens, de

les traiter et de les diffuser. Leurs missions sont strictement de nature statistique et non administrative : aucune décision n'y est prise relativement à une personne. On y produit des informations statistiques qui, quoique complètement anonymes, illustrent une facette de la société, une problématique, etc..

- Les OS sont donc de grands récolteurs d'informations auprès des citoyens, qu'il s'agisse de personnes, d'entreprises,

¹ Louise Bourque, directrice de la méthodologie, de la démographie et des enquêtes spéciales, Institut de la statistique du Québec, 200, chemin Sainte-Foy, 3^e étage, Québec (Québec) G1R 5T4.

d'institutions, etc., portant sur des sujets très divers, et parfois sensibles :

- Éducation
- Santé et bien-être
- Culture
- Activités commerciales, industrielles ou financières
- Travail et emploi
- Etc.

- En conséquence, les OS sont dépendants des citoyens pour réaliser leurs missions de produire de l'information essentielle à la gouverne d'une société. Comment alors obtenir cette indispensable participation des citoyens aux activités des OS, dans une société libre et démocratique, qui a à cœur le respect de la vie privée?
- Pour équilibrer les pouvoirs des OS en matière de collecte de renseignements avec le respect de la vie privée, les législateurs ont établi le principe du secret statistique, soit l'obligation juridique pour les OS de protéger la confidentialité des renseignements qu'ils obtiennent et détiennent.
- Ainsi, pour un OS, toute information qu'il détient est confidentielle : les renseignements personnels ainsi que les autres informations, qu'elles soient de nature sensible ou pas.
- De surcroît, les OS doivent être en mesure de démontrer aux citoyens qu'ils prennent toutes les mesures pour respecter le principe du secret statistique, et ainsi réduire au maximum les craintes qu'ils pourraient avoir concernant la sécurité et la confidentialité des renseignements personnels ou sensibles qu'ils fournissent. En conséquence, les OS se dotent de cadres normatifs pour s'assurer de respecter les exigences légales liées au secret statistique

➤ Objectifs de la présentation

La présentation vise à fournir un aperçu général des moyens dont se sont dotés à cet égard plusieurs OS. Les informations véhiculées ici sont issues des pratiques des instituts statistiques du Canada (Statistique Canada), du Québec (Institut de la statistique du Québec) et du Conseil de l'Europe (Recommandations du Conseil de l'Europe concernant la Protection des données à caractère personnel collectées et traitées à des fins statistiques, qui visent plus de 40 pays d'Europe).

- Les pratiques générales des OS seront présentées selon cinq grands thèmes :

- L'encadrement légal;
- L'identification et la justification des besoins de collecte de renseignements;
- La collecte des renseignements;
- Le traitement des renseignements;
- La diffusion des informations statistiques.

2. L'ENCADREMENT LÉGAL

- Comme mentionné précédemment, l'obligation de respecter la confidentialité des renseignements détenus par les OS, est inscrite dans les lois constitutives de ces organisations. Cette obligation repose sur les employés, et non sur les institutions.
- Tous les employés des OS sont assermentés.
- Les personnes qui commettraient une infraction au secret statistique sont passibles de poursuites pénales.
- Donc, du point de vue du citoyen qui est sollicité pour fournir des renseignements, la confidentialité des informations qu'il fournit constitue une garantie légale.

3. L'IDENTIFICATION ET LA JUSTIFICATION DES BESOINS DE COLLECTE DE RENSEIGNEMENTS

- D'une part, l'information statistique objective permet de prendre des décisions éclairées, tant au niveau des gouvernements que des entreprises, associations ou institutions. L'utilité de cette information n'a pas à être démontrée.
- D'autre part, les citoyens sont inondés de demandes de fourniture de renseignements de toutes sortes et provenant d'origines variées : organismes gouvernementaux, para-gouvernementaux, firmes privées de sondage ou de marketing.
- Pour rencontrer leur mandat de production de l'information statistique officielle, les OS se dotent de règles et de mécanismes pour limiter la collecte de renseignements à ce qui est strictement nécessaire et pertinent. Par exemple :
 - Règles :
 - Il y a utilisation des renseignements à des fins statistiques strictement.

- On vise la réduction du fardeau de réponse des citoyens, en maximisant l'utilisation des informations déjà recueillies, en exploitant les fichiers administratifs déjà constitués dans d'autres organisations.
- On limite la collecte de renseignements personnels à ce qui est réellement requis.
- Et on doit justifier les besoins de collecte de renseignements supplémentaires à ce qui est nécessaire et pertinent (le danger du ... « tant qu'à y être »).
- On négocie des accords de partage de données entre OS (Eurostat avec organismes des divers pays européens, Statistique Canada avec les organismes provinciaux).

▪ Mécanismes :

- Les OS se dotent de comités consultatifs formés de spécialistes externes de leurs divers champs d'intervention, pour les conseiller dans les grandes orientations à prendre, les nouveaux domaines à explorer et à mesurer, etc.
- Ils se dotent également de Comités d'éthique pour les conseiller sur les aspects éthiques de la collecte de renseignements sensibles.

➤ Donc, du point de vue du citoyen, chacun des renseignements qui lui est demandé peut être justifié par l'OS qui le recueille.

4. LA COLLECTE DES RENSEIGNEMENTS AUPRÈS DES CITOYENS

- Dans le cadre de la collecte de renseignements, les OS doivent établir un contact avec les citoyens qui soit le plus loyal et le plus sécuritaire possible.
- Le caractère loyal de la collecte de renseignements est assuré par la fourniture aux citoyens d'informations statutaires dont les principales sont les suivantes :
 - La garantie de confidentialité;
 - L'utilisation des renseignements à des fins strictement statistiques;
 - Les buts de l'enquête, ses utilisations, ses utilisateurs, etc.;
 - La source des informations ayant servi à établir le contact, le cas échéant;
 - Le caractère obligatoire ou facultatif de la participation à l'enquête (En vertu des Lois constitutives, les OS ont le pouvoir de rendre obligatoire la participation des

citoyens à leurs enquêtes. Toutefois, ils se dotent de règles strictes pour limiter le recours aux enquêtes obligatoires.);

- L'obtention d'un consentement de la part du citoyen qui soit libre, éclairé, et indubitable². Si la collecte porte sur des données sensibles, le consentement doit de plus être explicite³.
- L'obtention du consentement au partage de l'information avec des tiers, le cas échéant, en fonction des lois et politiques en vigueur.
- L'obtention du consentement en cas de couplages subséquents
- La possibilité de retirer son consentement en tout temps en cours de collecte.

▪ La sécurité des échanges d'information entre les citoyens et les OS doit être garantie. Outre les modes traditionnels de collecte que sont le téléphone et la poste, réputés sécuritaires, les OS utilisent avec circonspection les modes de collecte comportant un transfert électronique des renseignements demandés ou recueillis. Le véhicule usuel qu'est Internet ou le courrier électronique n'est pas utilisé. On se sert plutôt de modes de transmission garantissant le plus haut niveau de sécurité :

- sécurisation de l'échange d'information (encryptage de l'information);
- authentification de l'interlocuteur, au besoin;
- installation de l'interface de saisie dans un site privé, avec accès restreint, au besoin.

➤ Malgré la mise en place de ces mesures de sécurité, des OS constatent une certaine réticence des citoyens face à la collecte électronique des données, parce que ceux-ci ne se sentent pas capables d'évaluer les risques d'interception des renseignements qu'ils transmettent.

➤ Donc, lorsqu'il est contacté par un OS, le citoyen se voit pleinement informé des raisons justifiant la collecte, de ses droits, et des obligations de l'OS, notamment à l'égard du respect de la confidentialité des renseignements qu'il fournira. De plus, l'OS s'assure de la sécurité des échanges d'information avec les citoyens.

-
2. Libre : sans aucune forme de contrainte, d'influence ou de pression, ni directement, ni indirectement.
Éclairé : le citoyen a bien reçu l'information que l'OS doit lui fournir.
Indubitable : sans indication que le citoyen pourrait avoir des hésitations, craintes ou réticences.
 3. Explicite : comportant une forme d'accord formel, par exemple au moyen d'un consentement signé.

5. LE TRAITEMENT DES RENSEIGNEMENTS

Le processus de traitement des renseignements recueillis auprès des citoyens, allant de l'obtention de ceux-ci jusqu'à la constitution d'agrégats statistiques complètement anonymes, s'effectue dans un contexte de confidentialité et de sécurité. Les politiques et procédures à cet égard touchent trois volets : matériel, informationnel, humain.

➤ Volet matériel

- Accès physique aux locaux des OS restreint;
- Interdiction formelle de sortie de renseignements confidentiels de ces locaux;
- Politiques de gestion des documents (circulation restreinte, conservation dans des environnements verrouillés, destruction sécuritaire, etc.).

➤ Volet informationnel

- Réseaux informatiques protégés, passerelles de sécurité empêchant les intrusions externes;
- Sécurité des transactions électroniques (procédures de chiffrement);
- Gestion des accès (accès limité aux seules personnes devant y avoir accès, autorisation d'accès, durée de l'accès limitée, mots de passe, etc.);
- Gestion des renseignements personnels (séparés des autres renseignements recueillis le plus tôt possible, dès que le lien n'est plus nécessaire; destruction dès que plus nécessaire).

➤ Volet humain

- Formation et sensibilisation continues du personnel des OS;
- Développement d'une culture organisationnelle axée fortement sur le respect de la confidentialité et la sécurité.

➤ Ces aspects plus techniques ne sont généralement pas connus des citoyens. Toutefois, s'ils étaient portés à leur connaissance, on peut croire que cela concourrait à augmenter leur confiance en la sécurité et la confidentialité des renseignements qu'ils fournissent aux OS.

6. LA DIFFUSION DES INFORMATIONS STATISTIQUES

Les OS n'utilisent pas les renseignements individuels qu'ils détiennent pour prendre des décisions sur les citoyens; ils s'en servent pour produire et diffuser des

agrégats statistiques complètement anonymes. Ces produits statistiques sont généralement des analyses accompagnées de tableaux de résultats, contenant des moyennes, des proportions, des fréquences, etc. Parfois, et ce dans des contextes bien spécifiques, il peut s'agir de la transmission de fichiers de microdonnées rendu anonymes. Dans ces deux situations, des mesures sont prises pour garantir qu'il n'est pas possible, de façon indirecte, d'identifier un répondant à partir des produits diffusés, et ainsi divulguer de l'information confidentielle.

➤ Tableaux de résultats

- Ce sont déjà des agrégats, donc les renseignements personnels ou les identifiants ne sont pas présents;
- Les OS vérifient tous les tableaux à diffuser et s'assurent, à partir de techniques statistiques de masquage, qu'il n'est pas possible, par déduction, de reconnaître un répondant à l'enquête;
- Les techniques de masquage généralement utilisées dans ce contexte sont l'arrondissement aléatoire, ou la suppression de cellules.

➤ Fichiers de microdonnées

- De plus en plus, les OS s'associent avec des chercheurs externes pour maximiser l'exploitation de leurs produits statistiques. Dans bien des cas, cela requiert l'accès de la part des chercheurs à des fichiers de microdonnées.
- La retransmission de données confidentielles à des tiers, par exemple des chercheurs externes, peut se faire si le répondant en a fourni l'autorisation préalable. Le cas échéant, l'utilisation du fichier par la tierce partie est strictement limitée à des fins statistiques
- La diffusion publique de fichier de microdonnées est possible (notamment pour les chercheurs) mais seulement sous conditions :
 - Les renseignements personnels ou identifiants sont éliminés du fichier.
 - Le fichier a subi un traitement statistique de masquage permettant de s'assurer qu'il n'est pas possible d'identifier un répondant par recoupement de variables.
 - Les techniques de masquage utilisées sont principalement le regroupement de valeurs extrêmes, le regroupement de modalités de réponse, la suppression de données, l'élimination de variables, l'ajout de bruit aléatoire.

Bref, les OS vont au-delà de la simple anonymisation lorsqu'ils retransmettent des produits statistiques. Ils s'assurent qu'il n'est pas possible d'identifier un citoyen, ni directement, ni indirectement par déduction. Ces pratiques ne sont pas très connues des citoyens. Encore là, on peut penser que ceux-ci verraient leurs éventuelles craintes à l'égard de la divulgation de renseignements confidentiels réduites, s'ils étaient au courant de ces pratiques.

7. CONCLUSION

Au cours des années qui vont venir, il faut s'attendre à voir se généraliser mondialement les tensions créées par l'opposition entre :

- Les besoins toujours plus nombreux et détaillés de renseignements sur les personnes, les entreprises, les institutions, etc.
 - Le respect de la vie privée (personnes) et la protection des données stratégiques (entreprises)
- Dans ce contexte, et pour maintenir leur crédibilité, les OS devront poursuivre leurs efforts en vue de consolider la participation des citoyens à la réalisation de leurs missions. Pour ce faire, je suggère trois axes autour desquels les OS devraient déployer leurs efforts en vue de rassurer les citoyens au sujet de la sécurité de leurs renseignements personnels ou confidentiels.

- **Le renforcement des façons de faire** : les OS devraient, de façon continue, mettre à jour et renforcer leur cadre normatif, c'est-à-dire les politiques, procédures, règles d'éthiques, etc., en matière de sécurité et de confidentialité, et s'assurer qu'il est bien appliqué.
- **La transparence à l'égard des façons de faire** : les OS devraient diffuser, faire connaître ce cadre normatif aux citoyens; en effet, au-delà des mesures concrètes de sécurité et de confidentialité qui sont appliquées, il y a la perception qu'ont les citoyens du respect de la confidentialité des informations qu'ils détiennent sur eux. Cette perception des citoyens est aussi importante que les mesures elles-mêmes; une impression négative peut démolir tous les efforts mis en place par une organisation, même parmi les meilleures. De surcroît, on constate une préoccupation de plus en plus marquée des médias pour les questions de respect de la vie privée, de là la nécessité pour les OS de publiciser leurs politiques et procédures.
- **L'amélioration continue des façons de faire** : les OS devraient, de façon continue, se tenir informés des plus récents développements scientifiques en matière de confidentialité statistique et de sécurité technologique et investir dans la recherche en ces matières.

