REPUBLIQUE ET CANTON DE GENEVE
Préposé cantonal à la protection des données et à la transparence

Projet de loi d'application de la loi fédérale sur les jeux d'argent

Avis du 3 janvier 2020

Mots clés : veille réglementaire, collecte de données personnelles sensibles, base légale formelle

Contexte : Le 17 décembre 2019, le Département de la cohésion sociale (DCS) a sollicité un avis du Préposé cantonal à la protection des données et à la transparence (PPDT) au sujet du projet de loi d'application de la loi fédérale sur les jeux d'argent, plus particulièrement concernant l'art. 22 du projet. Cette disposition habilite les autorités compétentes à traiter des données personnelles, y compris des données personnelles sensibles.

Bases juridiques : art. 56 al. 3 litt. e LIPAD; art. 23 al. 8 RIPAD

1. Caractéristiques de la demande

La loi fédérale sur les jeux d'argent du 29 septembre 2017 (LJAr; RS 935.51) réserve aux cantons des compétences résiduelles en matière de jeux de grande envergure (art. 28 LJAr), ainsi qu'en matière de jeux de petite envergure (art. 41 LJAr). La loi fédérale et l'ordonnance du 7 novembre 2018 (OJAr; RS 935.511) fixent un certain nombre d'exigences dans ces domaines, mais l'article 41 LJAr permet aux cantons de "*prévoir des dispositions relatives aux jeux de petite envergure allant plus loin que celles du présent chapitre ou interdire certains jeux de petite envergure*". Selon l'exposé des motifs joint au projet de loi, "*dans le souci d'assurer une meilleure protection de la population contre les risques liés au jeu excessif, tout en permettant l'exploitation légale de ces jeux sans entrave abusive, le Conseil d'Etat genevois a choisi d'exploiter cette marge de manœuvre. C'est là l'objet du présent projet de loi*".

Les dispositions du projet de loi d'application de la loi fédérale sur les jeux d'argent soumis pour avis au Préposé cantonal et qui ont trait à la protection des données personnelles sont les suivantes:

Art. 2 Compétences

[2] Les autorités participant à l'application de la présente loi et de ses dispositions d'exécution collaborent entre elles. Elles se transmettent mutuellement les renseignements et documents en tant que cela est nécessaire à l'accomplissement de leurs tâches.

Art. 22 Données personnelles

[1] Pour l'accomplissement de leurs tâches légales, les autorités compétentes sont habilitées à traiter les données personnelles, y compris les données sensibles, recueillies dans le cadre de l'examen des demandes d'autorisation et des comptes ou des tâches de surveillance visées aux articles 16 et suivants de la présente loi.

[2] Les données traitées dans le cadre de la surveillance sont conservées pendant 10 ans au maximum après la fin de l'événement auquel la récolte de données est liée.

[3] Lorsqu'une procédure est engagée avant la fin du délai prévu à l'al. 1, le délai court dès la fin de la procédure.

L'exposé des motifs précise ce qui suit, s'agissant de cette dernière disposition:

"Il s'agit ici simplement de disposer d'une base légale formelle permettant de traiter les données nécessaires à la bonne application de la loi. Pour l'autorité de surveillance, ces données comprendront notamment celles obtenues dans le cadre de l'examen des requêtes en autorisation, de l'activité de contrôle et du prononcé des sanctions. Ces dispositions s'inspirent de l'article 110 LJAr, et les délais de destruction des données de l'article 98 OJAr".

2. Les dispositions fédérales pertinentes

La LJAr détermine les critères à prendre en considération lors de l'octroi d'autorisation d'exploitation de jeux de petite envergure, autorisation qui relève de la compétence de l'autorité cantonale de surveillance et d'exécution. Les dispositions particulièrement pertinentes sont les suivantes:

Art. 33 Conditions générales

[1] L'autorisation d'exploitation d'un jeu de petite envergure peut être délivrée si:

a. l'exploitant:

1. est une personne morale de droit suisse,

2. jouit d'une bonne réputation,

3. garantit une gestion et une exploitation des jeux transparentes et irréprochables;

b. le jeu est conçu de façon à pouvoir être exploité de manière sûre et transparente et à présenter un risque faible de jeu excessif, de criminalité et de blanchiment d'argent.

Art. 40 Surveillance

[1] L'autorité cantonale qui autorise et surveille les jeux de petite envergure contrôle le respect des dispositions légales relatives à ces jeux.

[2] Elle peut notamment:

a. exiger de l'exploitant les renseignements et documents nécessaires et effectuer des contrôles;

b. prendre des mesures provisionnelles pendant la durée de l'enquête;

c. en cas de violation de la présente loi ou d'irrégularité, ordonner les mesures nécessaires au rétablissement de l'ordre légal ou à la suppression de l'irrégularité.

Art. 41 Droit cantonal

[1] Les cantons peuvent prévoir des dispositions relatives aux jeux de petite envergure allant plus loin que celles du présent chapitre ou interdire certains jeux de petite envergure.

[2] Les art. 32, 33, 34, al. 3 à 7, et 37 à 40 ne s'appliquent pas aux petites loteries organisées à l'occasion d'une réunion récréative, avec des lots uniquement en nature, lorsque l'émission, le tirage des billets et la distribution des lots sont en corrélation directe avec la réunion récréative et que la somme totale maximale des mises est peu élevée.

[3] Le Conseil fédéral définit la somme maximale.

La LJAr prévoit l'instauration d'une autorité intercantonale de surveillance et d'exécution pour les cantons ayant autorisé les jeux de grande envergure. S'agissant du traitement de données personnelles par cette autorité, la LJAr prévoit, à son art. 110:

Pour l'accomplissement de ses tâches légales, l'autorité intercantonale peut traiter des données personnelles, y compris les données sensibles relatives à la santé, aux mesures d'aide sociale, aux poursuites ou sanctions pénales et administratives, ainsi que des profils de la personnalité.

3. Les règles de protection des données personnelles à Genève

La loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001 (LIPAD; RSGE A 2 08) a fait l'objet d'une révision importante en 2008, par laquelle la protection des données personnelles a été ajoutée au champ d'application matériel de la loi en sus de son volet relatif à la transparence.

Depuis le 1er janvier 2010, date de l'entrée en vigueur de cette modification législative, un autre objectif figure désormais dans le texte légal à son art. 1 al. 2 litt. b : *"protéger les droits fondamentaux des personnes physiques ou morales de droit privé quant aux données personnelles les concernant"*.

Par donnée personnelle, il faut comprendre *"toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable"* (art. 4 litt. a LIPAD). Tant que les données n'ont pas été rendues anonymes, l'on se trouve bien face à des questions relatives à la protection de données personnelles.

Les données personnelles sensibles comprennent les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles; la santé, la sphère intime ou l'appartenance ethnique; des mesures d'aide sociale; des poursuites ou sanctions pénales ou administratives (art. 4 litt. b LIPAD).

La LIPAD énonce un certain nombre de principes généraux régissant la collecte et le traitement des données personnelles (art. 35 à 40 LIPAD).

- Base légale (art. 35 al. 1 et 2 LIPAD)

  Le traitement de données personnelles ne peut se faire que si l'accomplissement des tâches légales de l'institution publique le rend nécessaire. En outre, la loi stipule que lorsqu'il s'agit de traiter de données personnelles sensibles ou de profils de la personnalité, la tâche considérée doit soit être définie clairement par la loi, soit être absolument indispensable à l'accomplissement de la tâche en cause soit encore être nécessaire et, si c'est le cas, intervenir avec le consentement – libre et éclairé – de la personne concernée.

- Bonne foi (art. 38 LIPAD)

  Il n'est pas permis de collecter des données personnelles sans que la personne concernée en ait connaissance, ni contre son gré. Quiconque trompe la personne concernée lors de la collecte des données – par exemple en collectant les données sous une fausse identité ou en donnant de fausses indications sur le but du traitement – viole le principe de la bonne foi. Il agit également contrairement à ce principe s'il collecte des données personnelles de manière cachée.

- Proportionnalité (art. 36 LIPAD)

  En vertu du principe de la proportionnalité, seules les données qui sont nécessaires et qui sont aptes à atteindre l'objectif fixé peuvent être traitées. Il convient donc toujours de peser les intérêts en jeu entre le but du traitement et l'atteinte à la vie privée de la personne concernée en se demandant s'il n'existe pas un moyen moins invasif permettant d'atteindre l'objectif poursuivi.

- Finalité (art. 35 al. 1 LIPAD)

  Conformément au principe de finalité, les données collectées ne peuvent être traitées que pour atteindre un but légitime qui a été communiqué lors de leur collecte, qui découle des circonstances ou qui est prévu par la loi. Les données collectées n'ont ensuite pas à être utilisées à d'autres fins, par exemple commerciales.

- Reconnaissabilité de la collecte (art. 38 LIPAD)

La collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée. Cette exigence de reconnaissabilité constitue une concrétisation du principe de la bonne foi et augmente la transparence d'un traitement de données. Cette disposition implique que, selon le cours ordinaire des choses, la personne concernée doit pouvoir percevoir que des données la concernant sont ou vont éventuellement être collectées (principe de prévisibilité). Elle doit pouvoir connaître ou identifier la ou les finalités du traitement, soit que celles-ci lui sont indiquées à la collecte ou qu'elles découlent des circonstances.

- Exactitude (art. 36 LIPAD)

  Quiconque traite des données personnelles doit s'assurer de l'exactitude de ces dernières. Ce terme signifie également que les données doivent être complètes et aussi actuelles que les circonstances le permettent. La personne concernée peut demander la rectification de données inexactes.

- Sécurité des données (art. 37 LIPAD)

  Le principe de sécurité exige non seulement que les données personnelles soient protégées contre tout traitement illicite et tenues confidentielles, mais également que l'institution en charge de leur traitement s'assure que les données personnelles ne soient pas perdues ou détruites par erreur.

- Destruction des données (art. 40 LIPAD)

  Les institutions publiques détruisent ou rendent anonymes les données personnelles dont elles n'ont plus besoin pour accomplir leurs tâches légales, dans la mesure où ces données ne doivent pas être conservées en vertu d'une autre loi.

Finalement, l'art. 39 LIPAD traite de la communication des données, en fonction du destinataire. S'agissant de la communication de données entre institutions publiques soumises à la LIPAD, l'art. 39 al. 1 à 3 prévoit :

[1] Sans préjudice, le cas échéant, de son devoir de renseigner les instances hiérarchiques supérieures dont elle dépend, une institution publique ne peut communiquer des données personnelles en son sein ou à une autre institution publique que si, cumulativement :

a) l'institution requérante démontre que le traitement qu'elle entend faire des données sollicitées satisfait aux exigences prévues aux articles 35 à 38;

b) la communication des données considérées n'est pas contraire à une loi ou un règlement.

[2] L'organe requis est tenu de s'assurer du respect des conditions posées à l'alinéa 1 et, une fois la communication effectuée, d'en informer le responsable sous la surveillance duquel il est placé, à moins que le droit de procéder à cette communication ne résulte déjà explicitement d'une loi ou d'un règlement.

[3] Les institutions publiques communiquent aux autorités judiciaires les données personnelles que celles-ci sollicitent aux fins de trancher les causes dont elles sont saisies ou de remplir les tâches de surveillance dont elles sont investies, sauf si le secret de fonction ou un autre secret protégé par la loi s'y oppose.

Cette disposition est complétée par l'art. 14 RIPAD qui dispose à son al. 2 :

[2] La démonstration du respect des conditions posées à l'article 39, alinéa 1, lettres a et b, peut s'effectuer de manière simplifiée en indiquant cumulativement :

a) le contexte légal ou réglementaire dans lequel s'inscrit la mission de l'institution requérante, y compris l'existence d'éventuelles règles spéciales ou la mention de leur défaut;

b) le fait que le fichier destiné à recevoir les données personnelles figure ou non dans le catalogue institué par l'article 43 de la loi, avec son numéro de référence;

c) la finalité de la transmission souhaitée.

4. Appréciation

L'art. 2 du projet prévoit l'assistance administrative entre les autorités participant à l'application de la loi: les renseignements et documents sont mutuellement transmis en tant que cela est nécessaire à l'accomplissement de leurs tâches. Les Préposés saluent la présence d'une base légale formelle à l'assistance administrative. La disposition prévue est conforme aux conditions posées par l'art. 39 al. 1 à 3 LIPAD.

L'art. 22 du projet a trait spécifiquement au traitement de données personnelles, et constitue plus particulièrement une base légale formelle pour le traitement de données personnelles sensibles. Il convient de saluer la présence de cette disposition dans le projet de loi présentement soumis, car elle remplit l'exigence posée par l'art. 35 al. 2 LIPAD. L'art. 22 al. 1 vise les données recueillies dans le cadre de l'examen des demandes d'autorisation et des comptes ou des tâches de surveillance. Ainsi, la finalité pour laquelle les données sont recueillies figure dans le texte légal; par contre, tel n'est pas le cas du type de données sensibles qui pourraient être traitées (condamnations pénales ou administratives, par exemple). Une précision à cet égard permettrait de garantir, au niveau légal déjà, la bonne application du principe de la proportionnalité.

L'al. 2 prévoit expressément la durée de conservation des données, ce qui est à saluer. En effet, en termes de sécurité du droit, une telle précision est souhaitable. Une durée de 10 ans après la fin de l'événement auquel la récolte de données est liée ne semble pas excessive et correspond au délai de conservation prévu par le droit fédéral, s'agissant des données collectées par la commission fédérale des maisons de jeu (CFMJ). L'al. 3 prévoit que ce délai peut être prolongé en cas de procédure, ce qui crée un nouveau dies a quo (à cet égard, l'al. 3 se réfère au délai de l'alinéa 1, alors qu'il semble qu'il devrait se référer au délai de l'alinéa 2).

* * * * * *

Les Préposés remercient le DCS de les avoir consultés et se tiennent à disposition pour tout renseignement complémentaire.

Joséphine Boillat
Préposée adjointe

Stéphane Werly
Préposé cantonal