Une nouvelle loi adaptée aux défis de l'ère numérique

Florence Henguely, le 4 septembre 2023

La suppléante du Préposé fédéral à la protection des données et à la transparence (PFPDT) revient sur l'entrée en vigueur de la nouvelle Loi fédérale sur la protection des données.

Introduction

Le 1er juillet 1993 entrait en vigueur la première Loi fédérale du 19 juin 1992 sur la protection des données. Dans son message du 23 mars 1988, le Conseil fédéral justifiait déjà la nécessité de légiférer par « l'avènement de l'informatique et des technologies des télécommunications, la multiplication des traitements de données, et la diffusion d'informations personnelles toujours plus nombreuses au sein de la société, de l'économie et de l'État ». Trente ans plus tard, notre vie quotidienne se déroule dans une réalité numérique que le législateur de l'époque ne pouvait pas prévoir. Néanmoins, les principes du traitement des données personnelles alors codifiés par le législateur se sont révélés stables. La nouvelle Loi fédérale du 25 septembre 2020 sur la protection des données (LPD), qui est entrée en vigueur le 1er septembre 2023, s'aligne sur les mêmes principes : dans le nouveau droit, la transparence, la proportionnalité et la finalité constituent encore les piliers du traitement des données personnelles.

Notre quotidien a bien changé depuis, au rythme d'Internet et des smartphones. La connexion permanente à Internet, qui permet à la société numérique d'aujourd'hui d'effectuer « en ligne » les tâches du quotidien – des opérations bancaires aux rencontres – a décuplé le volume et l'intensité du traitement des informations personnelles. Néanmoins, la mission de l'autorité fédérale indépendante de surveillance en matière de protection des données, qui consiste à placer la protection de la personnalité et des droits fondamentaux au-dessus de ce qui est technologiquement possible, est plus que jamais d'actualité.

La loi révisée instaure des nouveautés non seulement pour les personnes traitant des données et pour les personnes concernées, mais aussi pour le PFPDT, dont elle étend les tâches et les pouvoirs.

Nouveautés institutionnelles

Le chef du PFPDT, donc le Préposé, sera à l'avenir élu par le Parlement. Jusqu'ici, il était nommé par le Conseil fédéral et sa nomination était soumise à l'approbation de l'Assemblée fédérale. Cette nouvelle règle renforce l'indépendance de l'office par rapport à l'exécutif et sa légitimité démocratique. Le Préposé engagera lui-même son personnel et disposera de son propre budget, qui sera transmis tel quel à l'Assemblée fédérale.

Par ailleurs, ce sera désormais au Conseil fédéral de déterminer si la législation d'un État tiers garantit un niveau de protection adéquat pour permettre le transfert de données de Suisse vers l'étranger sans mesures de précaution supplémentaires. La liste des États concernés figure en annexe de la nouvelle Ordonnance du 31 août 2022 sur la protection des données (OPDo).

- *Les émoluments*

L'art. 59 LPD liste les prestations pour lesquelles le PFPDT percevra des émoluments auprès des personnes privées. Ce sera par exemple le cas des prises de position concernant les codes de conduite ou les analyses d'impact relatives à la protection des données, de l'approbation des clauses type de protection des données et de celle des règles d'entreprise contraignantes. Les conseils généraux que le PFPDT fournira à des personnes privées seront eux aussi soumis à des émoluments.

- *Les enquêtes*

La LPD prévoit que le PFPDT ouvre une enquête si des indices suffisants font penser qu'un traitement de données pourrait être contraire à des prescriptions de protection des données (art. 49 al. 1 LPD). L'enquête est une procédure administrative formelle. Elle sert à la collecte et à l'établissement des faits juridiquement pertinents et permet de vérifier, du point de vue juridique, si les faits constatés violent des prescriptions de protection des données. Si l'enquête révèle que des prescriptions de protection des données sont violées, le PFPDT peut ordonner des mesures administratives, aux conditions prévues par l'art. 51 LPD.

L'enquête peut être ouverte d'office ou sur dénonciation. Les premiers indices d'une éventuelle violation des prescriptions peuvent avoir été perçus par le PFPDT dans le cadre de ses tâches légales de surveillance ou de conseil ou se fonder, en tout ou partie, sur des faits décrits par les personnes concernées ou des tiers (par ex. médias ou organisations de consommateurs).

Idéalement, la dénonciation est adressée au PFPDT au moyen du formulaire en ligne dispo-

nible sur son site, mais elle peut en principe être faite sous n'importe quelle forme. Aucun délai n'est imparti à la dénonciation. Toutefois, les faits dénoncés devraient être relativement actuels, afin que le PFPDT puisse, dans le cas d'une violation des prescriptions de protection des données, ordonner en temps utile les mesures administratives appropriées visées à l'art. 51 LPD.

Le PFPDT a rédigé un document complet s'agissant des enquêtes du PFPDT sur les violations des règles de protection des données, ainsi qu'un aide-mémoire qui donne un aperçu de l'instrument de l'enquête. Les documents en question sont accessibles à cette adresse.

- *Le droit pénal*

Contrairement aux autorités de surveillance de l'UE, le PFPDT restera privé de tout pouvoir de sanction. Les dispositions de droit pénal accessoire de la LPD ont par contre été étoffées dans la LPD (art. 60 ss LPD). Sont désormais punissables la violation intentionnelle des obligations d'informer, de renseigner et de collaborer et la violation intentionnelle des devoirs de diligence, notamment lors de la communication de données personnelles à l'étranger, d'une sous-traitance et de la fourniture de la sécurité des données. Les amendes pénales sont plafonnées à CHF 250'000 et infligées à la personne privée responsable du traitement. L'amende subsidiaire prévue pour les personnes morales est quant à elle plafonnée à CHF 50'000.

Le PFPDT a rédigé une page complète contenant des informations spécifiques s'agissant des dispositions pénales de la LPD. La page est accessible à cette adresse.

Responsabiliser plutôt que sanctionner

La principale valeur ajoutée de la nouvelle LPD réside dans les instruments qui obligent les acteurs traitant les données – dans le domaine de l'économie autant qu'au sein de l'administration fédérale – à analyser et documenter à temps les effets des systèmes numériques sur la sphère privée et sur l'autodétermination des personnes concernées. Ces instruments mettent l'accent sur l'action préventive et sur la responsabilisation des acteurs traitant les données :

- *Le devoir d'informer*

Afin d'atteindre l'objectif de transparence visé par la révision, l'art. 19 LPD consolide le devoir d'informer pour les entreprises. Pour toute collecte envisagée de données person-

nelles, le responsable du traitement privé devra informer au préalable la personne concernée de manière adéquate, que la collecte de données soit directement effectuée auprès d'elle ou non. L'ancienne LPD ne prévoyait ce devoir d'informer que pour les données personnelles sensibles et les profils de la personnalité.

Concrètement, l'identité et les coordonnées du responsable du traitement devront être communiquées, de même que la finalité du traitement et, le cas échéant, les destinataires ou les catégories de destinataires des données personnelles. Autrement que dans le RGPD, des informations devront aussi être fournies sur l'État destinataire et sur les garanties éventuelles d'un niveau approprié de protection des données. Les entreprises doivent ainsi vérifier et actualiser leur déclaration relative à la protection des données.

Si le traitement entraîne une décision individuelle automatisée, le responsable du traitement, en vertu de l'art. 21, devra informer la personne concernée et lui accorder le droit d'être entendu et celui de vérifier qui lui reviennent.

- *Le droit d'accès de la personne concernée*

Le droit d'une personne concernée de demander si des données personnelles la concernant sont traitées est consolidé dans la nouvelle LPD. L'art. 25 dresse une liste étendue des informations que le responsable du traitement devra au moins transmettre (par ex. la durée de conservation des données personnelles traitées). Il prévoit également que la personne concernée devra recevoir toutes les informations nécessaires pour qu'elle puisse faire valoir les droits qui lui sont accordés selon la nouvelle LPD et pour que la transparence du traitement soit garantie.

Le PFPDT met à disposition un formulaire type pour les demandes de droit d'accès. Le formulaire est disponible à cette adresse.

- *Les conseillers et conseillères à la protection des données*

En vertu de l'art. 10 LPD, une entreprise privée peut désigner un conseiller à la protection des données, lequel peut, mais ne doit pas, être lié à elle par un contrat de travail. Dans les deux cas, l'activité de conseil sera séparée des autres tâches de l'entreprise. Il est aussi recommandé de ne pas mélanger les dossiers du conseil sur la protection des données avec ceux des autres activités de conseil et de représentation juridique. Les conseillers doivent par ailleurs pouvoir porter leur point de vue à la connaissance de la direction de l'entreprise en cas de divergence d'opinion. Au contraire du RGPD, la désignation d'un conseiller reste facul-

tative pour les personnes privées. Seuls les organes fédéraux en sont légalement tenus de nommer un conseiller.

Le conseiller est non seulement l'interlocuteur à l'interne en matière de protection des données, mais aussi l'intermédiaire avec la protection des données administrative et le premier contact du PFPDT. Outre le conseil général et la formation de l'entreprise en matière de protection des données, il a pour tâche de participer à l'élaboration et à l'application de conditions d'utilisation et de dispositions de protection des données. Si le conseiller interne exerce sa fonction de manière indépendante et sans recevoir d'instruction et s'il n'exerce pas de tâches incompatibles avec sa fonction, l'entreprise pourra, après avoir effectué une analyse d'impact relative à la protection des données, se fonder uniquement sur le conseil interne même si un risque élevé persiste, sans avoir à consulter le PFPDT.

- *L'analyse d'impact relative à la protection des données (AIPD)*

Les analyses d'impact ne sont pas nouvelles dans le droit suisse sur la protection des données, et les organes fédéraux y sont déjà tenus. Si le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, la LPD prévoit que le responsable du traitement privé devra désormais également procéder au préalable à une AIPD (art. 22 LPD).

L'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque existe surtout lorsqu'un profilage à risque élevé ou un traitement à grande échelle de données sensibles est prévu.
Lorsqu'un système, un produit ou un service est certifié au sens de la LPD ou lorsqu'un code de conduite reposant sur une analyse d'impact est observé, il sera possible de renoncer à une telle analyse.

S'il ressort d'une AIPD que le traitement envisagé présente encore, malgré les mesures prévues par le responsable du traitement, un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement doit consulter le PFPDT préalablement au traitement. Au cas où le PFPDT aurait des objections concernant l'AIPD elle-même, il suggérera au responsable du traitement des précisions ou des ajouts. Ce devrait surtout être le cas lorsque le texte est si général qu'il ne décrit qu'insuffisamment les risques prévisibles ou les mesures. Si les objections concernent le traitement envisagé en soi, le PFPDT proposera des mesures de modification appropriées au responsable du traitement.

Contrairement aux codes de conduite, les prises de position du PFPDT ne devront pas être publiées. En leur qualité de documents officiels toutefois, elles seront soumises à LTrans. Le responsable du traitement privé peut renoncer à consulter le PFPDT s'il a consulté à l'interne son conseiller à la protection des données.

Le PFPDT met à disposition une page spécifique, ainsi qu'un aide-mémoire, s'agissant des AIPD. Les documents sont disponibles à cette adresse.

- *Le devoir d'annoncer les violations de la sécurité des données*

En vertu de l'art. 24 LPD, le responsable du traitement devra nouvellement annoncer au PFPDT les cas de violation de la sécurité des données entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Cette disposition s'applique aussi bien aux responsables du traitement privés qu'aux organes fédéraux. L'annonce au PFPDT doit être faite dans les meilleurs délais. Le responsable du traitement effectuera au préalable une prévision des conséquences possibles de la violation ainsi qu'une première évaluation afin de déterminer s'il pourrait y avoir péril en la demeure, si la personne concernée doit être informée de l'événement et de quelle manière.

Trois portails de notification en ligne

En prévision de l'entrée en vigueur de la LPD, le PFPDT a mis en place trois portails de notification :

1. DataReg : Ce portail permet aux organes fédéraux de déclarer le registre de leurs activités de traitement selon l' 12 LPD. Il remplace l'ancien système de déclaration des fichiers du secteur privé et des autorités WebDataReg qui a été désactivé le 1er septembre 2023. En effet, la LPD dispense désormais le secteur privé de déclarer ses fichiers.
2. Le portail de déclaration des conseillers à la protection des données : La LPD permet aux entreprises de pratiquer l'autorégulation. L'entreprise qui nomme un conseiller ou une conseillère à la protection des données et qui communique cette nomination au PFPDT bénéficie de facilités en matière d'AIPD. Le conseiller à la protection des données est chargé de surveiller le respect par l'entreprise des prescriptions en matière de protection des données et de la conseiller dans ce domaine. Ce portail sert à transmettre au PFPDT les coordonnées des conseillères et des conseillers nommés par les entreprises.
3. DataBreach : Le portail d'annonce des violations de la sécurité des données au sens de

l' 24 LPD met à la disposition des responsables du traitement un canal numérique sûr pour déclarer les cas de violation entraînant un risque élevé pour la personne concernée. Le formulaire en ligne aidera le responsable du traitement à effectuer la saisie structurée et complète des données requises, garantira le traitement efficace des déclarations par le Préposé et simplifiera les analyses statistiques.

La loi sur la protection des données ne vise pas à protéger les données, mais la personnalité humaine. Dans notre monde en pleine mutation numérique où la traçabilité et la transparence du traitement de données se réduisent comme peau de chagrin, la nouvelle LPD permet de protéger le droit à une vie privée et autonome de manière efficace et conforme à l'État de droit.

Proposition de citation : Florence HENGUELY, Une nouvelle loi adaptée aux défis de l'ère numérique, 4 septembre 2023 *in* www.swissprivacy.law/249

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.