Introduction et cadre légal

M231 — Appliquer la protection et la sécurité des données

Jérôme Frosssard

EPAI

2 décembre 2023

Plan

Plan

Qu’est-ce que la protection des données ?

La protection des données fait référence aux pratiques et politiques visant à assurer le respect de la **personnalité** et des **droits fondamentaux**, de la **vie privée**, et du **consentement** des personnes concernées, lors du **traitement** de **données personnelles**.

Elle implique la mise en œuvre et l’application de :

- **Normes juridiques** : sur le plan national (LPD) et supranational (RGPD)
- **Mesures organisationnelles** : procédures, bonnes pratiques, formation, etc.
- **Mesures techniques** : contrôle d’accès, chiffrement, sauvegardes, etc.

Une **violation de la sécurité des données** peut avoir des conséquences graves pour le **responsable du traitement** qui s’expose notamment à de lourdes amendes ; plus encore pour les **personnes concernées** qui pourraient voir leurs conditions matérielles d’existences dégradées ou même, dans des cas extrêmes, leur vie mise en danger.

L'argument « Rien à cacher »

Une grande partie des « géants du Web » et, pour des raisons différentes, de la droite conservatrice ne sont pas favorables aux règlementations sur la protection des données.

Voilà, par exemple, ce que déclarait Eric Schmidt en 2009 alors qu'il était PDG de Google :

> ***« Je pense qu'il faut faire preuve de jugeote. S'il y a quelque chose que vous faites et que personne ne doit savoir, peut-être qu'il faudrait ne pas le faire en premier lieu. Si vous avez besoin qu'on respecte à ce point votre vie privée, le fait est que les moteurs de recherche — y compris Google — enregistrent et conservent des informations pendant un certain temps. Il faut bien se rendre compte que nous, aux États-Unis, sommes soumis au Patriot Act et donc qu'il est possible que toutes ces informations soient mises à la disposition des autorités à leur demande. »***

L’argument « Rien à cacher » — Activité

Que pensez-vous de la déclaration d’Eric Schmidt ?

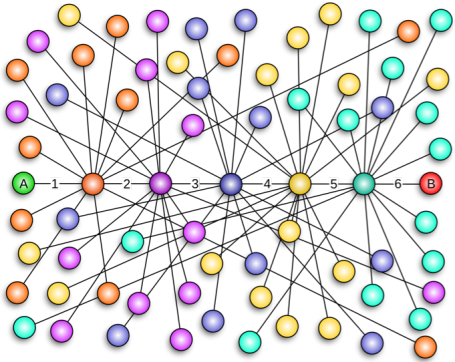
- Réfléchissez à la question et formulez quatre contre-arguments.
- D’abord individuellement pendant 5 min, puis 15 min en groupe.

Six degrés de séparation

La théorie des « six degrés de séparation », proposée en 1929 par le Hongrois Frigyes Karinthy, dit que n'importe quelle personne est reliée à n'importe quelle autre sur la planète par une chaîne de relations individuelles de six maillons, au plus.

Si une personne est placée sous surveillance, ce n'est pas seulement cette personne qui est surveillée, mais également des personnes qui se trouvent à un, ou même deux degrés de séparation.

Cela peut faire beaucoup de monde.

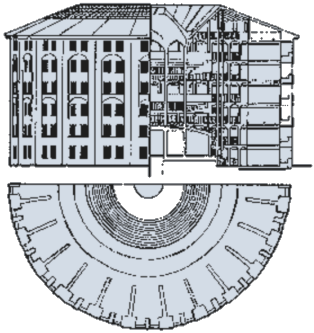


Panoptisme

Le panoptique est un modèle de prison imaginé par Jeremy Bentham au XVIIIe siècle. Ce modèle repose sur une tour de surveillance centrale où un unique gardien peut observer les détenus logés dans des cellules disposées tout autour. Comme les prisonniers ne peuvent pas savoir s'ils sont observés ou non, ils se conduisent comme s'ils l'étaient en permanence.

Appliqué à l'ensemble de la société, le panoptisme devient un moyen de contrôle. Michel Foucault développe cette idée dans son ouvrage « Surveiller et punir ».

Deleuze la résume ainsi : « la formule abstraite du panoptisme n'est plus "voir sans être vu", mais "imposer une conduite quelconque à une multiplicité humaine quelconque". »



Sphère privée

La notion de **sphère privée** ou de **vie privée** a beaucoup évolué au fil des siècles. Aujourd'hui, elle est principalement liée à celles d'intimité et de vie familiale.

La sphère privée comprends notamment :

- l'intimité : identité sexuelle, état de santé, opinions politiques et religieuses, appartenance ethnique, relations sexuelles et amoureuses, mœurs, relations personnelles, sociales, appartenance syndicale, vie professionnelle
- la vie familiale et le domicile
- les loisirs
- les circonstances de la mort
- le droit à l'image
- la correspondance privée
- l'honneur et à la réputation

Protectioin de la sphère privée

La protecton de la sphère privée doit donc assurer :

- Le **droit au secret** : un individu à le droit de choisir à qui il communique des informations personnelles.
- Le **droit à l'image** : un individu doit consentir à toute utilisation de son image.

Cette protection par la loi est exigée par la Déclaration universelle des droit de l'homme, dont l'article 12 dit :

> « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

La protection de la vie privée est d'autant plus importante que les personnes concernées sont vulnérables, appartenant à des groupes stigmatisés ou marginalisés. Si l'on n'a rien à cacher, ce n'est peut-être pas le cas d'un·e ami·e, d'un·e camarade, ou d'un·e collègue.

Plan

Principaux textes de loi

En matière de protection des données, deux textes législatifs majeurs établissent le cadre juridique :

- La **loi fédérale sur la protection des données ou LPD**[1] du droit national suisse.
- Le **règlement**[2] **général sur la protection des données ou RGPD** du droit de l'Union européenne.

La Suisse n'est membre de l'Union européenne, mais le RGPD s'applique à toutes les entreprises et organisations qui traitent des données personnelles des résidents de l'UE, indépendamment de leur emplacement.

Remarques :

1. La LPD est entrée en vigueur très récemment, le 1er septembre 2023, c'est pourquoi elle a parfois encore appelé « nouvelle loi sur la protection des données » ou nLPD.
2. Dans le droit européen, les règlements sont des actes contraignants comme le sont les lois dans le droit national.

Traité n°108

Un autre texte essentiel dans le cadre de la protection des données est la **Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108)**, ratifié par la Suisse en 1997.

Ce texte de 1981 est un traité du Conseil de l'Europe qui constitue le « premier instrument international contraignant » ayant pour « objet de protéger les personnes contre l'usage abusif du traitement automatisé des données »

Dans le résumé du texte, on peut lire :

> *« Outre des garanties prévues en ce qui concerne le traitement automatisé des données à caractère personnel, elle proscrit le traitement des données "sensibles" relatives à l'origine raciale, aux opinions politiques, à la santé, à la religion, à la vie sexuelle, aux condamnations pénales, etc. »*

Plan

Donnée personnelle et personne concernée

Selon l'article 5 de la LPD, on entend par :

- **Données personnelles** : « *toutes les informations qui se rapportent à une personne identifiée ou identifiable* »
- **Personne concernée** : « *la personne physique dont les données personnelles font l'objet d'un traitement* »

L'article 4 dU RGPD définit une **donnée à caractère personnel** comme :

« toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »

Données sensibles

Selon l'article 5 de la LPD, les **données sensibles** incluent les données :

- « sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales »
- « sur la santé, la sphère intime ou l'origine raciale ou ethnique »
- « génétiques »
- « biométriques identifiant une personne physique de manière univoque »
- « sur des poursuites ou sanctions pénales et administratives »
- « sur des mesures d'aide sociale »

Dans le RGPD ces éléments sont explicitement ou implicitement inclus dans la définition d'une donnée à caractère personnel.

Profilage et profilage à risque élevé

La définition que donne le RGPD du **profilage** dans son article 4 est reprise mot à mot (ou presque) dans l'article 5 de la LPD :

> *« toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique »*

La LPD définit encore le **profilage à risque élevé** comme :

> *« tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique »*

Consentement de la personne concernée

L'article 4 du RGPD définit le **consentement de la personne concernée** comme :

> *« toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »*

La LPD ne définit explicitement la notion de consentement. Toutefois, dans les principes de la loi, on peut lire :

> *« Lorsque le **consentement de la personne concernée** est requis, celle-ci ne consent valablement que si **elle exprime librement sa volonté** concernant un ou plusieurs traitements déterminés et **après avoir été dûment informée** »*

Traitement

L'article 5 de la LPD définit un **traitement** comme :

« toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données »

L'article 4 du RGPD définit un **traitement** comme :

« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »

Responsable du Traitement

L'article 5 de la LPD définit le **responsable du traitement** comme :

> *« la personne privée ou l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles »*

L'article 4 du RGPD définit le **responsable du traitement** comme :

> *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement »*

Sous-traitant

L'article 5 de la LPD définit le **sous-traitant** comme :

> *« la personne privée ou l'organe fédéral qui traite des données personnelles pour le compte du responsable du traitement. »*

L'article 4 du RGPD définit le **sous-traitant** comme :

> *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »*

Violation de la sécurité des données

L'article 5 de la LPD définit une **violation de la sécurité des données** comme :

« toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données »

L'article 4 du RGPD définit une **violation de données à caractère personnel** comme :

« une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »

Plan

Grands principes de la protection des données

On peut identifier 9 grands principes :

- Principe de finalité
- Principe de proportionnalité
- Principe de léicité (ce qui est légal et légitime)
- Principe de transparence
- Principe d'exactitude
- Principe de sécurité
- Principe de « privacy by design » / « privacy by default »
- Principe de durée de conservation limitée
- Principe de responsabilité (*accountability*)

Principe de finalité

Les données ne peuvent être traitées que dans le but pour lequel elles ont été récoltées. Par exemple, une adresse électronique fournie pour un abonnement à newsletter ne doit pas être utilisée pour de la prospection commerciale.

- La finalité d'un traitement doit être déterminée, légitime et explicite. Elle permet de déterminer la pertinence des données recueillies et de fixer leur durée de conservation. Tout détournement de finalité est passible de sanctions pénales.
- En particulier, elles ne peuvent en aucun cas être traitées ultérieurement de façon incompatible avec les finalités initial.
- Le traitement ultérieur à des fins archivistiques, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré comme incompatible avec les finalités initiales.

Principe de proportionnalité

- On parle aussi de minimisation des données.
- La récolte des données doit être limitée à ce qui est strictement nécessaire pour la réalisation de l'objectif.
- Ce principe s'applique en tenant compte de la finalité du traitement et de la nature des informations collectées.

Principe de licéité

Tout traitement de données personnelles doit être licite.

Pour être licite, le traitement doit respecter les règles destinées à protéger la personnalité et doit poser sur un motif justificatif appelé sur une « base légale ».

De plus, selon le RGPD, le responsable du traitement doit :

- définir la base légale du traitement **avant** sa mise en place et pour toute sa durée.
- informer la personne concernée avant la récolte des données personnelles.

Principe de licéité — Base légale

Selon le RGPD, il existe six bases légales :

- La personne concernée a donné son « consentement » au traitement de ses données pour une ou plusieurs finalités spécifiques
- Le traitement est nécessaire à l' « exécution d'un contrat ». Dans ce cas, le responsable du traitement ne peut traiter que les données strictement nécessaires à l'exécution du contrat.
- Le traitement est nécessaire au respect d'une « obligation légale » à laquelle est soumis le responsable du traitement.
- Le traitement est nécessaire à la « sauvegarde des intérêts vitaux » de la personne concernée ou d'une autre personne physique.
- Le traitement est nécessaire à l'exécution d'une « mission d'intérêt public »
- Le traitement est nécessaire aux fins des « intérêts légitimes » poursuivis par le responsable du traitement

Principe de transparence

Un traitement est transparent si le responsable du traitement fournit à la personne concernée toutes les informations préalables au traitement et s'il communique par écrit à propos de l'exercice de ses droits ou d'une violation de ses droits.

- Les informations communiquées doivent être compréhensibles et formulées dans des termes clairs et simples.
- Le principe de transparence implique un devoir d'information active. Le responsable du traitement DOIT communiquer, par exemple : son identité et ses coordonnées, la finalité du traitement, les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises.
- Il peut y avoir des exceptions, par exemple, si la personne a déjà reçu les informations nécessaires ou si le traitement est prévu par la loi.

Principe d'exactitude

Les données personnelles doivent être exactes et, si nécessaire, tenues à jour.

- Toutes les mesures raisonnables doivent être prises par le responsable du traitement pour que les données à caractère personnel qui sont inexactes, compte tenu des finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.
- La personne concernée a le droit de demander au responsable du traitement une rectification des données inexactes. Celui-ci doit alors apporter les mesures de correction nécessaires.

Principe de sécurité

Le responsable du traitement et le sous-traitant doivent prendre des mesures techniques et organisationnelles de protection afin d'en garantir la sécurité des données.

- Les risques pour la sécurité des données peuvent être la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées, ou l'accès non autorisé à ces données de manière accidentelle ou illicite.
- Cette obligation de sécurité nécessite un contrôle régulier et une anticipation de scénarios éventuels.
- En Suisse, le Conseil fédéral édicte des dispositions sur les exigences minimales en matière de sécurité des données (OPDo).

Principe de « Privacy by Design » / « Privacy by Default »

Privacy by Design

Le responsable du traitement doit mettre en place au moment de la détermination des moyens du traitement et au moment du traitement, des mesures techniques et organisationnelles qui prennent en compte les principes de protection des données et permettent de les respecter.

Privacy by Default

Le responsable du traitement doit également mettre en place des mesures qui permettent de garantir par défaut que le traitement est limité à ce qui est nécessaire. Cela s'applique à la quantité de données collectées, à leur utilisation, à leur durée de conservation et à leur accessibilité.

Principe de durée de conservation limitée

La conservation des données ne doit pas excéder la durée nécessaire au regard des finalités pour lesquelles elles sont traitées, à moins qu'il n'existe une obligation légale.

- La durée de conservation des données doit être communiquée aux personnes concernées lors de leur collecte.
- Toutefois les données à caractère personnel peuvent être conservées plus longtemps dans le cadre d'un traitement à des fins archivistiques, à des fins de recherche scientifique ou à des fins statistiques, pour autant que soient mises en place les mesures techniques garantissant les droits des personnes concernées.

Remarque : Ce principe est explicitement mentionné dans le RGPD. La LPD ne l'évoque pas explicitement, mais on en retrouve la plupart des éléments dans ses articles.

Principe de durée de conservation limitée — Phases de conservation

La conservation des données comprend trois phases :

- Phase courante : les données sont actives et utilisées
- Phase intermédiaire : le responsable du traitement doit conserver les données pour des raisons légales ou pour une utilisation dans le cadre d'un contentieux
- Phase d'archivage : le responsable du traitement doit se poser la question de la suppression des données, des procédés de destruction, d'effacement, d'anonymisation ou de pseudonymisation.

Principe de responsabilité (*accountability*)

Le responsable du traitement doit être capable de démontrer qu'il a mis en place des mesures techniques et organisationnelles pour assurer la conformité de tous les traitements.

Les principales obligations pour l'entreprise qui découlent de ce principe sont :

- La nomination d'un délégué à la protection des données.
- L'établissement de règles internes assurant la conformité au RGPD.
- L'établissement d'un registre de tous les traitements.
- La réalisation d'analyses d'impact, si nécessaire.
- Le respect des principes de Privacy by Design et Privacy by Default.
- La réalisation d'une politique de sécurité des données.
- La notification en cas de violation de données personnelles.

Remarque : Ce principe est explicitement mentionné dans le RGPD. La LPD ne l'évoque pas explicitement, mais on en retrouve la plupart des éléments dans ses articles.

Plan

Conclusion

Pour conclure, voici une citation d'Edward Snowden :

Lorsque vous dites « le droit à la vie privée ne me préoccupe pas, parce que je n'ai rien à cacher », cela ne fait aucune différence avec le fait de dire « Je me moque du droit à la liberté d'expression parce que je n'ai rien à dire », ou « de la liberté de la presse parce que je n'ai rien à écrire ».