

CONCEPT POUR LA PROTECTION DES DONNÉES

Le concept de protection des données pose de nouveaux jalons pour une protection des données moderne et efficace. Cette version actualisée poursuit l'approche pionnière consistant à retirer la protection des données de la responsabilité des personnes concernées et à définir au lieu de cela un cadre clair pour les entités traitant les données.



1 INTRODUCTION

La numérisation croissante et l'évolution rapide des technologies entraînent à la fois des opportunités et des risques. En particulier, l'interconnexion de grands volumes de données ainsi que le recours à l'intelligence artificielle affectent directement les droits de la personnalité. Selon la récente étude [Digital Radar Suisse 2024](#) (en allemand), les risques liés à l'utilisation personnelle des technologies numériques sont perçus comme significativement plus élevés qu'auparavant. Les personnes interrogées ont notamment pointé la « protection des données/sécurité informatique » ainsi que la « surveillance par les technologies » comme les principaux problèmes des technologies numériques.

De nombreuses personnes se sentent dépassées par la numérisation. Ce malaise est accentué par les rapports quasi hebdomadaires faisant état de fuite de données, ce qui affaiblit la confiance à l'égard du traitement des données. Or, cette confiance de la population est cruciale si l'on souhaite permettre l'émergence de nouvelles formes de démocratie numérique et d'administration électronique (e-government), ainsi que de nouveaux modèles économiques numériques. Ceci vaut également pour les espaces de données (« Datenräume »), qui permettent une utilisation secondaire des données personnelles au-delà de la finalité initiale.

Pour instaurer la confiance nécessaire, une gestion soigneuse des données est indispensable, fondée sur une protection des données ciblée et efficace. Protection des données et utilisation des données ne constituent pas une contradiction ; bien au contraire, elles dépendent l'une de l'autre.

2 CONDITIONS APPLICABLES AU TRAITEMENT DES DONNÉES SELON LA LOI FÉDÉRALE SUR LA PROTECTION DES DONNÉES

Selon l'article premier LPD, la loi a pour objet la « protection de la personnalité et des droits fondamentaux des personnes physiques dont les données font l'objet d'un traitement ». C'est une formulation très ouverte et générale, laissant planer une incertitude quant à l'objet précis de cette protection.

Les conditions de traitement licite des données sont prévues à l'article 6 (en relation avec l'art. 31) de la LPD. Le traitement de données personnelles doit être licite, transparent, conforme au principe de la bonne foi et proportionné. Il est également soumis au respect de la finalité du traitement. Par ailleurs, les responsables de traitement sont tenus de garantir l'exactitude des données traitées. La LPD prévoit également des dispositions relatives à l'anonymisation des données pour préserver les droits de la personnalité. En principe, les données anonymisées ne sont pas soumises aux exigences de la loi sur la protection des données, à condition qu'il soit impossible de rétablir un lien avec la personne concernée. Cependant, la pratique démontre qu'une réelle anonymisation est souvent difficile à garantir.

En vertu de l'art. 31 LPD, le traitement de données par des entités privées n'est autorisé que s'il repose sur le consentement de la personne concernée, un intérêt prépondérant public, privé ou sur une base légale. En revanche, lorsque le traitement est effectué par un organe fédéral, il faut dans tous les cas une base légale pour qu'il soit licite (art. 34 LPD). Ainsi, le traitement de données personnelles, même sensibles, peut être justifié par une base légale ou un intérêt prépondérant public ou privé sans que la personne concernée n'en ait connaissance ou n'y ait consenti.

3 LES LIMITES DE LA PROTECTION DES DONNÉES EN SUISSE

La loi fédérale sur la protection des données concrétise le droit constitutionnel à la protection de la personnalité. Selon l'article 13 al. 2 de la Constitution fédérale (Cst.), toute personne a droit à la protection contre l'usage abusif de ses données personnelles. Cette limitation du texte à l'utilisation abusive des données personnelles ne répond pas pleinement à l'objectif de protection et ne va donc pas assez loin (voir le commentaire Stämpfli sur la loi de protection des données).

Dans la pratique, en référence à l'art. 13 al. 2 Cst., le concept de droit à l'autodétermination en matière d'information s'est également établi. Il désigne le droit des individus à pouvoir décider par eux-mêmes de la divulgation et de l'utilisation de leurs données personnelles. Si cette notion semble évidente, ce droit bénéficie toutefois d'un faible ancrage juridique et ne peut être revendiqué que de manière limitée dans la pratique. Les intérêts prépondérants des responsables du traitement des données ou des obligations légales le restreignent considérablement. En outre, ce droit individuel reporte la responsabilité sur les personnes concernées elles-mêmes, les obligeant à gérer activement leur protection, que ce soit en cliquant sur des bandeaux cookies, en sélectionnant les bons paramètres de confidentialité ou en se défendant contre des pratiques intrusives. Par ailleurs, la protection des données ne concerne pas seulement les personnes qui divulguent leurs données, mais également la société dans son ensemble.

À notre sens, le fondement du droit suisse de la protection des données devrait être le droit au respect de la vie privée prévu par l'article 8 de la Convention européenne des droits de l'homme (CEDH). Ni le paradigme centré sur l'abus ni le droit à l'autodétermination informationnelle ne garantissent pleinement ce droit à la vie privée.

Face à ces lacunes, il est nécessaire de repenser la protection des données et d'élaborer un nouveau concept de base. La protection des données n'est pas une fin en soi. À cette fin, il convient tout d'abord de définir clairement contre quoi le droit à la protection des données doit effectivement protéger les individus. Ces objectifs de protection et le concept qui en découle doivent garantir qu'aucun préjudice ne résulte du traitement des données, ni pour les individus, ni pour la société dans son ensemble. Ils doivent également garantir le maintien d'un espace ouvert à l'innovation.

Une protection efficace et complète des données doit être une évidence sur laquelle les personnes peuvent compter sans devoir elles-mêmes agir activement.

4 OBJECTIFS DE PROTECTION

Partant des critiques formulées à l'égard du but trop général de la loi sur la protection des données ainsi que du flou concernant la délimitation de la protection qu'il accorde, il est nécessaire de définir clairement des objectifs spécifiques de protection. On distingue à cet égard six objectifs principaux :

4.1 Protection contre la manipulation

La protection contre la manipulation vise à préserver la liberté individuelle de décision et la formation autonome de la volonté.

Par « manipulation », on entend une influence intentionnelle, ciblée et généralement dissimulée, exercée sur les décisions d'une autre personne afin de contourner ou d'affaiblir son autonomie décisionnelle et son contrôle sur ses propres décisions. La manipulation peut causer un préjudice à la personne concernée et vise, en exploitant les faiblesses humaines, à orienter le comportement des individus ou de groupes.

4.2 Protection contre la discrimination

Les traitements de données ne doivent pas être discriminatoires. Selon l'article 8 alinéa 2 de la Constitution fédérale, une discrimination existe lorsqu'une personne est traitée de manière différente, sans justification, sur une base raciste¹ ou en raison de caractéristiques protégées telles que l'origine, le sexe, l'âge, la langue, la position sociale, le mode de vie, les convictions religieuses, philosophiques ou politiques ou un handicap physique, mental ou psychique.

Des dispositions visant la protection contre la discrimination existent ponctuellement dans des lois spécifiques, telles que le Code pénal (art. 261bis CP), la loi sur l'égalité (LEg) ou encore la loi sur l'égalité pour les personnes handicapées (LHand). Cependant, ces dispositions ne traitent pas directement de la discrimination résultant du traitement de données. Le droit civil relatif à la protection de la personnalité (art. 28 et suivants CC) protège contre les atteintes à la personnalité, mais ne place pas au centre la question de la discrimination. Les réglementations actuelles ne suffisent donc pas à protéger efficacement contre la discrimination causée par le traitement des données.

4.3 Protection contre la surveillance et préservation de l'anonymat

La protection contre la surveillance vise à garantir la liberté personnelle et le développement de la personnalité (art. 10 al. 2 Cst.), la liberté d'expression (art. 16 Cst.), ainsi que d'autres libertés fondamentales, telles que la liberté de réunion (art. 22 Cst.) et le respect de la sphère privée (art. 13 Cst.). Il est donc crucial d'éviter tout effet dissuasif (« chilling effects ») susceptible d'empêcher l'exercice effectif de ces droits fondamentaux.

La préservation de l'anonymat garantit la liberté de circulation et de se comporter anonymement dans l'espace public.

L'anonymat revêt une importance centrale dans l'exercice des droits fondamentaux dans l'espace numérique. Sur Internet, l'anonymat constitue une protection essentielle contre la surveillance indésirable. Dans les États répressifs, il permet l'échange d'informations dans un environnement risqué, garantit les libertés individuelles et protège contre la discrimination. En outre, l'anonymat protège contre la collecte indésirable de données, aspect particulièrement important à l'ère numérique.

Bien que l'anonymat puisse, dans certains cas, favoriser des dynamiques problématiques telles que les discours de haine et la radicalisation, les études montrent que ces phénomènes ne découlent pas directement de l'anonymat, mais surviennent également lorsque les auteurs agissent en utilisant leur nom réel. Par ailleurs, des moyens efficaces tels que les contre-discours existent pour combattre ces dynamiques tout en préservant l'anonymat.

4.4 Protection contre les atteintes à la santé et aux opportunités de vie et de développement

La protection contre les atteintes à la santé physique et psychique, ainsi qu'aux opportunités de vie et de développement, vise à éviter que les personnes ne subissent un préjudice du fait d'évaluations erronées, notamment celles réalisées par des systèmes automatisés de prise de décisions (Automated Decision-Making Systems, ADMS) basés sur l'intelligence artificielle. Cette protection inclut le droit à une évaluation (ou une réévaluation) par une personne humaine, ainsi que le droit à des mesures de protection supplémentaires telles que des obligations renforcées de diligence ou une certification.

4.5 Protection contre la stigmatisation

La permanence et l'ubiquité des données contredisent le fonctionnement même de la perception humaine, laquelle opère une sélection et un oubli naturels. La protection contre la stigmatisation doit assurer que les informations ne soient accessibles seulement aussi longtemps qu'un intérêt public le justifie. Le jugement de la Cour de justice de l'Union européenne (CJUE), selon lequel les informations ne doivent pas nécessairement être supprimées à la source, mais plutôt au point d'accès (« Google Spain », droit à l'oubli), répond à cette nécessité.

Même si le traitement initial des données est licite, il peut devenir illicite avec le temps, notamment lorsque les données ne sont plus pertinentes ou nécessaires à leur finalité initiale. La personne concernée doit alors avoir la possibilité de demander que les résultats accessibles au public ne contiennent plus de données qui la stigmatisent. Cela permet aux personnes concernées de poursuivre leur vie sans être durablement stigmatisées par des informations pour lesquelles il n'y a plus d'intérêt public.

En conséquence, la suppression des données préjudiciables devrait permettre aux personnes concernées de se libérer de la stigmatisation.

4.6 Protection de la société ouverte et de la démocratie libre

Le traitement des données n'affecte pas uniquement les individus, mais également la société dans son ensemble et la démocratie libre.

La société libre peut être menacée par le « social scoring » par exemple. Cette pratique repose sur la surveillance et le contrôle, menant à une uniformisation forcée des comportements. Une démocratie fonctionnelle et stable exige une société pluraliste exempte de dirigisme étatique.

La démocratie libre est également mise en danger lorsque des informations ciblées ou de fausses informations diffusées massivement influencent les élections à des fins de manipulation. Lorsque les messages sont ciblés et personnalisés et qu'il n'y a pas de transparence sur la diffusion de ces informations sont diffusées, l'espace de débat risque de se fragmenter, entraînant une distorsion de l'opinion publique. L'accès à diverses informations et perspectives doit être garanti afin de permettre des opinions diverses et un processus démocratique pluraliste.

Enfin, il est crucial d'éviter tout effet dissuasif (« chilling effects ») à cause desquels les individus renonceraient à exercer leurs libertés fondamentales en raison de la surveillance ou de répercussions négatives. Une protection efficace des données établit la confiance nécessaire pour permettre l'exercice effectif des libertés fondamentales, telles que la liberté d'expression (art. 16 Cst.) et la liberté de réunion (art. 22 Cst.), sans crainte d'être surveillé ou sanctionné. Cette protection constitue une condition indispensable à l'existence d'une démocratie libérale.

5 CONCEPT

À partir des objectifs de protection définis ci-dessus, il convient d'élaborer un concept visant une protection des données ciblée et efficace, capable de créer la confiance nécessaire tout en favorisant l'innovation. Contrairement à l'approche dominante dans le discours actuel sur la protection des données qui met l'accent sur le consentement préalable et le principe de finalité limitée, le nouveau concept place au centre le respect des objectifs de protection ainsi que le droit à une codécision substantielle, dont le respect et l'application effective doivent être garantis. Ce concept régit le traitement des données en général, sans se limiter exclusivement aux données personnelles. Il établit également des principes généraux relatifs au traitement des données, prévoit une interdiction absolue pour certaines catégories de traitements particulièrement risqués et fixe des règles claires concernant leur mise en œuvre. Ainsi est créé un cadre assurant la protection des droits des personnes concernées et de la société dans son ensemble.

5.1 Principes fondamentaux

Les traitements de données sont autorisés dans la mesure où ils garantissent une protection complète contre les traitements illicites de données. Cette protection est assurée par le respect des objectifs de protection et des principes généraux, ainsi que par l'application effective du droit à une codécision substantielle. Dans ce cadre, les traitements de données sont licites.

Les principes généraux suivants doivent être respectés :

- Les traitements de données effectués par les acteurs et actrices privés et publics doivent préserver les objectifs de protection, tant des individus que de la société.
- Les traitements de données effectués par des organes étatiques nécessitent impérativement une base légale claire, précisant de manière explicite quelles données sont traitées, dans quel but et de quelle manière.

5.2 Interdiction absolue

En principe, pour que les traitements de données soient licites, il suffit que le respect des objectifs de protection soit assuré (et, pour les traitements de données par des organes étatiques, qu'une base légale claire existe). Toutefois, certains traitements de données présentant un risque élevé pour les individus ou la société, et qui ne peuvent garantir le respect des objectifs de protection, sont totalement interdits et ne sauraient être justifiés. Cela concerne notamment les traitements biométriques ou la surveillance de masse non ciblée (par exemple, la reconnaissance faciale dans les espaces publics) ainsi que le social scoring.

5.3 Codécision substantielle

Le droit à l'autodétermination informationnelle, tel qu'actuellement conçu, implique que chaque individu est personnellement responsable de la protection de ses propres données. Or, dans la pratique, l'efficacité réelle de ce droit est clairement limitée. Par conséquent, il incombe aux responsables du traitement des données de respecter les intérêts des personnes concernées et de garantir le respect des objectifs de protection. Sous ces conditions, un traitement de données conforme aux principes énoncés et aux objectifs de protection peut être effectué même sans consentement préalable.

De plus, grâce au droit à une codécision substantielle, les personnes concernées ne doivent pas simplement être informées du traitement de leurs données (traitement conforme aux objectifs de protection), mais doivent également pouvoir participer activement, facilement et efficacement à la prise de décision concernant ce traitement. Le cœur du droit à une codécision substantielle est constitué par la possibilité d'exercer facilement un droit d'opposition, tant à l'égard du traitement des données lui-même que des modalités de ce traitement, telles que l'anonymisation. Pour cela, les responsables du traitement doivent respecter une obligation stricte de transparence et de diligence. En particulier, ils doivent mentionner clairement la traçabilité du traitement des données, notamment en cas de transmission à des tiers, ainsi que le recours à des systèmes automatisés de prise de décisions (ADMS), tels que l'intelligence artificielle.

En se basant sur le cadre fourni par les objectifs de protection et ce nouveau concept, ce droit à une codécision substantielle assure une protection des données nettement plus efficace et mieux ciblée que le droit actuellement en vigueur et le principe d'autodétermination informationnelle.²

5.4 Sécurité des données

La sécurité des données constitue une condition préalable indispensable à une protection efficace des données. À ce titre, les responsables du traitement des données ont l'obligation d'assurer que la sécurité des données est garantie et que les failles sont efficacement évitées conformément aux règles techniques reconnues et au devoir de diligence.

5.5 Mise en œuvre

Dès lors que les objectifs de protection, le droit à une codécision substantielle des personnes concernées et la sécurité des données sont garantis, les traitements de données – en particulier ceux concernant des données personnelles – peuvent être effectués sans restrictions supplémentaires. En revanche, le non-respect des objectifs de protection est inadmissible et constitue une violation du règlement. Le respect effectif des objectifs de protection doit donc être assuré par des sanctions efficaces et des mécanismes adéquats de mise en œuvre. En particulier, la prise de risques importants ou la violation systématique des principes fondamentaux, des interdictions ou du droit à une codécision substantielle doit entraîner des sanctions sévères.

Les institutions scientifiques, les organisations de la société civile, les médias ainsi que les autorités doivent bénéficier d'un droit d'information étendu. Les associations et les autorités de contrôle doivent disposer d'un droit de recours. L'autorité de contrôle compétente devrait pouvoir prononcer des sanctions administratives. En cas de succès devant les tribunaux, les associations doivent être indemnisées proportionnellement aux frais encourus. Afin de pallier le déséquilibre de pouvoir entre les responsables du traitement des données et les personnes concernées, il convient d'introduire une inversion de la charge de la preuve. Par ailleurs, il doit être possible de vérifier les décisions résultant de l'utilisation de systèmes automatisés de prise de décisions (ADMS, intelligence artificielle), par exemple par un accès aux données pertinentes.

6 EFFETS

Le concept ainsi proposé garantit une protection des données ciblée et efficace, fondée sur les objectifs de protection énoncés. Les responsables du traitement des données sont tenus à davantage de responsabilité quant au respect des intérêts des personnes concernées et de la société dans son ensemble. Les individus disposent d'un droit substantiel à la codécision. Ainsi, la confiance envers l'utilisation et le traitement des données est renforcée.

1. Dans la Constitution (art. 8 al. 2 Cst.) et le Code pénal (art. 261bis CP), le terme « race » est employé pour définir la discrimination. Or, ce terme implique une vision de l'humanité basée sur la prétendue existence de différentes « races humaines », perpétuant ainsi un héritage historique lié à la violence raciste. L'emploi même de ce terme constitue une contradiction irréconciliable avec le but déclaré de ces dispositions, à savoir la lutte contre la discrimination raciste (cf. <https://www.amnesty.ch/fr/sur-amnesty/langage-inclusif/glossaire>).
2. Dans la loi fédérale sur la protection des données (LPD), le consentement de la personne concernée constitue (à côté de la justification par un intérêt prépondérant privé ou public ou une base légale) « seulement » un moyen permettant de remédier à une atteinte illicite à la personnalité. Cette possibilité de consentement affaiblit en réalité les droits des personnes concernées. Un droit d'opposition facilement exerçable, capable de rendre illicite une atteinte à la personnalité, n'est pas prévu, alors même que Société Numérique (« Digitale Gesellschaft ») avait vivement revendiqué un tel droit jusqu'à la fin de la révision de la LPD. Ainsi, le droit à une codécision substantielle prévu dans le présent concept pour la protection des données assure, dans la pratique, davantage d'autodétermination informationnelle que le régime actuel prévu par la LPD.

cms

Soutenu par

Christoph Merian Stiftung