Concept pour la Protection des données

Société Numérique
2023

Concept pour la Protection des données

Société Nummérique 2023

Introduction

L' avancement de la numérisation et le développement rapide des technologies sont porteurs d'opportunités autant que de dangers. Le recoupement de grandes bases de données entre elles tout comme le recours à l'intelligence artificielle constituent de réelles entraves aux droits individuels des personnes. Les résultats du sondage post-électoral sur le référendum sur l'e-ID, rejeté à 64.4 % des suffrages en 2021, a montré à quel point la protection des données est une préoccupation centrale pour la population suisse.

De nombreuses personnes se sentent dépassées par la transformation numérique. Le malaise qui en résulte est renforcé par les révélations quasi-hebdomadaires concernant des fuites de données. Or, la confiance de la population est d'une importance capitale pour de nouvelles possibilités de démocratie numérique et de cyberadministration, tout autant que pour de nouveaux modèles commerciaux. Il en va de même pour les «espaces de données», dans lesquels une utilisation secondaire des informations personnelles doit être possible au-delà de la motivation initiale ayant justifiée la collecte de données.

Loi sur la protection des données et Constitution fédérale

Selon son article 1, la loi sur la protection des données (LPD) a pour but de «protéger la personnalité et les droits fondamentaux des personnes physiques dont les données personnelles font l'objet d'un traitement». Cet article est formulé de manière très ouverte et générale. Ce qui doit être concrètement protégé n'est pas clair. Selon l'art. 13 al. 2 de la Constitution fédérale (Cst.), sur lequel vient s'ancrer la loi sur la protection des données, «toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent». Ce que cette notion d'abus inscrite dans la constitution signifie, c'est qu'il n'est possible de saisir la justice qu'une fois que des pratiques abusives sont déjà advenues et que le fardeau de la preuve incombe aux individus concernés. Une telle limitation est inhabituelle pour la formulation de droits fondamentaux, qui ne sont normalement restreints qu'à travers l'art. 36 de la Constitution.

La formulation de l'art 13 al. 2 Cst. est par conséquent critiquée comme trop réduite. La jurisprudence l'interprète comme un droit à l'autodétermination informationnelle, c'est-à-dire le droit des individus à pouvoir décider eux-mêmes de la divulgation et de l'utilisation de leurs données personnelles. Si le droit à l'autodétermination en matière d'information semble évident, il n'est que faiblement détaillé dans la loi. Dans la pratique, il n'est pas vraiment possible de l'invoquer. Les intérêts prépondérants des organisations traitant les données ou les obligations légales sont autant de limites à son application. Il est également problématique de faire reposer la responsabilité de l'application d'un droit fondamental sur les individus eux-mêmes, qu'il s'agisse de cliquer sur les bannières de cookies, de trouver les bons paramètres de confidentialité ou de se défendre contre des pratiques abusives.

La protection des données ne concerne toutefois pas seulement les individus, mais aussi la société dans son ensemble. Ainsi, en cas de manipulation électorale, c'est-à-dire de manipulation de (groupes de) personnes pour influencer le résultat d'une élection, l'impact individuel est faible, mais les dommages causés à la société peuvent être énormes.

Au vu de ces lacunes, il est nécessaire de repenser la protection des données et de développer un concept qui serve de nouvelle base. La protection des données n'est pas une fin en soi. C'est pourquoi il est d'abord nécessaire de définir clairement contre quoi le droit de la protection des données doit réellement protéger. Ces objectifs de protection de ce concept visent à garantir que les individus d'une part et la société d'autre part ne subissent aucun préjudice lié au traitement de données. Dans le même temps, ils veillent à laisser le champ libre à l'innovation.

Objectifs de protection

Partant de la critique de la loi sur la protection des données considérant son objectif comme trop peu spécifique et son champ de protection comme peu clair, il convient d'être concret. Il en résulte les sept objectifs de protection suivants:

Droit d'être protégé contre les manipulations

La protection contre les manipulations vise à protéger la liberté de décision individuelle et la formation démocratique de la volonté.

Par manipulation, on entend l'influence exercée intentionnellement, de façon ciblée et généralement dissimulée sur la décision d'une autre personne, dans le but de subvertir son autocontrôle et son pouvoir de décision. La manipulation peut entraîner un préjudice pour la personne concernée. En exploitant les faiblesses humaines, elle vise à orienter le comportement d'individus ou de groupes. Plus une personne est vulnérable, plus elle est exposée.

Droit d'être protégé contre la discrimination

Les traitements de données ne doivent pas être discriminatoires. Il y a discrimination lorsqu'une personne est traitée de manière raciste [1] ou de manière différente des autres sans raison objective du fait 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 réglementations visant à protéger contre la discrimination se trouvent de manière isolée

dans des lois comme le droit pénal (art. 261bis CP), la loi fédérale sur l'égalité entre hommes et femmes (LEg) ou la loi sur l'égalité pour les personnes handicapées (LHand). Ces dispositions n'ont toutefois pas pour objet direct la discrimination par le traitement des données. En droit civil, la protection de la personnalité protège contre les atteintes à la personnalité (art. 28 ss. CC), mais la discrimination n'est pas au centre des préoccupations. Les réglementations existantes sont insuffisantes contre la discrimination par le traitement des données.

Droit d'être protégé contre la surveillance et droit à l'anonymat
La protection contre la surveillance doit permettre de garantir la liberté personnelle et le développement de la personnalité (art. 10 al. 2 Cst.), la liberté d'expression (art. 16 Cst.) et d'autres droits fondamentaux, comme notamment la liberté de réunion (art. 22 Cst.) et la protection de la sphère privée (art. 13 Cst.). Pour cela, il est particulièrement important que l'exercice des droits fondamentaux sont préservés de tous possibles effets dissuasifs («chilling effects»).

Le droit à l'anonymat garantit la liberté de mouvement, c'est à dire le droit de se déplacer et se comporter dans l'espace public de manière fondamentalement anonyme.

Droit d'être protégé contre les atteintes à la santé ou aux opportunités de développement et de vie
La protection contre les atteintes à la santé mentale et physique ainsi qu'aux opportunités de développement et de chances vie vise à garantir que les personnes ne soient pas lésées par une (mauvaise) évaluation effectuée par des systèmes décisionnels automatisés (ADMS, intelligence artificielle). Ce principe de protection se traduit par le droit à une (ré) évaluation par un être humain des décisions ainsi prises et, pour les évaluations où cela n'est pas possible, à des mesures de protection supplémentaires comme un devoir de diligence accru ou une certification.

Droit à la transparence et devoir de diligence
Le droit à la transparence donne aux personnes le droit de savoir précisément quelles données les concernant font l'objet d'un traitement. Cela implique un droit de regard substantiel. Pour cela, le traitement des données doit être clairement identifiable et un droit d'opposition facilement accessible doit pouvoir être exercé là-même où le traitement se passe. Les personnes qui traitent les données doivent garantir une traçabilité en cas

de leur transmission à des tiers, une possibilité de correction et d'opposition ainsi qu'un droit d'effacement dans le cadre du droit de regard substantiel. L'utilisation de systèmes décisionnels automatisés (ADMS, intelligence artificielle) doit être identifiable.
La sécurité des données est une condition préalable à une protection des données efficaces. Les personnes chargées du traitement doivent veiller à ce que la sécurité des données soit garantie et à ce que les violations soient effectivement évitées, en faisant preuve de diligence conformément aux règles techniques reconnues.

Droit à l'oubli
Le droit à l'oubli doit garantir que les informations ne soient pas disponibles de manière permanente, afin de permettre une resocialisation. La permanence et l'ubiquité des données vont à l'encontre du fonctionnement de la perception humaine, qui sélectionne et oublie. L'arrêt Google Spain, SL, Google Inc vs Agencia Española de Protección de la Cour de justice de l'Union européenne (CJUE) en tient compte, selon lequel l'effacement ne doit pas se faire à la source, mais là où l'information peut être trouvée.

Droit à la protection de la société ouverte et de la démocratie
Les traitements de données peuvent avoir des conséquences non seulement pour les individus mais aussi pour la société dans son ensemble et la démocratie. Une société ouverte est menacée par le scoring social, qui se base sur la surveillance et le contrôle, et conduit à l'uniformisation de la société. Une démocratie stable et fonctionnelle nécessite une société pluraliste, libre de tout dirigisme étatique.

La démocratie est menacée lorsque des informations ciblées ou la diffusion consciente et massive de (fausses) informations à des fins de manipulation influencent les élections. Lorsque les messages sont ciblés et adaptés individuellement à certains groupes de personnes (et sans qu'il y ait de transparence sur les informations diffusées), la société encoure le risque réel de voir la sphère publique se fragmenter avec des conséquences néfastes pour la formation de l'opinion publique, qui peut se retrouver sujette à des distorsions. L'accès à différentes points de vue et informations doit être garanti pour permettre la formation d'une opinion diversifiée et pluraliste dans le processus démocratique.

Il s'agit d'éviter les effets dissuasifs («chilling effects») par lesquels les personnes n'exercent plus leurs droits fondamentaux en raison de la surveillance ou de la peur de consé-

quences indésirables. Une protection des données efficace permet la confiance nécessaire pour garantir que les personnes puissent exercer leurs droits fondamentaux, tels que la liberté d'opinion, d'expression ou de réunion, sans craindre d'être surveillées et sanctionnées. Il s'agit là d'une condition sine qua non pour l'existence d'une démocratie.

Concept

De ces objectifs de protection découle un concept pour une protection des données ciblée et efficace, qui permet la confiance et encourage l'innovation. Ce concept met l'accent sur le respect des objectifs de protection et leur application. Il se distancie des concepts de consentement au traitement des données et de limitation des finalités. Il réglemente le traitement des données et non les données personnelles en tant que telles. Le concept comprend des principes pour ce traitement, une interdiction absolue pour certains traitements de données, un droit de regard substantiel pour les personnes concernées par les décisions ainsi que des dispositions pour son application.

Principes

Les traitements de données doivent être possibles sans consentement, dans le respect des objectifs de protection. Les personnes chargées du traitement des données se doivent de préserver l'équilibre entre les intérêts des personnes concernées et de veiller à ce que le traitement des données n'ait pas de conséquences indésirables pour les individus et la société. Les traitements de données ne doivent pas mettre en danger le fonctionnement d'une société démocratique et ouverte. En outre, ils doivent respecter les prescriptions en matière de transparence, de droit de regard substantiel aux décisions et de sécurité des données. Dans ce cadre, le traitement des données doit être possible indépendamment de toute limitation de la finalité, c'est à dire sans que son autorisation ne soit conditionnée à un usage particulier.

Les principes suivants s'appliquent :

Les traitements de données privés et publics doivent respecter les objectifs de protection des individus et de la société.

Le traitement de données par les autorités publiques doit impérativement reposer sur une base légale claire indiquant précisément quelles données sont traitées, dans quel but et comment.

Interdictions

Les traitements de données sont en principe légitimes dès lors que le respect des objectifs de protection est assuré (et qu'il existe une base légale claire dans le cas d'un traitement de données par les autorités publiques). Toutefois, les traitements de données qui comportent un risque important pour les individus ou la société et qui ne peuvent pas garantir les objectifs de protection sont absolument interdits et ne peuvent en aucun cas être justifiés. Il s'agit notamment de la surveillance biométrique de masse (par exemple la reconnaissance faciale dans l'espace public), de la surveillance sans motif préalable et du scoring social.

Droit de regard substantiel

Le droit à l'autodétermination en matière d'information est limité dans la pratique. Les personnes qui traitent les données ont donc l'obligation de préserver les intérêts des personnes concernées et de respecter les objectifs de protection. Un traitement de données dans le cadre des principes et dans le respect des objectifs de protection est possible sans consentement. Toutefois, les traitements de données doivent être sûrs et reconnaissables pour les personnes concernées. Elles doivent avoir la possibilité d'intervenir par rapport à la décision, notamment pour exercer facilement un droit d'opposition.

Mise en œuvre

Si les objectifs de protection sont respectés, les données, et en particulier les données personnelles, peuvent être traitées sans restriction. Toutefois, si les objectifs de protection ne sont pas respectés, il s'agit d'une violation de la réglementation et le traitement des données est inadmissible. La garantie des objectifs de protection doit par conséquent être assurée par des sanctions et des mécanismes d'application efficaces. L'acceptation de risques très importants et la violation systématique des principes, des interdictions et du droit de regard substantiel doivent tout faire l'objet de sanctions lourdes. Il existe un droit d'information étendu vis-à-vis de la science, des organisations de la société civile, des médias et des autorités. Les associations et les autorités de surveillance ont le droit d'intenter une action en justice. En cas de succès devant les tribunaux, les associations doivent être indemnisées à hauteur de leurs dépenses. Un renversement du fardeau de la preuve doit contrecarrer l'asymétrie de pouvoir vis-à-vis des personnes traitant les données. Il doit

être possible de vérifier les décisions prises lors de l'utilisation de systèmes décisionnels automatisés (ADMS, intelligence artificielle), par exemple en accédant aux données.

Effets

Le concept conduit à une protection des données ciblée et efficace dans le respect des objectifs de protection. Les personnes qui traitent les données sont davantage tenues de préserver les intérêts des personnes concernées et de la société. Les individus ont un droit de regard substantiel de participation et d'intervention sur la décision. La confiance dans l'utilisation et le traitement des données est renforcée.

[1] Dans la Constitution (art. 8 al. 2) et la loi (art. 261bis du Code pénal), la définition de «discrimination» se réfère à la notion de «race». Le mot suggère une image de l'humain basée sur l'idée de «races» humaines différentes et renvoie à une longue histoire de violence raciste. L'utilisation de ce terme est donc en contradiction totale avec l'objectif de la disposition, qui est de lutter contre la discrimination raciale. (voir https://www.institut-fuer-menschenrechte.de/themen/rassistische-diskriminierung/begriff-rasse; https://www.amnesty.de/glossar-fuer-diskriminierungssensible-sprache).