UNIL | Université de Lausanne
IDHEAP
Institut de hautes études
en administration publique

Ismaël Tall

Le renforcement de la loi fédérale sur la protection des données : le cas de la protection de la vie privée dès la conception (privacy by design)

Cahier de l'IDHEAP 289/2015

Unité *Droit public*

Ismaël Tall

Le renforcement de la loi fédérale sur la protection des données : le cas de la protection de la vie privée dès la conception (*privacy by design*)

Cahier de l'IDHEAP 289/2015

Unité *Légistique*

Travail de mémoire
Rapporteur : Prof. Luzius Mader

ISBN 978-2-940390-75-5

IDHEAP
Institut de hautes études en administration publique
Université de Lausanne
Bâtiment IDHEAP, 1015 Lausanne
Tél. +41 (0)21 692 68 00, Fax +41 (0)21 692 68 09
E-mail : idheap@unil.ch – www.unil.ch/idheap

Page de remerciements

Mes remerciements au Professeur Luzius Mader qui a supervisé ce travail et fourni de précieux conseils et au Professeur Bertil Cottier pour son expertise lors de la soutenance.

SOMMAIRE

LISTE DES ABRÉVIATIONS

AFCDP	Association française des conseillers à la protection des données
AG	Aktiengesellschaft
al.	alinéa
AOL	America Online Inc.
art.	article
BDSG	Bundesdatenschutzgesetz
CC	Code civil suisse, du 10 décembre 1907, RS 210
CEDH	Convention européenne des droits de l'homme
CEPD	Contrôleur européen à la protection des données
CIL	Correspondant informatique et libertés
CJUE	Cour de justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
Conv.	Convention
consid.	considérant
CP	Code pénal suisse, du 21 décembre 1937, RS 311.0
CSS	Cascading Styles Sheets
Cst.	Constitution fédérale, du 18 avril 1999, RS 101
DFJP	Département de justice et police
Dir.	Directive
DPO	Data Protection Officer
EIVP	Evaluation d'impact sur la vie privée

FISAA	Foreign Intelligence Surveillance Act of 1978, Amendments Act of 2008
FSFP	Fédération suisse des fonctionnaires de police
G29	Groupe « Article 29 »
GPS	Global Positioning System
HTML	Hypertext Markup Language
ibid.	ibidem
IP	Internet Protocol
ISO	International Organization for Standardization
LEIS	Loi fédérale du 12 juin 2009 sur l'échange d'informations entre les autorités de poursuite pénale de la Confédération et celles des autres Etats Schengen, RS 362.2
let.	lettre
LIBE	Commission Libertés civiles, justice et affaires intérieures
LPD	Loi fédérale du 19 juin 1992 sur la protection des données, RS 235.1
Ltrans	Loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (Ltrans), RS 152.3
MCF	Message du Conseil fédéral
n°	numéro
NSA	National Security Agency
NTIC	Nouvelles technologies de l'information et de la communication
OaccD	Ordonnance du 17 juin 1996 sur le système suisse d'accréditation et la désignation de laboratoires d'essais et d'organismes d'évaluation de la conformité, d'enregistrement

	et d'homologation (Ordonnance sur l'accréditation et la désignation, OaccD), RS 946.512
OCDP	Ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD), RS 235.13
OFJ	Office fédéral de la justice
OLPD	Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD), RS 235.11
ONU	Organisation des Nations Unies
p.	page
P3P	Platform for Privacy Preferences Project
PCDA	Plan Do Check Act
PET	Privacy enhancing technologies
PFPDT	Préposé fédéral à la protection des données et à la transparence
PFPD	Préposé fédéral à la protection des données
PIA	Privacy impact assessements
PIT	Privacy-invasive technologies
PIVP	Protection intégrée de la vie privée
RFID	Radio frequency identification
RH	Ressources humaines
RS	Recueil systématique du droit fédéral
SAS	Service d'accréditation suisse
SGPD	Système de gestion de la protection des données
TIC	Technologies de l'information et de la communication

UE	Union européenne
ULD	Unabhängiges Landeszentrum für Datenschutz
W3C	World Wide Web Consortium
WWW	World Wide Web

RÉSUMÉ

La protection des données est un élément essentiel d'un Etat de droit et une société démocratique, car elle accorde à chaque individu le droit de disposer de ce qui fait partie de sa sphère privée.

Actuellement en Suisse, la loi fédérale sur la protection des données (LPD) est en vigueur depuis 1993. En 2010, l'Office fédéral de la justice a supervisé une évaluation de son efficacité : il en résulte que cette dernière a été prouvée, mais tendra à diminuer fortement dans les années à suivre. Pour causes principales : l'évolution des technologies, caractérisée notamment par le développement des moyens de traitement de données toujours plus variés et conséquents, et un manque d'informations des individus par rapport à la protection des données en générale et à leurs droits. Suite à l'évaluation, cinq objectifs de révision ont été formulés par le Conseil fédéral, dont celui d'intégrer la *privacy by design* ou « protection de la vie privée dès la conception » dans la loi. Ce concept, qui est également repris dans les travaux européens en cours, est développé à l'origine par l'*Information and Privacy Commissionner* de l'Ontario (Canada), Ann Cavoukian. Le principe général de la *privacy by design* est que la protection de la vie privée doit être incluse dans les systèmes traitant les données lors de leur conception.

Souvent évoquée comme une solution idéale, répondant au problème de l'inadéquation de la loi par la logique de prévention qu'elle promeut, la *privacy by design* demeure toutefois un souhait dont l'application n'est que peu analysée. Ce travail cherche justement à répondre à la question de la manière de la mettre en œuvre dans la législation suisse. Se basant sur les textes et la doctrine juridiques et une littérature dans les domaines de l'économie, l'informatique, la politique et la sociologie des données personnelles, il propose tout d'abord une revue générale des principes et définitions des concepts-clés de la protection des données en Suisse et dans le cadre international. Puis, il propose deux possibilités d'intégration de la *privacy by design* : la première est une solution privée non contraignante qui consiste à promouvoir le concept et faire en sorte que les responsables de traitement décident par eux-mêmes d'intégrer la

privacy by design dans leurs projets ; ce procédé est possible grâce au renforcement du processus de certification déjà en cours. La deuxième option est une solution contraignante visant à intégrer le principe directement dans la loi et de prendre les mesures pour le rendre effectif ; ce travail montre que le développement de la figure du conseiller à la protection des données permet d'atteindre cet objectif. Enfin, des considérations générales sur l'application du principe sont abordées, telles que l'influence des développements en cours dans l'Union européenne sur la Suisse par rapport à la protection des données et la limite posée par le principe de territorialité.

1 INTRODUCTION

La protection des données est un enjeu majeur de notre société. Selon son principe, tout citoyen doit pouvoir garder un contrôle sur ses données, car il possède un droit à la vie privée ; c'est en Suisse un droit fondamental. Par données, on entend toutes les informations permettant d'identifier une personne. De ce fait, la protection des données relève de la vie privée.

La protection des données est un élément essentiel d'un Etat de droit et une société démocratique en accordant à chaque individu le droit de disposer de ce qui fait partie de sa sphère intime. Il est issu de l'individualisme et du libéralisme qui apparaissent au cours du 19ème siècle et se concrétise sous la forme d'un droit à être laissé en paix (Meier 2010, §3). La notion de sphère privée se développe, ainsi donc de toutes les données qui s'y rapportent. Si le droit à une vie privée existe depuis fort longtemps déjà, du moins en Suisse, la question spécifique de la protection des données fait son apparition dans les années 70. La société se complexifie, les moyens de communication se développent, les premiers balbutiements de l'informatique se font entendre. En Europe et en Suisse, la nécessité de placer un cadre légal autour de la circulation des données se fait sentir, surtout par rapport aux possibilités grandissantes de collecter et transférer des données. Tour à tour, les pays européens se dotent d'une loi sur la protection des données. La Suisse adopte la loi sur la protection des données (LPD) en 1992, une loi reprenant les principes édictés dans la Convention 108 du Conseil de l'Europe datant de 1981, qui traite justement de la protection des données. Quant à l'Union européenne, elle adopte une directive en 1995, la Directive 94/45/CE.

Bien que la volonté de se doter d'une législation sur les données – européenne et suisse – fut en partie motivée par des questions d'évolution des technologies dans la société, la force de ces lois résidait, et réside pour l'instant toujours, dans leur portée générale. En effet, elles sont neutres d'un point de vue technologique : aucun concept trop technique ne s'y insère, ce qui permet une adaptation de la loi face aux évolutions de la société. En plus de leur souplesse, les lois énoncent des

principes généraux essentiels sur tout traitement des données tels que la nécessité d'une base légale, la proportionnalité, la bonne foi et la finalité d'un traitement.

2 PROBLÉMATIQUE

Aujourd'hui, malgré l'efficacité de ces différentes législations, force est de constater que la société a bien changé. Les législations suisse et européenne sont entrées en vigueur avant l'émergence d'Internet, qui a révolutionné les moyens de communication et d'informations. Les nouvelles technologies de l'information et de la communication (NTIC) ont vécu un essor formidable depuis le début des années 2000. Les ordinateurs se miniaturisent, tout en en multipliant leurs capacités de stockage et de calcul. La technologie prend globalement une place considérable dans notre vie quotidienne. Avec tous ces moyens, une information telle qu'une donnée personnelle par exemple peut circuler très vite. A l'heure où la transmission de l'information peut se faire en un clic et dépasse les frontières, la question de l'efficacité de la protection des données fait surface, en Suisse tout comme dans l'Union européenne. Les risques d'abus se multiplient et mettent alors en danger le citoyen, laissant entrevoir un futur qui n'a rien à envier à la dystopie orwellienne. Par ailleurs, en juin 2013, l'affaire PRISM a secoué le monde entier en montrant que l'Agence nationale de sécurité (NSA) américaine utilisait les données personnelles issues d'utilisateurs de services des géants de l'informatique comme Google, Facebook, Apple à des fins personnelles. L'enjeu de la protection des données a pris encore plus d'ampleur depuis ces révélations, mais la loi est-elle justement toujours adaptée ?

En Suisse, la LPD a déjà fait l'objet d'une révision en 2006, puis 2008. Mais cela ne suffit pas. Conscient des évolutions technologies exponentielles dans la société et les nouveaux comportements de la population, l'Office fédéral de la justice (OFJ) a décidé en 2010 de procéder à une évaluation de la LPD, en vertu de l'art. 170 Cst. L'évaluation a consisté à analyser la mise en œuvre de la LPD, interviewer des experts, interroger la population sur leur perception sur la question des données personnelles et mettre en perspective le rôle du préposé fédéral à la protection des données et à la transparence (PFPDT). Il a résulté de l'évaluation que la loi était encore efficace, mais les enjeux des données personnelles n'étaient que peu connus par les individus. Les évaluateurs ont proposé plusieurs pistes d'amélioration de

la loi, parmi lesquelles la *privacy by design* ou protection des données dès la conception, concept qui fait l'objet de ce travail. La *privacy by design* désigne le fait de concevoir des systèmes traitant les données de manière à ce qu'ils respectent dans leur architecture les principes essentiels de la protection des données. Il s'agit d'un mode de pensée qui va plus loin que la logique actuelle qui veut qu'un citoyen ou le PFPDT peut saisir la justice s'il pense qu'il y a un abus. Dans la protection des données dès la conception, on se situe dans le champ de la prévention. Cette solution est généralement évoquée dans les différents projets de modernisation des législations sur la protection des données dans les autres pays européens, l'UE et le Conseil de l'Europe.

Si la *privacy by design* apparaît souvent comme une solution idéale, la question des modalités d'une éventuelle application de ce concept n'apparaît pas. C'est ce que nous aimerions développer à travers ce travail. Ainsi, la question de recherche est la suivante :

De quelle manière peut-on mettre en forme et intégrer la question de la protection de la vie privée « dès la conception » dans la législation suisse ?

Si nous avons choisi d'étudier la protection de la vie privée dès la conception plutôt qu'une autre mesure proposée par le Conseil fédéral, c'est que les conséquences de son application seraient un grand bouleversement dans la logique de la protection des données. Savoir que tous les outils pouvant traiter des données soient conçus de façon à respecter les principes essentiels de la vie privée serait un pas de géant vers une société évoluant dans un environnement respectant par principe la vie privée.

3 MÉTHODE ET PLAN

L'analyse de l'intégration d'une nouvelle disposition dans une loi se fait en plusieurs étapes préalables. La méthode que nous emploierons est calquée sur la méthode de conception d'une loi, telle que définie dans le *Guide de législation « module loi »* proposé par l'OFJ (2008) et intitulée « phase de conception ». Elle détermine les mesures à prendre pour concevoir une loi ; chronologiquement, elle se situe après la phase d'impulsion et de planification et précède l'élaboration d'un avant-projet, la procédure de consultation, les délibérations parlementaires et la mise en œuvre.

Les étapes de la phase de conception sont les suivantes :

- Définir le problème et ses causes (OFJ 2008, §51 – 59) : cette étape « permet de déterminer si et, le cas échéant, pourquoi un état de fait doit être soumis à une réglementation ou pourquoi celle qui existe doit être modifiée » (*ibid*., §51). L'analyse de la dynamique d'un problème se fonde alors sur sa la nature de ce problème, ses causes, son contexte, son évolution, sa durée, ses effets, entre autres (*ibid*., §56). Une telle revue permet alors de déterminer les modalités d'intervention de l'Etat.
- Fixer les objectifs (*ibid*., §60 – 68) : cette étape « sert à définir l'état que l'on entend atteindre ou, du moins, qu'il serait souhaitable d'atteindre » (*ibid*., §60). En se devant de conserver un certain réalisme et un caractère concret, les objectifs déterminés indiquent le fil rouge d'une future recherche de solutions et les critères d'évaluation (*ibid*., §61).
- Définir le cadre normatif (*ibid*., §69 – 75) : cette étape existe du fait que « tout acte législatif nouveau ou modifié est appelé à s'insérer dans un cadre normatif existant » (*ibid*., §69). Elle permet de comprendre le contexte juridique qui est formé du droit fédéral, européen et international.
- Rechercher, élaborer et sélectionner des solutions (*ibid*., §76 – 89) : par la recherche de solutions, il s'agit de déterminer l'étendue des possibilités de résoudre le problème dégagé préalablement tout en répondant aux objectifs visés. Cette étape fait appel à des bonnes

connaissances sur le sujet et à une certaine imagination. Les solutions trouvées sont alors soumises à une évaluation plus ou moins formalisée (de l'expérience d'une solution dans un autre contexte à la simulation informatique, par exemple) et choisies en fonction des résultats.

– Elaborer une esquisse d'acte normatif (*ibid*., §90 – 97) : l'esquisse « définit dans les grandes lignes le contenu essentiel de l'acte, présente, dans la mesure du possible, des variantes de la solution choisie et contient des explications portant sur les points principaux rédigés par l'acte [...] » (*ibid*., §90). Elle traite notamment des moyens d'atteindre les objectifs, de la place dans la systématique, du niveau normatif (nouvel acte ou modifications de dispositions actuelles), du champ d'application, du contenu normatif, de la structure de l'acte et du calendrier des étapes.

Suite à cette phase de conception vient la réalisation d'un avant-projet, de l'écriture du rapport explicatif et de sa mise en consultation. Bien plus tard viennent alors les délibérations parlementaires.

Pour ce travail, les éléments issus du guide de législation servent avant tout de cadre structurant et permettent de mettre en évidence le contexte et les enjeux de la *privacy by design* et de répondre à la question de recherche. En effet, l'intégration d'un nouveau concept dans la législation demande une mise en contexte législatif, une évaluation de l'adéquation entre le problème identifié et la solution et l'analyse de possibles alternatives. Autant d'éléments fournissant des réponses au « comment ».

Dans ce travail, nous allons nous inspirer de ces étapes portant sur la phase de conception d'une loi, sans pour autant les suivre à la lettre, car d'une part elles sont issues d'un guide à destination des acteurs de l'administration publique et d'autre part, une partie des travaux sur le renforcement de la LPD a été réalisée par l'OFJ dans le cadre de l'évaluation de la loi. Ainsi, nous aborderons tout d'abord le cadre normatif suisse et international, afin de comprendre le contexte dans lequel évolue la notion de protection des données et de pouvoir donner une définition précise aux concepts-clés qui l'accompagnent. Les

dynamiques de renforcement des différentes législations seront également passées en revue (point 4).

Puis une définition précise du concept de *privacy by design* sera proposée, en expliquant l'origine de la notion et la volonté de son intégration en Suisse et dans le contexte international (point 5). Nous ouvrirons ensuite un chapitre général (point 6) sur les enjeux de la *privacy by design* et de la protection des données. Dans ce point seront abordés les impulsions à l'origine de la volonté de renforcement de la loi. Sachant qu'en Suisse, la volonté d'intégrer la *privacy by design* est issue notamment de l'évaluation de la LPD réalisée par l'OFJ (2011), nous reprendrons les développements du rapport d'évaluation décrivant les motifs d'une nécessité d'adaptation de la loi. Il s'agit en somme de présenter le problème public et de ses causes. Ceux-ci seront alors détaillés et mis en perspective. Enfin, nous nous intéresserons aux possibilités de mettre en pratique la *privacy by design* dans la législation suisse. Seront présentées les solutions paraissant les plus appropriées, leur mise en forme dans la loi et leurs implications (point 7).

Tout au long du travail sera mobilisée une littérature touchant à des domaines variés. Les sources juridiques, les documents officiels et la doctrine seront grandement utilisés et seront accompagnés d'une littérature portant les aspects techniques, économiques et sociologiques de la protection des données personnelles.

4 CADRE NORMATIF

Avant de s'intéresser à la *privacy by design* et aux raisons qui motivent son application, il s'agit de bien comprendre le cadre normatif, suisse et international, grâce à un *survol général* de la législation sur la protection des données. La présentation de ce cadre débute par le contexte international – surtout européen – puis nous nous intéresserons à la législation suisse. Nous aborderons ensuite les changements en cours dans les différents textes présentés.

4.1 DÉVELOPPEMENT DE LA PROTECTION DES DONNÉES DANS LE CADRE INTERNATIONAL

4.1.1 L'ART. 8 CEDH

La protection des données personnelles est assurée par la Convention européenne des droits de l'homme (CEDH), dont l'art. 8 al. 1 stipule : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ». Une jurisprudence importante concerne les données de nature médicale ou sexuelle (Meier 2010, §56). Par exemple, l'arrêt *Dudgeon* (22 octobre 1981, série A, n° 45) sur la violation de l'art. 8 CEDH par la répression de relations homosexuelles ou encore l'arrêt *Cossey* (27 septembre 1990, série A, n° 184) sur le changement de sexe relevant de la vie privée.

4.1.2 LA CONVENTION DU CONSEIL DE L'EUROPE

La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données personnelles (STE n°108 ou Conv. 108, en vigueur en Suisse depuis le 1er février 1998) est née de la nécessité d'un accord international par rapport au traitement automatisé des données (voir Rapport explicatif de la Conv. 108). Plusieurs Etats européens avaient une loi nationale sur la protection des données, notamment suite à deux Résolutions émises par le Comité des Ministres dans les années 70 énonçant des principes de protection des données respectivement dans le secteur public et privé. Le Conseil de l'Europe l'adopte le 28 janvier 1981 ; elle entre en vigueur le 1er octobre de cette même année.

Afin de saisir au mieux les dispositions de la Convention, reprenons les termes d'un extrait du rapport explicatif qui l'accompagne qui détermine les trois parties principales comme étant : « les dispositions de droit matériel sous forme de principes de base; les règles spéciales concernant les flux transfrontières de données; les mécanismes d'entraide et de consultation entre les Parties » (Rapport explicatif de la Conv. 108, consid. 18). La Conv. 108 dispose d'un caractère *non executing*, c'est à dire que « les droits des individus ne peuvent découler directement d'elle » (*ibid*., consid. 38).

Dans le chapitre I sur les dispositions générales, elle définit le but : « *Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données»)* » (art 1er Conv. 108). Elle établit dans ce chapitre également des définitions (reprises en partie en Suisse dans la LPD) et le champ d'application. Les principes de bases sont établis dans le chapitre II ; l'art. 4 Conv. 108, qui est sa première disposition, oblige les parties à respecter les principes énoncés aux art. 5 à 11. L'art. 5 Conv. 108 établit une liste de la « qualité des données », principes de bases à respecter lors de tout traitement automatisé (données obtenues licitement, à des fins déterminées – et non excessives –, exactes et dont la durée de conservation n'excède pas la finalité). Dans la LPD, comme nous le verrons en détail, les principes de base sont similaires à ceux énoncés ici, bien qu'en termes différents. Comme dans LPD, on évoque des données « à caractère particulier » (« sensibles » dans la loi suisse), ici à l'art. 6 Conv. 108. Les autres dispositions du chapitre II sont la sécurité des données contre une perte ou une destruction (art. 7 Conv. 108), les moyens de droit en cas de violation des principes (art .8 Conv. 108), les exceptions de dérogation aux principes (notamment en raison de la protection de la sûreté de l'Etat), les sanctions (art. 10 Conv. 108) et la portée non limitante de la Convention (art. 11 Conv. 108). Le chapitre III et son seul art. 12 Conv. 108 règle les flux transfrontières des données, son but est de « concilier les conditions nécessaires à une protection des données efficace avec le principe de la libre circulation

des informations sans considération de frontières » (Rapport explicatif de la Conv. 108, consid. 62). Les articles 13 à 17 Conv. 108 du chapitre IV sur l'entraide établissent les dispositions sur l'assistance mutuelle que doivent se porter les Parties, les garanties, les procédures et les motifs de refus de cette aide. Enfin, les chapitres V, VI, et VII et leurs articles traitent respectivement du comité consultatif, des amendements et des clauses finales.

Deux grandes idées générales se détachent de la Convention. Il s'agit premièrement de la neutralité technologique du texte, comme pour la LPD, qui permet une souplesse dans l'interprétation. Les normes juridiques s'adaptent ainsi à l'évolution technologique. Deuxièmement, le traitement automatisé des données à la fois par les personnes privées et publiques est concerné, tout comme la LPD[1].

Actuellement, 45 des 47 pays membres du Conseil de l'Europe ont ratifié la Convention, dont les 27 membres de l'UE. La Suisse l'a ratifiée le 2 octobre 1997 et elle est entrée en vigueur le 1er février 1998 (Meier 2010, p. 87).

Le Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, du 8 novembre 2001 (STE n° 181) vient compléter la Conv. 108. Il entre en vigueur le 1er juillet 2004. En Suisse, il est ratifié le 20 décembre 2007, avec une entrée en vigueur le 1er avril 2008, à l'occasion de la révision (novelle) de 2006. Le Protocole renforce les principes de la Conv. 108 et ajoute deux dispositions. La première prévoit que les Parties doivent disposer d'autorités de contrôle indépendantes chargées de faire respecter les principes énoncés dans la Convention. La deuxième traite du flux transfrontières de données : une transmission de données d'un Etat à l'autre ne peut se faire que si ce dernier dispose d'un niveau de protection adéquat (Rapport explicatif du Protocole).

[1] La LPD va plus loin encore en portant à la fois sur le traitement des données automatisé et manuel.

4.1.3 LE DROIT COMMUNAUTAIRE EUROPÉEN

4.1.3.1 LA DIRECTIVE 95/46/CE

Dans l'UE, une directive règle la protection des données. Il s'agit de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Avant l'entrée en vigueur du Traité de Lisbonne en décembre 2009, la directive relevait du premier pilier de l'UE.

Nous ne nous attarderons pas sur le texte dans ce travail. De manière générale, la directive est similaire avec la LPD par rapport aux principes de protection des données, aux définitions des différents acteurs, au transfert de données vers un pays tiers. Par sa nature de directive, elle demande aux Etats membres de l'UE une adaptation de leur législation à ses normes.

Toutefois, une disposition attire l'attention. Il s'agit de l'institution du groupe de protection des personnes à l'égard du traitement des données à caractère personnel (Groupe29 ou G29). En vertu de l'art. 29 Dir. 95/46/CE al. 2, « *le groupe se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission* ». L'art. 29 Dir. 95/46/CE définit les modalités d'élection et indique ses caractères indépendant et consultatif. Le G29 a pour mission de veiller à une application homogène de la directive dans les Etats membres ; il agit auprès de la Commission comme informateur sur le niveau de protection dans la Communauté et les pays tiers et comme conseiller par rapport aux projets de la Commission au sujet des données personnelles (art. 30 Dir. 95/46/CE). Il rédige un rapport annuel par la suite publié sur les questions des données personnelles (art. 30 al. 6 Dir. 95/46/CE). Il possède également la compétence d'émettre des recommandations de sa propre initiative (art. 30 al. 3 Dir. 95/46/CE). Par sa mission, le G29 a publié de nombreux documents utiles sur un grand nombre de sujets ayant un lien avec la protection des données.

D'autres textes communautaires ont un lien – moins direct – avec la protection des données, mais ils ne sont pas applicables en Suisse (Voir Meier 2010, §109 pour une liste exhaustive).

4.1.3.2 LA DÉCISION-CADRE 2008/977/JAI

Le 27 novembre 2008, le Conseil de l'UE adopte la Décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. La décision-cadre est un instrument adopté par le Conseil de l'UE qui ne s'applique pas directement, mais doit être repris par les Etats. La décision-cadre a été motivée par le fait que les Etats avaient besoin d'une réglementation claire dans le domaine de l'échange des données et que la Directive 95/46/CE ne remplissait pas ce rôle (MCF 2009, p. 6095). Elle rappelle les principes fondamentaux déjà décrits dans la Conv. 108, mais contient surtout des dispositions sur les modalités de transmission des données entre les Etats liés par les accords de Schengen. En principe, la transmission de données d'un Etat à un autre doit respecter les fins pour lesquelles il a été effectué, mais il peut y avoir des exceptions « à des fins de prévention et de détection d'infractions pénales, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales ou pour prévenir tout risque pour la sécurité publique »[2]. Sur le traitement des données, la décision-cadre rappelle les principes de licéité, de finalité, de sécurité, d'exactitude des données (elles doivent être rectifiées en cas d'erreur) et demande aux Etats de traiter des données sensibles (appartenance ethnique, opinion politique, convictions personnelles, appartenance syndicale, santé, vie sexuelle) qu'en cas d' « absolue nécessité »[3].

4.1.4 AUTRES TEXTES (PACTE ONU II, RÉSOLUTION DES NATIONS UNIES, LIGNES DIRECTRICES DE L'OCDE)

Parmi les autres textes relatifs à la protection des données dans le cadre international, on recense en premier lieu le pacte ONU II[4], s'appuyant

[2] http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/jl0018_fr.htm

[3] *ibid*.

[4] Pacte international du 16 décembre 1966 relatif aux droits civils et politiques, en vigueur en Suisse (RS 0.103.2).

sur la Déclaration universelle des droits de l'homme, dont l'art. 17 stipule :

« 1. *Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.* »

« 2. *Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.* »

La protection des données relève de ces dispositions implicitement (Meier 2010, §77).

En deuxième lieu, la Résolution 45/95 du 14 décembre 1990 des Nations Unies recommande l'application des *Principes directeurs pour l'utilisation des fichiers personnels informatisés*. Ce n'est pas un texte contraignant.

En troisième lieu, les recommandations de l'OCDE servent également de cadre juridique. Dans ses *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* du 23 septembre 1980, l'OCDE recommande cinq principes[5] : la limitation en matière de collecte, la qualité des données (finalité du traitement), la limite d'utilisation des données, les garanties de sécurité et la participation individuelle (celle des personnes faisant l'objet de traitement). Les *Lignes directrices* ont fait l'objet d'une révision adoptée le 11 juillet 2013 : parmi les modifications, on retient le renforcement de la responsabilité des entreprises et l'obligation des responsables de traitement de notifier les failles de sécurité[6].

4.2 LÉGISLATION SUISSE

La norme qui nous intéresse le plus sur la protection des données en Suisse est la loi fédérale sur la protection des données (LPD). Avant d'y revenir, nous allons d'abord, par ordre d'importance, explorer les autres normes traitant de près ou de loin à la protection des données en Suisse.

---

[5] http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonnesdecaracterepersonnel.htm

[6] http://www.cnil.fr/linstitution/actualite/article/article/l-ocde-revise-ses-lignes-directrices-en-matiere-de-vie-privee/

4.2.1 BASES CONSTITUTIONNELLES

L'art 13. Cst sur la protection de la sphère privée stipule :

> « 1. *Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent* ».
>
> « 2. *Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications.* »

L'article est inscrit dans la nouvelle Constitution de 1999. Dans son message du 20 novembre 1996, le Conseil fédéral appuie la nécessité d'intégrer la protection des données dans le chapitre des droits fondamentaux : « le droit à la protection des données personnelles (2e al.) constitue l'un des aspects du droit à la sphère privée. A l'ère de la société de l'information, il convient donc de l'énoncer expressément dans la constitution » (MCF 1996, p. 155). La protection des données s'appliquait en Suisse toutefois déjà auparavant *via* l'art. 8 CEDH et surtout la LPD, adoptée en 1992. Selon Meier (2010), la protection s'étend au-delà des « abus » mentionnés dans l'art. 13 al. 2 Cst : « elle comprend un véritable *droit* à l'autodétermination informationnelle, à savoir le droit de ne pas accepter un traitement qui ne correspond pas à la volonté exprimée » (§17), un droit « conçu à la fois comme une composante et une extension de la sphère privée plus largement protégée part l'art. 13 al. 1 Cst [...]) » (§18). Notons également les fonctions corrective et préventive du droit (§19), agissant respectivement lorsqu'il y a eu violation et postulant « une interdiction générale de traitement des informations, qui ne peut en principe être levée que par la personne concernée, aux conditions qu'elle-même aura fixées ou acceptées » (§19).

Comme il s'agit d'un droit fondamental, une restriction est possible en vertu de l'art. 36 Cst. qui rappelle que « *toute restriction d'un droit fondamental doit être fondée sur une base légale* » (al. 1), être justifié par un intérêt public (al. 2), respecter le principe de proportionnalité par rapport au but visé (al. 3) et ne pas violer l'essence du droit fondamental (al. 4). Selon Walter (cité dans Meier 2010, §21), « l'utilisation

d'informations demeure une condition de réalisation de la société. On ne peut l'éviter, mais elle doit être canalisée. Le droit de la protection des données sert cet objectif et assure à la personne le respect de son autonomie, de son individualité et de sa dignité ». Nous reviendrons plus tard (point 7.1.1) sur le « dilemme » de l'importance des données dans une société de l'information pour l'économie et la volonté des autorités (et des citoyens) de maintenir et renforcer la protection des données.

4.2.2 L'ARTICLE 28 CC

Depuis 1912, date de l'entrée en vigueur du Code civil, l'article 28 CC protège la vie privée. Il fut révisé en 1985 et stipule : «*Celui qui subit une atteinte illicite dans sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe*.»

La disposition est vague et les personnes dont les données étaient traitées autant que les personnes traitant les données se situaient dans un flou juridique, les premiers ne sachant pas quand et s'ils étaient lésés, les seconds n'ayant pas connaissance des conditions de conservation, d'exploitation, etc. des données (Meier 2010, §46 – 47). La jurisprudence a permis de préciser certains critères, mais globalement le flou demeurait, si bien que certaines organisations privées ont édicté elles-mêmes certaines règles (MCF 1988, p. 427).

4.2.3 LA LPD

Avant d'aborder les concepts-clés de la LPD, nous allons retracer l'historique de son adoption. Puis nous verrons les révisions que la loi a subies.

4.2.3.1 HISTORIQUE DE L'ADOPTION DE LA LPD

Une motion du conseiller national Bussey du 17 mars 1971 intitulée « Législation concernant l'utilisation des ordinateurs » (N II. 12. 72, Bussey) est l'instigatrice de la LPD. La motion, transformée en postulat en 1972 (Meier 2010, §176) met déjà en évidence la croissance exponentielle des outils technologies des ordinateurs, alors que ces derniers se trouvent à un état « primitif ». Il est notamment écrit :

> « Ce développement extraordinaire n'est pas le fruit d'un engouement passager, mais la conséquence logique des remarquables capacités de ces machines d'un nouveau genre. Ainsi, l'ordinateur peut enregistrer dans ses fichiers magnétiques des informations représentant des centaines de millions de lettres ou de chiffres, et les mettre instantanément à la disposition de nombreuses personnes, par l'intermédiaire de terminaux pouvant se situer à grande distance.
>
> Les mémoires de l'ordinateur permettent la création de véritables banques d'informations, qui peuvent par exemple regrouper un grand nombre de renseignements jusqu'alors dispersés, ayant trait à une personne ou à une entreprise. Si l'on peut admettre que nos administrations traiteront les renseignements accumulés avec la retenue nécessaire, il n'en va pas nécessairement de même des entreprises privées. »

On remarque donc la justification d'un encadrement législatif par l'avancement des nouvelles technologies de l'information et de la communication (NTIC), mais également l'idée que le traitement abusif des données est possible, notamment par les entreprises privées.

Deux initiatives parlementaires déposées par le conseiller national Gerwig le 22 mars 1977 suivent (Meier 2010, §177 ; MCF 1988, p. 434). La première insiste sur la nécessité d'adopter un article constitutionnel, la seconde énumère les exigences d'une loi sur la protection des données. Une commission est alors chargée de préparer un avant-projet qui sera accepté en 1984 et mis en consultation. Les conclusions de la consultation sont les suivantes : les points favorables sont notamment « l'institution d'un régime juridique commun aux traitements de données automatisés et aux traitements de données manuels, de la création d'une catégorie spéciale de données, « les données sensibles », de l'obligation de faire enregistrer certains types de fichiers, et de l'octroi aux personnes concernées d'un droit d'accès et de rectification » (MCF 1988, p. 435). Parmi les dispositions contestées, on évoque entre autres le principe d'une loi commune entre le secteur public et privé (Meier 2010, §184). De plus, les dispositions concernant le secteur privé ont reçu un accueil défavorable, surtout par les

organisations patronales, les organisations économiques (sauf celles en faveur des consommateurs) et les représentants des professions sociales (MCF 1988, p. 437).

Un projet aboutit le 28 mars 1988. Pendant les travaux parlementaires qui suivent, la Suisse est marquée par l'affaire dite « des fiches », où une enquête parlementaire révèle que l'Etat surveillait 900'000 citoyens, dont de nombreux affiliés à la gauche, ce qui n'a pas manqué d'imprégner les débats sur la protection des données. La loi est adoptée en votation finale le 19 juin 1992. Elle entre en vigueur le 1er juillet 1993. Parallèlement à la LPD, l'Ordonnance relative à la loi fédérale sur la protection des données (OLPD) entre également en vigueur. Elle contient les règles d'application de la LPD.

4.2.3.2 CARACTÉRISTIQUES DE LA LPD

Afin de comprendre comment agit la LPD, nous allons à présent présenter les principales caractéristiques de la loi. La présentation de la LPD qui suit n'est évidemment pas exhaustive, car ce n'est pas le but du travail. Il s'agit avant tout de montrer les grandes lignes de la loi et ses principales dispositions. Une mise en lumière particulière est faite en premier lieu sur les définitions, car il est important de comprendre précisément ce que les termes spécifiques à la protection des données veulent dire (nous les utilisons dans ce travail). En deuxième lieu, l'accent est mis sur les principes, car ils sont le cœur de la loi et se retrouvent également dans les textes internationaux.

a) But, champ d'application et définitions

L'art. 1 LPD précise le but de la loi qui, contrairement à ce que son nom indique, consiste à protéger la *personnalité* et non les données mêmes (Meier 2010, Bondallaz 2007). L'art.1 LPD stipule : « *La présente loi vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données* ». La LPD se rattache donc au droit de la personnalité[7] et non au droit à la propriété, qui aurait concerné des données au-delà du cadre personnel (Pedrazzini 1994, p. 21). Les « droits fondamentaux » font référence à la liberté personnelle, découlant du droit non écrit (Meier 2010, §336), mais ils s'incarnent à présent dans l'art. 13 Cst. Le postulat implicite de l'art. 1 LPD est l'interdiction de traitement de données personnelles sauf sous certaines conditions (Walter 1994, p. 43).

L'art. 2 LPD traite du champ d'application de la LPD. Les personnes pouvant faire l'objet d'un traitement se trouvent être les personnes physiques et les personnes morales. Le traitement peut être effectué par des personnes privées et des organes fédéraux. On voit ici le caractère spécifique de la LPD se situant à la convergence du droit public et privé. Le Conseil fédéral justifiait cette loi commune au privé et au public en 1988 dans son message par le caractère universel des atteintes contre la protection des données et que ses principes fondamentaux s'appliquent dans les deux secteurs (MCF 1988, p. 439). A noter que les organes cantonaux et communaux ne sont pas mentionnés, en raison de l'absence de base constitutionnelle (Meier 2010, §356).

L'art. 3 LPD donne les définitions des concepts engagés par rapport aux données personnelles. On retrouve des définitions similaires à l'art. 2 de la Conv. 108, ainsi que à l'art. 2 de la Directive 95/46/CE.

A propos du concept même de données, ce que nous pouvons observer en premier lieu de ces définitions sont le caractère synonyme de « données personnelles » et « données » (*ibid.*, §419). Celles-ci se rapportent à « *toutes les informations qui se rapportent à une personne*

[7] Sur la définition de la personnalité et la protection de celle-ci, voir Meier 2010 (§331 – 339).

identifiée ou identifiable » (art. 1 let. a LPD). Meier (§422) précise encore les caractères potentiels de ces données : celles-ci peuvent être ordinaires ou sensibles, objectives ou subjectives, à caractère confidentiel. De plus, la forme des données peut être indifférente, de même que son type de support. Quand on parle de données, il peut s'agir à titre d'exemple de données d'identification (identité, n° AVS, adresse postale, adresse électronique, nom), de données physiques (taille, poids, âge, origine ethnique), de données médicales (état de santé, vaccinations), de données sociales (niveau d'études, profession, état civil, nombre d'enfants), de données judiciaires, de données financières, mais encore, plus subjectivement, des opinions personnelles, des préférences, des centres d'intérêts, des croyances religieuses, des données comportementales (fréquence d'utilisation des transports publics, données de connexion sur Internet, consommation d'électricité), des données géographiques (géolocalisation, utilisation d'une carte de crédit) ou des données relationnelles (réseau d'amis, participation à des associations), etc. (Rochelandet 2010, p. 15) ; la liste peut être très longue. Notons que les données anonymisées ne sont pas des données personnelles, celles qui le sont partiellement le sont ou le ne sont pas au sens de la LPD, selon les moyens qui doivent être mis en œuvre afin de ré-identifier une personne. Une personne est dite « identifiée » lorsqu'elle est directement liée à des informations la concernant, la personne est « identifiable » lorsque « par corrélation indirecte d'informations tirées des circonstances ou du contexte, il est possible de l'identifier avec les moyens technologiques disponibles » (Meier 2010, §432).

La personne concernée (art. 3 let. b LPD) est la personne faisant l'objet d'un traitement de données. Elle est soit une personne physique, soit une personne morale.

Les données sensibles sont définies à l'art. 3 let. c LPD. La loi entend par données sensibles, « *les données personnelles sur 1. les opinions ou activités religieuses, philosophiques, politiques ou syndicales, 2. la santé, la sphère intime ou l'appartenance à une race, 3. des mesures d'aide sociale, 4. des poursuites ou sanctions pénales et administratives.* » Cette énumération est exhaustive (*ibid.*, §475),

indépendante du « potentiel d'atteinte à la personnalité en cas de traitement illicite » (*ibid.*, §474). Les données sensibles sont une catégorie à part des données personnelles, elles font l'objet de dispositions spécifiques dans la LPD (par exemple l'obligation pour un maître du fichier de déclarer ses fichiers au PFPDT s'il y a traitement de données sensibles [art. 11a al. 3 let. a LPD]). En somme, on ne traite pas les données non-sensibles et sensibles de la même façon.

Le profil de la personnalité est « *un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique* » (art. 3 let. d LPD). Lorsqu'on assemble des données, il est possible de dresser un profil. Actuellement, les procédés de *data mining*, corollaire au phénomène des *big data* (voir point 6.1.1) offrent cette possibilité. Selon le Conseil fédéral, « les profils de la personnalité privent-ils la personne concernée de la liberté de donner d'elle-même l'image qu'elle souhaite » (MCF 1988, p. 454), ce qui porte atteinte à son épanouissement.

La LPD définit par traitement « *toute opération relative à des données personnelles - quels que soient les moyens et procédés utilisés - notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données* » (art. 3 let. e LPD). Une telle définition possède plusieurs caractéristiques. Selon Meier (2010, §521), elle est « *exemplative* » par l'utilisation du « notamment », « évolutive » en raison de son caractère neutre technologiquement, et surtout très large. Elle décrit également les étapes de traitement de données dans un ordre chronologique.

La communication est définie comme « *le fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant* » (art. 3 let. f LPD). Le Conseil fédéral avait indiqué qu'il s'agissait de « la phase la plus dangereuse » (MCF 1988, p. 455). Il s'agit de la possibilité pour un tiers de prendre connaissance de données personnelles (Meier 2010, §541). La communication peut être active (par exemple la transmission ou la publication) ou passive (par exemple une autorisation de consultation), volontaire ou forcée (par une autre loi) (*ibid.*, p. §541 – 548).

L'art. 3 let. g LPD définit le fichier comme étant « t*out ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée* ». L'ensemble de données, non défini dans la loi, exige que « les données doivent être agrégées en un ensemble qui concerne [...] *plus d'une personne* » (*ibid*., §562). De plus, « il y a lieu d'exiger que les données que les données ainsi rassemblées ne le soient pas par un hasard technique ou matériel, mais qu'elles présentent un *lien thématique logique* » (*ibid*., §574). C'est la fonction de fichier qui est importante, sinon tout support contenant des données personnelles serait un fichier, soit les serveurs du monde entier.

L'organe fédéral est défini comme « *l'autorité ou le service fédéral ainsi que la personne en tant qu'elle est chargée d'une tâche de la Confédération* » (art. 3 let. h LPD). On notera que les compétences du PFPDT diffèrent selon à ce qu'un traitement soit effectué par un organe fédéral ou une personne privée (voir art. 27 LPD). Les organes fédéraux sont les départements, offices et leurs subdivisions, les ex-régies fédérales, les commandements militaires, les autorités judiciaires fédérales, les autorités indépendantes et les personnes privées effectuant une tâche pour la Confédération (MCF 1988, p. 453 ; Meier 2010, §365). Les cantons et communes effectuant exécutant une tâche fédérale ne sont pas des organes fédéraux, mais ils sont soumis aux dispositions cantonales (la LPD exige néanmoins un standard minimum à l'art. 37).

Le maître du fichier défini à l'art. 3 let. i LPD est « *la personne privée ou l'organe fédéral qui décide du but et du contenu du fichier* ». La personne privée peut être une personne physique ou morale. Le maître du fichier décide du but et du contenu d'un fichier, peu importe qu'il dispose du contenu du fichier (MCF 1988, p. 456). La question de la délégation à un tiers survient : il peut être considéré comme maître du fichier ou non selon les situations. Une entreprise mandatant un tiers dont l'activité consiste « à mettre à disposition l'infrastructure technique permettant de faire subir à un ensemble préconstitué de données un traitement précis » (MCF 1988, p. 456) reste maître du fichier. Mais dans le cas où le tiers établit le fichier et les opérations qui l'entourent (Meier 2010, §590), par exemple un institut réalisant une étude de marché ou un détective privé (MCF 1988, p. 456), le tiers est le maître

du fichier. A l'heure du *cloud computing*[8], la question du maître du fichier devient de plus en plus épineuse. Notons que la Directive 95/46/CE de l'UE évoque la notion de « responsable de traitement » et pas celle de maître du fichier, tout comme certains cantons en Suisse, un terme « plus explicite » selon Meier (2010, §580). Dans la suite de ce travail, les deux expressions seront utilisées.

La dernière définition de l'art. 3 LPD porte sur la loi au sens formel. Elle comprend : « *1. lois fédérales, 2. résolutions d'organisations internationales contraignantes pour la Suisse et traités de droit international approuvés par l'Assemblée fédérale et comportant des règles de droit.* » (art. 3 LPD let. j). Cette définition est importante concernant d'autres dispositions de la LPD, notamment celles sur le traitement de données sensibles affirmant qu'il peut être effectif sous motif d'une *loi formelle*, entre autres (art. 17 al. 2 et art. 19 al. 3 LPD).

b) Principes généraux de protection des données

L'art. 4 ouvrant la section est considéré comme le « noyau dur » de la loi (MCF 1998, p. 457), car il définit les principes fondamentaux du traitement des données. Souvent, une infraction à la LPD correspond à la transgression de ces principes. Définis de manière très large, certains de ces principes sont très connus, d'autres concernent plus spécifiquement la protection des données. Par rapport à l'amélioration des moyens technologiques actuels, pour Meier, « [ces principes] doivent être respectés non seulement pour chaque traitement individuel de données, mais aussi dans la politique globale de traitement mise en œuvre » (2010, §632) ; la création, la conservation et la destruction de tout fichier doit être questionné, « même si les capacités de stockage informatique sont quasi-illimitées » (§632).

Selon l'art. 4 al.1 LPD, « t*out traitement de données doit être licite* ». Le traitement doit reposer sur une base juridique, comme ce qui se fait dans le secteur public (Bondallaz 2007, §543). Ainsi, seront illicites l'obtention de données par la violence, la menace, en violation du secret de fonction ou encore l'intrusion dans un domaine privé, l'intrusion dans

[8] Par cette expression, nous entendons l'externalisation de services d'une organisation à des serveurs délocalisés pour effectuer un traitement d'informations.

un système informatique, l'utilisation de méthodes de hameçonnage informatique (*pishing*), entre autres. Ces comportements illicites sont du registre du droit pénal.

L'art. 4 al. 2 LPD rappelle le principe de bonne foi. Il stipule que tout traitement de données « *doit être effectué conformément aux principes de la bonne foi et de la proportionnalité* ». Il s'agit d'un élément éthique fondamental de la LPD et du droit suisse, étroitement lié au principe de licéité. Il faut que les personnes concernées soient correctement informées du traitement leur concernant et qu'il ne soit réalisé à leur insu (MCF 1988, p. 457) ; en ce sens la bonne foi est également liée au principe de transparence (Meier 2010, §649 ; Bondallaz 2007, §544). A noter également que le responsable de traitement doit informer les personnes concernées (sa clientèle) en cas de défaillance de sécurité, un vol de données par exemple (Meier 2010, p. 266 – 267).

Quant à la proportionnalité, elle correspond à l'adage « la fin ne justifie *pas* les moyens ». Elle se compose de trois éléments : premièrement, l'aptitude, un moyen doit être apte à atteindre un but défini ; deuxièmement, la nécessité, il s'agit d'utiliser les moyens strictement nécessaires à l'atteinte d'un but, sans être excessif ; enfin, la proportionnalité au sens étroit, qui indique qu'un moyen doit être mesuré, proportionné, par rapport au but à atteindre (Mahon 2010, §49). Il s'agit selon Meier du principe « l*e plus souvent violé dans la pratique* » (2010, §669). Selon le PFPDT, la proportionnalité exige que « la collecte et le traitement impliqueront le moins de données personnelles possible, mais jamais plus que le strict nécessaire »[9], il s'agit, pour le monde numérique, du principe de « l'utilisation économe » des données (Bondallaz 2007, §545). Comme nous le verrons plus loin, la proportionnalité est liée au concept de *privacy by design* (point 7.3).

Selon l'art. 4 al. 3 LPD, « l*es données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances* ». Le traitement de données doit correspondre à la finalité déterminée (on parle de détermination du but) et cette finalité ne peut être modifiée (imputabilité

[9]http://www.edoeb.admin.ch/datenschutz/00618/00802/00812/index.html?lang=fr

du but), sauf si une disposition légale le permet. A l'heure des *big data*, où il est possible de générer et transférer une quantité gigantesque de données, la question de la finalité prend une importance certaine.

L'art. 4 al. 4 LPD introduit le principe de reconnaissabilité dans les termes suivants : « *la collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée* ». Pour les organes fédéraux, il s'agit d'un devoir d'information du traitement des données (art. 18a LPD) ; c'est le cas pour les personnes privées dans le cas du traitement de données sensibles (art. 14 LPD). La collecte doit être reconnaissable ; en connaissance de ceci, une personne pourra demander un accès à ses données au maître du fichier (art. 8 LPD). Selon le rapport sur la révision de la LPD, les circonstances et la conformité aux principes de la bonne foi et de la proportionnalité font qu'une collecte soit reconnaissable (PFPDT 2006, p. 3). Par exemple, un questionnaire pour un concours doit préciser que les données récoltées le soient pour un autre but (par exemple marketing) que le concours lui-même.

L'art. 4 al. 5 LPD porte sur le consentement et stipule : « *Lorsque son consentement est requis pour justifier le traitement de données personnelles la concernant, la personne concernée ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée. Lorsqu'il s'agit de données sensibles et de profils de la personnalité, son consentement doit être au surplus explicite* ». Le rapport sur la révision de la LPD rappelle que le consentement doit être libre (pas de pression ou menace, entre autres) et informé (avoir les connaissances sur les conséquences d'un refus par exemple) (PFPDT 2006, p. 4).

L'art. 5 al. 1 et l'art. 7 al. 1 LPD respectivement sur l'exactitude et la sécurité des données peuvent également être considérés comme des principes, d'ailleurs l'art. 12 LPD les mentionne comme principes au même titre que ceux énoncés à l'art. 4. LPD.

Selon l'art. 5 al. 1 LPD, « *celui qui traite des données personnelles doit s'assurer qu'elles sont correctes. Il prend toute mesure appropriée permettant d'effacer ou de rectifier les données inexactes ou incomplètes*

au regard des finalités pour lesquelles elles sont collectées ou traitées ». L'al. 2 stipule que toute personne peut demander une rectification. Le devoir d'exactitude est défini à l'art. 5, l'auteur de traitement d'un fichier doit s'assurer que les données sont exactes et prendre les mesures pour les rectifier s'ils sont complètes ou inégales. Deux objectifs se déploient dans cet article : pour la personne concernée, éviter une atteinte à la personnalité en raison de données fausses, par exemple dans les questions d'octroi de crédit (Meier 2010, §743), et pour le responsable de traitement, pouvoir utiliser des données exactes, donc à valeur économique (*ibid*.).

L'art. 7 al. 1 LPD stipule : « *les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées* ». Malgré l'impossibilité d'atteindre une sécurité absolue (Meier 2010, §782), le maître du fichier doit sécuriser les données grâce à des mesures jugées suffisantes, sans quoi il entre en violation de la LPD. Les menaces sont variées : elles peuvent aller à la perte d'un support physique contenant des données (par exemple des ordinateurs, des clés USB) à une faille informatique laissant permettant à des individus mal intentionnés de capter des données. Notons une particularité de ce principe : il accorde une importance plus conséquente au contenu des données même que les autres principes généraux (Meier 2010, §785).

c) Le registre des fichiers

En vertu de l'art. 11a, al. 1 LPD « *le préposé tient un registre des fichiers accessible en ligne. Toute personne peut consulter ce registre* ». Le registre est issu de la déclaration des fichiers par les personnes privées et les organes fédéraux. Quand il y a traitement de données, ils sont tenus de remplir une déclaration contenant, en vertu de l'art. 3 OLPD, les informations suivantes : le nom et l'adresse du maître du fichier, le nom et la dénomination complète du fichier, la personne auprès de laquelle peut être exercé le droit d'accès, le but du fichier, les catégories de données personnelles traitées, les catégories de destinataires des données et les catégories de participants au fichier, c’est-à-dire les tiers qui sont en droit d’introduire des données dans le fichier ou d’y procéder à des mutations. Le registre ainsi que les

formulaires de déclaration sont disponibles en ligne sur le site du PFPDT[10].

En reprenant la typologie de Meier (2010, §1465), les buts du registre sont « d'assurer la transparence de certaines données ; de facilité l'exercice du droit d'accès [art. 8 et 9 LPD] ; de permettre au PFPDT d'avoir une vue des traitements de données et de pouvoir le cas échéant intervenir selon les art. 27 et 29 LPD si le traitement n'est pas conforme à la protection des données ». Les organes fédéraux sont obligatoirement tenus de déclarer les fichiers (art. 11 al. 2 LPD), tandis que pour les personnes privées, elles sont tenues de le faire si « *elles traitent régulièrement des données sensibles ou des profils de la personnalité* » (art. 11a al. 3 let. a LPD) et si « *elles communiquent régulièrement des données personnelles à des tiers* » (art. 11a al. 3 let. b LPD), des conditions qui font intervenir respectivement le contenu des données et le traitement des données. L'art 11a al. 5 LPD décrit les conditions pour lesquelles le maître du fichier n'est pas tenu de déclarer ses fichiers. En bref, il s'agit des données traitées en vertu d'une obligation légale (par exemple, le secret professionnel), des traitements désignés par le Conseil fédéral comme n'étant pas susceptibles de menacer le droit des personnes concernées (ils sont décrits exhaustivement dans l'art. 4 OLPD), l'utilisation des fichiers pour la publication dans les médias ou par un journaliste comme instrument de travail personnel, des traitements par un maître du fichier ayant fait recours à un conseiller à la protection des données ou s'il a fait reçu un label de qualité suite à un processus de certification (dans ces deux derniers cas, il s'agit d'un « *allègement administratif* en matière de déclaration de fichiers » [Meier 2010, §1493]).

d) La communication transfrontière des données

L'art. 6 LPD contient les dispositions relatives à la communication transfrontière des données. Aujourd'hui, les données circulent entre les Etats pour un très grand nombre de raisons, qu'elles soient économiques (globalisation, délocalisation, centralisation des entreprises par exemple) ou relevant de la sécurité (lutte contre le terrorisme par exemple).

[10] http://www.edoeb.admin.ch/datenschutz/00626/00743/00858/index.html?lang=fr

Sachant que la législation suisse ne s'applique que sur le territoire suisse, « cette situation *empêche de facto la personne concernée d'exercer son droit à l'autodétermination informationnelle* » (*ibid*., §1248). D'où la nécessité de dispositions dans la loi suisse statuant sur les transferts effectués par les organisations sous législation nationale envers d'autres Etats. Comme évoqué précédemment, la Convention 108 fut pensée dans un but d'harmonisation de la législation entre les Parties pour permettre les flux transfrontières. L'art. 6 LPD s'applique donc à l'exportation des données à partir de la Suisse (*ibid*., §1268). Les deux principes de la communication des données à l'étranger sont d'une part l'existence d'un niveau adéquat de protection dans l'Etat en question et d'autre part une interdiction de communication quand la personnalité de la personne concernée est gravement menacée (ce qui découlerait d'une législation non adéquate ou d'une non-effectivité d'une législation appropriée sur le papier [Walter 2009, p.122]). L'art. 6 al. 2 LPD détaille les conditions permettant une communication en dépit d'une législation adéquate. En bref et pour reprendre le classement fait par Walter (2009, p.124 – 134), il s'agit de l'existence de clauses contractuelles, de règles internes des entreprises destinataires du transfert ou de code de conduite (dès lors qu'il s'agit de garanties effectives). Un exemple est celui du *Safe Harbor* ou « sphère de sécurité » ; il s'agit d'une garantie spéciale conclue entre la Suisse et les Etats-Unis, analogue à ce qui existe entre l'UE et les Etats-Unis. Ces derniers n'ont pas un niveau de législation adéquat selon les normes suisses ; pour pallier cela, les entreprises américaines peuvent souscrire librement à des principes de protection des données supérieurs à ceux en vigueur aux Etats-Unis, cependant moins sévères que les normes suisses et européennes (Walter 2009, p. 126). Des dérogations spécifiques sont également possibles (consentement de la personne concernée, existence d'un intérêt public prépondérant notamment). Les garanties doivent être annoncées au PFPDT, les modalités du devoir d'information étant réglées par le Conseil fédéral (art. 6 al. 3 LPD).

Le PFPDT propose sur son site une explication de la communication transfrontière des données en 24 questions (c'est document qui serait

plutôt à destination des entreprises)[11]. Il répond notamment à une question souvent demandée par rapport à ce sujet : la publication des données sur Internet. Il rappelle alors qu'en vertu de l'art. 5 OLPD, « *la publication de données personnelles au moyen de services d'information et de communication automatisés afin d'informer le public n'est pas assimilée à une communication à l'étranger* ». Cependant, « la collecte et la communication de données qui ne sont pas généralement accessibles au public (par ex. *cookies*, adresse IP) par le biais de l'Internet peuvent aussi remplir les critères d'un flux transfrontière de données » (Walter 2009, p. 119).

e) Le préposé fédéral à la protection des données et à la transparence

L'institution d'un préposé, son statut et sa fonction sont traitées aux art. 25, 26 et 26a LPD. Le PFPDT est nommé par le Conseil fédéral pour une durée de quatre ans et sa nomination demande l'approbation de l'Assemblée fédérale. En vertu de l'art 26, al. 3 « l*e préposé exerce ses fonctions de manière indépendante et sans recevoir d'instructions de la part d'une autorité. Il est rattaché administrativement à la Chancellerie fédérale* ». Parallèlement à la mise en œuvre de la Décision-cadre du 27 novembre 2008, l'indépendance du préposé a été renforcée. Le préposé actuel est Hanspeter Thür, depuis 2001 (également préposé à la transparence depuis 2006), le préposé suppléant est Jean-Philippe Walter. A noter que ce dernier vient également d'être élu président du Comité consultatif de la convention 108 du Conseil de l'Europe (voir point 4.3.3) pour un troisième mandat (période 2014 – 2016)[12].

Le rôle du PFPDT diffère dans sa marge d'action que ce soit sur le domaine public ou privé. Dans les attributions qui concernent les deux secteurs, le PFPDT a un rôle de conseiller sur la question de la protection des données ; par extension, il s'agit d'un rôle de médiation non inscrit formellement dans la loi (Cottier 1994, p. 215). Il tient également le registre du fichier, « pierre angulaire » de son activité (MCF 1988, p. 463). Le préposé possède un rôle dans la communication transfrontière des données, où il fait un examen de la législation d'autres

[11] http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=fr
[12] http://www.afapdp.org/archives/2559

Etats pour connaître son adéquation au droit suisse dans le cas d'un transfert. Le préposé émet également des recommandations suite à un établissement des faits effectué à la suite d'une demande de consultation d'un tiers. C'est le cas pour le secteur public depuis l'entrée en vigueur de la loi (art. 27 al. 5 et 6 LPD). Si la recommandation est ignorée, le département concerné doit donner une décision : s'il suit le PFPDT, l'office peut faire recours auprès du TAF ; s'il ne suit pas le PFPDT, ce dernier peut faire recours au TAF (Walter, 2012b, p. 27). Depuis la novelle de 2006, le PFPDT peut porter une affaire devant le TAF dans le secteur privé si une recommandation émise est rejetée ou non suivie (art. 29 al. 4 LPD) lorsque « *une méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes (erreur de système)* » (art. 29 al.1 let. a LPD).

Spécifiquement au secteur privé, outre les tâches générales décrites plus haut, le PFPDT n'a qu'un rôle de conseiller. Cette absence de prérogative étendue fut justifiée par une autonomie de la volonté de la personne : « les atteintes à la personnalité causées par des traitements effectués par des personnes privées sont, dans la conception du législateur, l'affaire de la personne concernée, laquelle est renvoyée vers le juge civil » (Cottier 1994, p. 211). Le conseil proféré par le PFPDT est d'ordre général, et non individuel (Meier 2010, §1888), sur des aspects juridiques et techniques. Le préposé peut également émettre des directives concernant les certifications (cf. OCPD), c'est-à-dire reconnaître les organismes de certification en vue de l'apposition de label aux entreprises. Le préposé n'a pas la compétence de donner des sanctions pénales ou administratives aux contrevenants, contrairement à une partie de ses homologues européens comme la CNIL française.

Le PFPDT a un rôle actif de surveillance des organes fédéraux (art. 27 LPD). Il s'agit pour lui de pouvoir enquêter sur les activités des organes fédéraux – sauf sur le Conseil fédéral – avec les possibilités d'établir des faits, demander des renseignements et émettre des recommandations.

Depuis l'entrée en vigueur de la loi fédérale sur la transparence (LTrans) le 1er juillet 2006, le préposé est également préposé à la transparence.

4.2.3.3 LES RÉVISIONS DE LA LPD

a) La révision de 2006

Une première impulsion de révision de la LPD commence au début des années 2000. La révision est motivée par deux interventions parlementaires et a notamment pour but d'adapter le Protocole additionnel de la Conv. 108 (STE n° 181). Les motions de la Commission de gestion du Conseil des Etats du 17 novembre 1998 « Liaisons "on-line". Renforcer la protection pour les données personnelles » (98.3529) et de la Commission des affaires juridiques du Conseil des Etats du 28 janvier 2000 « Renforcement de la transparence lors de la collecte des données personnelles » (00.3000) demandent respectivement une révision de la LPD en vue d'intégrer une base légale concernant les liaisons « on-line » et l'inscription dans la LPD l'obligation pour les maîtres du fichier d'informer les personnes concernées du traitement de données sensibles (MCF 2003, p. 1919 – 1920). Le PFPD a estimé que c'était l'occasion de moderniser la LPD ; une modernisation qui devait, selon la typologie de Meier (2010, §240), renforcer à la fois la responsabilité des personnes concernées (droit d'information, consentement) par les traitements et les responsables de traitement (devoir d'information), inciter au recours aux technologies permettant une meilleure protection des données, harmoniser les législations suisse et européenne, diminuer les contraintes bureaucratiques (suppression de la déclaration des flux transfrontières), renforcer le contrôle de la protection des données et renforcer les compétences du préposé. Un avant-projet est mis en consultation entre septembre 2001 et janvier 2002 ; il est notamment marqué par un grand soutien, sauf des milieux économiques souhaitant une stricte application des deux motions, sans aller plus loin (MCF 2003, p. 1934).

La novelle est finalement adoptée le 24 mars 2006 et entrée en vigueur le 1er janvier 2008. L'OLPD fut révisée en conséquence et est entrée en vigueur le 28 septembre 2007. Dans les grandes lignes, la révision se caractérise par une importance plus grande accordée à la transparence, l'obligation d'informer les personnes concernées lors de la collecte de données sensibles ou l'établissement d'un profil de la personnalité, elle abandonne la déclaration des transferts de fichiers à l'étranger et elle met

en place deux nouvelles dispositions incitatives, l'une permettant la certification *via* des labels des systèmes de traitement des données (l'ordonnance sur les certifications en matière de protection des données (OCPD) est adoptée à ce propos par le Conseil fédéral), l'autre permettant aux maîtres du fichier de faire appel à un conseiller à la protection des données. Parallèlement à la révision, la loi du 17 décembre 2004 sur le principe de la transparence de l'administration (Ltrans)[13] entre en vigueur le 1er juillet 2006. Le PFPD devient le PFPDT.

La révision a renforcé l'efficacité de la LPD, mais fut critiquée par la doctrine (voir Bondallaz 2008, Cottier 2007, Meier 2007), notamment en ce qui concerne le pouvoir de sanction, absent, du PFPDT.

b) La révision de 2008

Le Conseil de l'Union européenne adopte la Décision-cadre 2008/977/JAI. Celle-ci traite de la coopération en matière pénale par rapport au traitement des données personnelles. S'agissant d'un développement de l'acquis de Schengen, le Conseil fédéral approuve la reprise de la décision-cadre et décide le 13 mai 2009 d'ouvrir la procédure de consultation. La révision aboutit à la modification de dispositions dans plusieurs lois, dont la LPD, la LEIS et le CP. Sur la LPD, la révision concerne le devoir d'information lors de la collecte de données, différenciée selon que ce soit une personne privée ou un organe fédéral. La révision est également l'occasion pour le Conseil fédéral d'intégrer les recommandations qu'avaient effectuées l'UE pendant l'évaluation de la réglementation suisse en 2008 (Meier 2010, §266) et renforce l'indépendance du PFPDT sur les modalités de sa nomination, du renouvellement de sa fonction et de ses ressources[14].

Suite à l'évaluation législative ayant eu cours en 2010 et 2011 et les travaux actuels par le groupe de travail (voir point suivant), une prochaine révision de la LPD est à envisager.

[13] RS 152.3
[14] Sur l'effectivité de l'indépendance du PFPDT, voir Cottier (2011).

4.3 L'ÉTAT DES TRAVAUX SUR LA RENFORCEMENT DE LA PROTECTION DES DONNÉES EN SUISSE ET EN EUROPE

4.3.1 L'ÉVALUATION DE LA LPD

L'OFJ a mené une évaluation de l'efficacité de la LPD en 2010 et 2011. L'évaluation s'est appuyée sur 28 entretiens avec des experts en droit et technologies, une étude de cas des publications du PFPDT, une enquête sur 1014 personnes concernant leurs représentation de la protection des données, une étude de la jurisprudence et enfin une analyse comparative de la protection des données dans 10 pays (MCF 2011, p. 260). L'évaluation a été réalisée par une le bureau Vatter AG (Berne), l'Institut de droit européen de l'Université de Fribourg et l'Institut DemoScope, sous la supervision de l'OFJ et un groupe de travail constitué d'universitaires, d'un avocat et de représentants de l'administration fédérale, de l'économie, de Privatim (association des commissaires suisses à la protection des données) et du PFPDT (Walter 2012a). Une partie des résultats est reprise au point 6 sur l'analyse des enjeux actuels de protection des données.

De manière générale, les conclusions du rapport estiment qu'une révision de la LPD est nécessaire, malgré une relative efficacité jusque-là, la loi ne saura faire face à l'évolution technologique caractérisée par les puissants moyens de traitement de données. Suite au rapport, le Conseil fédéral détermine cinq pistes d'action pour une future révision (MCF 2011, p. 268) :

- une protection des données plus en amont
- une meilleure sensibilisation des personnes concernées
- une amélioration de la transparence
- une amélioration du contrôle et de la maîtrise des données
- une protection des mineurs

Le Conseil fédéral précise également qu'un regard attentif envers les travaux réalisés dans le cadre de l'UE sera nécessaire. D'ailleurs, comme nous le verrons au point suivant, les travaux sur une révision du régime de protection des données dans l'UE et le Conseil de l'Europe font

ressortir des problématiques et des solutions semblables à celles de la Suisse.

Suite à cette évaluation, le DFJP a été mandaté par le Conseil fédéral pour analyser « l'opportunité de renforcer la législation en matière de protection des données »[15]. A cette fin, un groupe d'accompagnement a été constitué ; ce dernier est constitué d'experts en protection des données, d'universitaires et représentants des milieux économiques. Avec le DFJP, il devrait sortir un rapport cette année ou l'année suivante sur la nécessité et les moyens de réformer la LPD.

Alors que les procédures de cette évaluation avaient commencées en printemps 2010, deux postulats sont transmis au Conseil national par Antonio Hodgers (« Adapter la loi sur la protection des données aux nouvelles technologies », postulat 10.3383) et Jean-Pierre Graber (« Atteintes à la sphère privée et menaces indirectes sur les libertés individuelles », postulat 10.3651) respectivement les 8 juin et 14 septembre 2010. Les deux font mention d'une nécessaire adaptation de la LPD au motif des évolutions technologiques incontrôlables. Les objectifs définis par le Conseil fédéral dans l'optique d'une future révision de la LPD sont une réponse à ces postulats.

4.3.2 RÈGLEMENT ET DIRECTIVE EUROPÉENS

Le 12 mars 2014, le Parlement européen a adopté en première lecture la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) par 621 voix pour, 10 contre et 22 absentions. Ce règlement vise à remplacer la Directive 95/46/CE, datant d'il y a presque 20 ans, et s'en inspire largement. La différence entre un règlement et une directive est que la première s'applique à la lettre dans tous les Etats membres de l'UE, tandis que la directive laisse aux nations une marge d'interprétation.

[15] https://www.bj.admin.ch/content/bj/fr/home/themen/staat_und_buerger/gesetzgebung/datenschutzstaerkung.html

Le projet de règlement a été publié le 25 janvier 2012 par la vice-présidente de la Commission européenne Viviane Reding. Puis l'été 2013 a été marqué par le scandale PRISM, révélé par l'informaticien Edward Snowden et les journaux *The Washington Post* et *The Guardian* et caractérisé par l'utilisation par la NSA des données stockées chez au moins neuf grandes entreprises américaines (Google, Facebook, Microsoft, Apple, YouTube, AOL, Yahoo!, Skype et PalTalk) pour des raisons de lutte contre le terrorisme. A partir de ce moment, la Commission a décidé de resserrer l'agenda[16]. Le 20 octobre 2013, la Commission Libertés civiles, justice et affaires intérieures (LIBE) du Parlement européen a approuvé le projet, qui a ensuite été soumis aux eurodéputés le 12 mars 2014. Le règlement passe à présent dans les mains du Conseil de l'UE, dans le cadre de la procédure de codécision.

Les principaux points du règlement sont les suivants :

– le renforcement des obligations des responsables de traitement avec l'introduction de la protection de la vie privée dès la conception (équivalent de la *privacy by design*) ;
– le renforcement du droit des personnes concernées avec notamment l'introduction du droit à l'oubli numérique[17] ;
– l'introduction des analyses d'impact préalables à certains traitements de données ;

[16]Notons que l'UE était au courant de cette opération surveillance (voir l'article en ligne de Kallenborn [2013]), sachant que l'espionnage de la NSA s'inscrit dans une base légale américaine (*Foreign Intelligence Surveillance Act Amendments* Act, spécifiquement l'art. 702) étendue pour cinq ans en décembre 2012. L'indignation européenne face à l'existence d'un programme de surveillance de la NSA relève plutôt de l'ampleur du phénomène.

[17]Dans un arrêt publié le 13 mai 2014, la Cour de justice de l'Union européenne (CJUE) a estimé que : « L'exploitant d'un moteur de recherche sur Internet est responsable du traitement qu'il effectue des données à caractère personnel qui apparaissent sur des pages web publiées par des tiers » (Le document est disponible à l'adresse suivante : http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070fr.pdf). Suite à l'arrêt, Google a mis en place un formulaire permettant un déréférencement le 30 mai 2014 et Microsoft est en train de préparer un processus similaire pour son moteur de recherche Bing. Google a enregistré plus de 70'000 requêtes en un mois (Voir http://www.hebdo.ch/news/politique/google-re%C3%A7u-70000-demandes-de-droit-%C3%A0-loubli-en-un-mois).

- l'introduction d'un délégué à la protection des données aux entreprises sous certaines conditions ;
- l'applicabilité de la loi pour « tout acteur hors de l'UE qui proposerait des biens ou des services, payants ou gratuits, à des personnes résidant dans l'Union, ou qui profilerait ces personnes » (Mattatia 2013). En outre, « [a]fin de mieux protéger les citoyens européens contre des activités de surveillance massive, telles que celles dévoilées depuis juin 2013, les députés ont modifié les dispositions : avant de communiquer les données personnelles de citoyens européens à un pays tiers, toute entreprise (par exemple un moteur de recherche, un réseau social ou un fournisseur de services d'informatique en nuage) serait tenue de demander une autorisation préalable à une autorité nationale de protection des données dans l'UE. Les entreprises devraient également informer la personne concernée d'une telle demande »[18] ;
- le renforcement du rôle des autorités de protection des données, avec notamment l'introduction de possibilités de sanction dissuasives (5 % du chiffre d'affaire ou 100 millions d'euros d'amende pour une entreprise), de leur indépendance et de la coopération entre eux.

Une nouvelle directive est également à l'étude. Affichant des objectifs et dispositions similaires au projet de règlement européen, elle se trouve « en retrait par rapport au cadre juridique européen général qui est envisagé » (Guérin-François 2012, p. 26). Sans entrer dans les détails, notons une plus grande harmonisation des normes entre les Etats membres, soit la garantie de niveau de protection adéquat et une meilleure coopération entre eux (Walter 2012c). Il s'agit également d'instaurer un « régime spécial tenant compte de la nature particulière des activités répressives » (*ibid.*, p. 12).

En plus de l'approbation du projet de règlement européen, le Parlement a adopté une résolution visant à mettre fin à la surveillance massive, en

[18] http://www.europarl.europa.eu/news/fr/news-room/content/20140307IPR38204/html/Des-r%C3%A8gles-plus-strictes-pour-prot%C3%A9ger-la-vie-priv%C3%A9e-%C3%A0-l%27%C3%A8re-num%C3%A9rique

particulier des Etats-Unis. La résolution[19] demande notamment la suspension des accords « Safe Harbor » entre l'UE et les Etats-Unis, sous prétexte que la lutte contre le terrorisme ne devrait pas engendrer un trop gros dispositif de surveillance, et un appel à ce que l'Europe cherche à développer ses propres solutions informatiques, alternatives aux offres américaines.

4.3.3 MODERNISATION DE LA CONVENTION 108

La modernisation de la Conv. 108 est en cours de consultation, réalisée par le Comité conventionnel de la Conv. 108 (dit le Comité T-PD) . Les principaux changements se font sous l'égide de la neutralité technologique, des principes fondateurs de la protection des données, de la cohérence entre la juridiction de la Convention et celle de l'UE et le maintien de la portée générale applicable à toutes les Parties[20]. Dans les grandes lignes, les changements consistent à modifier les points présentés ci-dessous (de Terwangne 2012).

Premièrement, concernant les définitions, la nouvelle version de la Conv. 108 prévoit de remplacer le terme de « maître du fichier » par « responsable de traitement » et abandonne la définition du « fichier automatisé » ; en revanche, elle ajoute deux nouvelles définitions, celles de « destinataire » (la personne physique ou morale qui reçoit) et de « sous-traitant » (la personne physique ou morale agissant pour le compte d'un responsable de traitement).

Deuxièmement, sur le champ d'application, le projet prévoit de mettre une limite à l'application de la Conv. 108 lorsqu'il s'agit de traitement de données par une personne physique dans le cadre privé. Cette exception serait valable sauf s'il existe une intention de la personne à rendre des données accessibles « à des personnes ne relevant pas de la sphère personnelle » (art. 3, al. 1*bis* du projet de Conv. 108).

[19] Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI))

[20] http://www.edoeb.admin.ch/datenschutz/00628/00665/00667/index.html?lang=fr

Troisièmement, il s'agit d'inclure le principe de proportionnalité dans les principes de protection. Il n'existe pas dans la présente Conv. 108 ; il est également possible de l'appliquer en parallèle avec le principe de minimisation des données[21].

Quatrièmement, concernant les données sensibles, le projet ajoute à la liste pré-établie les données génétiques (l'ADN étant unique à chaque individu – sauf les « vrais » jumeaux – il contient une quantité massive d'informations, ce qui présente un risque d'abus s'il venait à être dévoilé [de Terwangne 2012, p. 45]), les données « concernant des infractions et celles concernant des mesures de sûreté connexes » (art. 6 al. 2 let. a projet de Conv. 108) et les données « révélant l'appartenance syndicale » (art. 6 al. 2 let. b projet de Conv. 108). De plus, le projet intègre une disposition visant à faire du contexte lors d'un traitement de données un élément permettant de mettre en place un régime de protection spécifique, comme s'il s'agissait de données sensibles. Les Etats contractant peuvent également renforcer la liste des données sensibles.

Cinquièmement, le droit des personnes concernées est renforcé. Ainsi, le droit « à ne pas être soumis à une décision automatisée » est intégré ; il se conçoit dans un but de dignité humaine, il « découle de la volonté farouche que l'Homme ne soit pas soumis entièrement à la machine » (de Terwangne 2012, p. 47), soit de s'opposer à ce qu'un ordinateur décide en analysant des donnés. Les droits sur la reconnaissance du raisonnement à l'origine d'un traitement de données et d'opposition s'ajoutent également au projet. La question du droit à l'oubli est également au cœur des débats ; une telle disposition serait un grand pas pour les personnes concernées par rapport à leur maîtrise de leurs données, mais ce droit entre en opposition à la liberté d'expression, d'information, voire au devoir de mémoire (*ibid.*, p. 47). Le projet de Conv. 108 n'introduit pas ce droit, le comité consultatif préférant mettre en avant le principe de finalité sur la conservation des données et le droit de rectification des données déjà existant.

Sixièmement, le devoir des acteurs est concerné. Le responsable de traitement doit pouvoir garantir une transparence sur le traitement des

[21] http://www.edoeb.admin.ch/datenschutz/00628/00665/00667/index.html?lang=fr

données, ce qui équivaut à une obligation d'information. La personne concernée doit savoir qui traite les données, la finalité et le destinataire du traitement (*ibid*., p. 56). Ces informations sont similaires à la logique du registre des fichiers en vigueur en Suisse. Le projet vise également à obliger les responsables de traitement à prendre des mesures appropriées concernant la sécurité des données. D'autres obligations s'ajoutent dans un nouvel article : le principe d' « *accountability* » exigeant des responsables de traitement de prendre toutes les mesures appropriées pour faire respecter les règles de la Conv. 108, l'obligation des responsables de traitement à réaliser des analyses de risques et la prise en compte de la protection de la vie privée dès la conception (de Terwangne 2012, p. 60 – 61).

Septièmement, le flux transfrontière des données est revu. Une nouvelle disposition devrait fusionner l'art. 12 Conv. 108 sur la communication entre les Parties et le Protocole additionnel de 2001 sur le flux entre les Etats contractant et les Etats tiers à la Conv. 108. Les travaux sont en cours et le comité conventionnel observe ce qui se prépare dans l'UE (*ibid*., p. 63).

Enfin, le pouvoir des autorités de contrôle est renforcé. L'art. 12bis, al. 2 du projet donne à ces autorités un pouvoir d'investigation et d'intervention, un pouvoir de sanction des infractions administratives, le pouvoir de porter une affaire en justice à l'autorité compétente et la charge de sensibiliser et d'éduquer sur le thème de la protection des données.

Les mesures à venir dans la Conv. 108 se retrouvent dans les autres projets d'autres institutions de révision des normes sur la protection des données et ne manqueront pas de servir de cadre à une éventuelle révision de la LPD en Suisse. Pour Jean-Philippe Walter, la Conv. 108 aurait même une portée plus grande, car des Etats non européens peuvent la signer et la ratifier ; selon lui, elle « renferme un potentiel unique pour devenir la norme majeure d'une législation universelle de protection des données »[22].

22http://www.edoeb.admin.ch/datenschutz/00628/00665/00667/index.html?lang=fr

5 LE CONCEPT DE « *PRIVACY BY DESIGN* »

Dans ce point, nous allons à présent présenter la notion de *privacy by design* et les dynamiques en cours visant à l'intégrer dans la législation.

5.1 L'ORIGINE DE LA NOTION

Le concept de *privacy by design* apparaît en 1997 ; il est pensé par la commissaire à l'information et à la protection de la vie privée (« *Information and Privacy Commissioner* ») de la province canadienne de l'Ontario, Ann Cavoukian. Cette notion, qu'on pourrait traduire en français par la protection intégrée de la vie privée (PIVP) ou protection de la vie privée dès la conception (nous utiliserons les termes de *privacy by design* et de protection dès la conception dans la suite de ce travail), propose d'intégrer dans un cadre légal une protection des données pendant la création de nouveaux outils et systèmes traitant des données.

La *privacy by design* s'articule autour de sept principes – quelque peu similaires – développés par Ann Cavoukian et émis dans un guide (Cavoukian 2011a, p. 2) :

- « Prendre des mesures proactives et non réactives ; des mesures préventives et non correctives » (*ibid.*) : ce premier principe indique que les mesures relatives à la protection des données doivent être prises préalablement et non pas lorsqu'un éventuel abus a été constaté. En somme, il s'agit de l'adage « mieux vaut prévenir que guérir » (Mouchard 2013).
- « Assurer la protection implicite de la vie privée » (Cavoukian 2011a, p. 2) : dans tout traitement de données, un standard de protection des données est de mise. Selon Mouchard (2013, p. 17), ce principe équivaut à faire de la protection des données un droit fondamental (ce qui est le cas en Suisse).
- « Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques » (Cavoukian 2011a, p. 2) : un système d'information doit être développé en intégrant les principes de protection de la vie privée lors de sa conception ; ils ne doivent pas être ajoutés postérieurement.

- « Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle » (*ibid*.) : selon cette idée, la *privacy by design* ne doit pas être pensée comme un obstacle à d'autres intérêts. Il s'agit d'éviter « les fausses dichotomies, par exemple celle qui oppose la protection de la vie privée à la sécurité » (*ibid*.). Ainsi, le résultat devrait être gagnant pour toutes les parties. Ce principe se détache clairement des autres (Krebs 2013, p. 13), car il évoque l'existence d'autres parties (et d'autres intérêts).
- « Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements » (Cavoukian 2011a, p. 2) : pendant la période de conservation, jusqu'à leur destruction, les données devraient être protégées.
- « Assurer la visibilité et la transparence » (*ibid*.) : l'usage qui est fait des données par les organismes les traitant doit être explicite et transparent. Ainsi, la confiance entre un consommateur et une entreprise, par exemple, serait améliorée.
- « Respecter de la vie privée des utilisateurs » (*ibid*.) : ce septième principe demande que les questions de protection des données soient pensées en fonction du particulier. Il s'agit par exemple pour une organisation de montrer clairement quelles sont ses politiques de confidentialité et de proposer des outils d'amélioration de la protection. L'intérêt du citoyen / consommateur par rapport à sa vie privée doit prédominer.

Lors de la 32e conférence mondiale des commissaires à la protection des données et de la vie privée qui se déroulait en octobre 2010 à Jérusalem, la *privacy by design* a été au cœur des débats. Les différents commissaires invités (dont le préposé suisse) ont résolu d'adopter et promouvoir la *privacy by design* et ces principes, et de la reconnaître comme un élément fondamental de la vie privée.

De manière générale, la *privacy by design*, s'inscrit dans la troisième génération de la protection des données. Selon Poullet (2005), la première génération a été celle des principes généraux de la protection des données. La Convention 108 du Conseil de l'Europe en fait partie. La deuxième génération était quant à elle caractérisée par l'apparition des mesures de coercition : l'apparition de préposés à la protection des

données et les contrôles de la légalité du traitement des données se sont développés. Enfin, la troisième génération, à venir, devra être celle de la prévention. Une analogie originale à la prévention routière (Poullet 2005, Mouchard 2013) permet de mieux comprendre les nouveaux enjeux de la protection des données. La régulation des réseaux routiers a d'abord commencé par les principes de règles générales. Puis, des règles spécifiques et des sanctions ont progressivement fait leur apparition. A présent, les nouveaux moyens de réguler le trafic routier agissent directement sur les véhicules, qui par exemple, ne peuvent pas atteindre une vitesse trop puissante. La *privacy by design* s'inscrit dans cette même logique de prévention et réglages des paramètres au moment de la conception.

La *privacy by design* est également étroitement liée aux nouvelles évolutions technologiques et numériques dans notre société. La mise en place de tels principes demandent non seulement les compétences de juristes et tout autre acteur impliqué dans la réalisation d'une politique publique, mais aussi à des techniciens, informaticiens notamment, à même d'intégrer les questions de protection des données dans l'architecture d'un outil.

5.2 LA *PRIVACY BY DESIGN* : UNE SOLUTION PARTAGÉE PAR DIFFÉRENTES INSTITUTIONS

5.2.1 LE NOUVEAU RÈGLEMENT EUROPÉEN (PREMIÈRE LECTURE ACCEPTÉE LE 14 MARS 2014)

Le projet de règlement européen fait mention explicite de la *privacy by design* dans son article 23 « Protection des données dès la conception et protection des données par défaut » (Chapitre IV Responsable du traitement et sous-traitant ; Section 1 Obligations générales). Il stipule :

> *« 1. Compte étant tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre , le responsable du traitement applique, tant lors de la définition des moyens de traitement que lors du traitement proprement dit, les mesures et procédures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme aux prescriptions*

> *du présent règlement et garantisse la protection des droits de la personne concernée. »*
>
> *« 2. Le responsable du traitement met en œuvre des mécanismes visant à garantir que, par défaut, seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement, ces données n'étant, en particulier, pas collectées ou conservées au-delà du minimum nécessaire à ces finalités, pour ce qui est tant de la quantité de données que de la durée de leur conservation. En particulier, ces mécanismes garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques. »*
>
> *« 3. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser d'éventuels critères et exigences supplémentaires applicables aux mesures appropriées et aux mécanismes visés aux paragraphes 1 et 2, en ce qui concerne notamment les exigences en matière de protection des données dès la conception applicables à l'ensemble des secteurs, produits et services. »*
>
> *« 4. La Commission peut définir des normes techniques pour les exigences fixées aux paragraphes 1 et 2. Ces actes d'exécution sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2. »*

La *privacy by design* est mentionnée à l'al. 1, tandis que l'al. 2 concerne la *privacy by default* (voir point 7.3.3). Les al. 3 et 4 donnent le pouvoir à la Commission de préciser les critères et exigences découlant de l'exercice de la *privacy by design via* des actes délégués, ainsi que de définir les normes techniques *via* un examen par un comité. Selon la CNIL, l'art. 23 al. 1 est « positif sur les principes », car il fait mention non seulement des mesures techniques, mais également des mesures organisationnelles (Guérin-François 2012, p. 18). Mais la CNIL critique une « centralisation de la régulation de la vie privée au profit de la

Commission[23] qui dispose d'un pouvoir normatif important » qui est « contraire à un système participatif, reposant sur une coopération approfondie entre autorités compétentes » (p. 18) par rapport aux al. 3 et 4. Une mise en œuvre est possible est possible selon la CNIL avec les outils de PIA (évaluation approfondie des impacts d'un outil traitant des données, *privacy impact assessements*) et la certification (évaluation rapide).

Le 12 mars 2014, la proposition de règlement a été acceptée par le Parlement européen en première lecture, avec 207 amendements. L'amendement 118 sur l'art. 23 émet des changements conséquents, qui convergent avec les remarques de la CNIL. Concernant l'al. 1, l'amendement fait mention explicite des principes définis à l'art. 5 (« Principes relatifs au traitement des données à caractère personnel ») de la protection des droits de la personne concernée. Le Parlement ajoute également que la protection dès la conception « tient compte en particulier de la gestion du cycle de vie complet des données à caractère personnel, depuis la collecte jusqu'à la suppression en passant par le traitement ». Il évoque explicitement les études d'impact (PIA) à réaliser par le responsable de traitement (*cf.* art. 33) avant les procédures et mesures à entreprendre. Les al. 3 et 4 sont supprimés dans l'amendement.

5.2.2 LA *PRIVACY BY DESIGN* DANS LE PROJET DE MODERNISATION DE LA CONVENTION 108

Le projet de modernisation de la Conv. 108 intègre une nouvelle disposition sur les « obligations complémentaires » (art. 8*bis*) des responsables du traitement. On retrouve d'abord le principe d' « *accountability* » et l'analyse des risques, puis la *privacy by design* à l'al. 3 :

> *« Chaque Partie prévoit que les produits et services destinés au traitement de données doivent prendre en compte les implications du droit à la protection des données à caractère personnel dès leur conception et faciliter la conformité des traitements de données au regard du droit applicable. »*

[23] Souligné dans le texte.

En plus de garantir une meilleure protection des données, la *privacy by design* est également perçue comme économiquement intéressante, partant du principe qu'il est plus efficient d'intégrer la protection avant plutôt que d'effectuer des ajustements sur un produit déjà opérationnel (de Terwangne 2012, p. 62). En 2011, Walter affirmait toutefois qu'un « certain scepticisme » se dégageait quant à la nécessité d'introduire le concept de *privacy by design*, dans la mesure où cet aspect est déjà prévu dans les principes de bases et que l'obligation d'effectuer une analyse des risques est suffisante[24].

5.2.3 LA VOLONTÉ D'INTÉGRER LA *PRIVACY BY DESIGN* EN SUISSE

Suite aux travaux sur la révision de la LPD, le Conseil fédéral a émis cinq objectifs à atteindre concernant la protection des données. Le premier de ces objectifs défend une protection plus en amont, « dès la phase de conception des nouvelles technologies » (MCF 2011, p. 268). Le Conseil fédéral défend ce principe, car il permet d'éviter de voir les problèmes « après coup ». Il veut également chercher à privilégier les technologies offrant une meilleure protection.

Selon Walter, l'application de ce principe permettrait « d'éviter la collecte et le traitement de données superflues, de limiter la conservation de ces données au minimum nécessaire et d'offrir aux personnes concernées une meilleure maîtrise sur leurs données [...] » (2012a, §25). Nous pouvons y décerner un lien entre la protection dès la conception et le principe de minimisation des données que nous développerons plus loin (point 7.3.1). Dans une interview accordée au site comparis.ch, le PFPDT Hanspeter Thür affirme que les deux grandes priorités de la révision de la LPD sont la *privacy by design* et la *privacy by default*, deux « maîtres-mots » (Säemann 2014)[25].

[24] http://www.edoeb.admin.ch/datenschutz/00628/00665/00667/index.html?lang=fr
[25] Disponible à cette adresse: http://fr.comparis.ch/comparis/konsumentenstimme/2014-1/datenvertrauens-index.aspx

Au parlement, un postulat du conseiller national Jean-Christophe Schwaab déposé le 25 septembre 2013 fait mention explicite de la *privacy by design*. Le texte déposé[26] stipule :

> « Le Conseil fédéral est chargé d'étudier l'opportunité d'une modification de la législation sur la protection des données pour y introduire le concept de la protection de la vie privée dès la conception ("*privacy by design*", cf. Cavoukian, Ann, "Operationalizing privacy by design: A Guide to Implementing Strong Privacy Practices", Toronto 2012). Chaque nouvelle technologie traitant des données personnelles ou permettant d'en traiter doit garantir dès sa conception et lors de chaque utilisation, même si elle n'a [*sic*] pas été prévue à l'origine, le plus haut niveau possible de protection des données. »

Dans son développement, le conseiller national affirme que la protection de la vie privée dès la conception est à la fois une réponse aux technologies traitant une quantité toujours plus grande de données interconnectées, mais aussi une réponse aux entreprises « qui tentent de décourager les particulier de protéger au mieux leurs données personnelles grâce à des procédures longues, compliquées et surtout changeant fréquemment »[27]. Le Conseil fédéral a proposé d'accepter le postulat.

[26] Un renforcement de la protection des données grâce au « privacy by design » (postulat 13.3807)

[27] http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20133807

6 ENJEUX SUR LA PROTECTION DES DONNÉES

6.1 LES ÉVOLUTIONS TECHNOLOGIQUES

L'argument principal justifiant un renforcement de la LPD – et des autres normes hors de Suisse – est celui de l'évolution des technologies permettant de nouvelles possibilités quant au traitement des données personnelles et redéfinissant les possibilités de capter, conserver, transférer les données personnelles. Vidéo-surveillance, web 2.0, *cloud comupting*, puces RFID, « Internet des objets », etc. la liste est très longue. Face à ces nouveaux outils, la LPD telle qu'elle est en vigueur actuellement ne suffira plus à encadrer toutes les situations. C'est d'ailleurs à partir de ce constat que fut menée l'évaluation de la loi par l'OFJ. Il s'agit à présent de bien cerner les enjeux caractéristiques de ce qui est entendu par « évolution technologique » et de voir en quoi elle constitue une part importante du problème public – et également une part des solutions. Plutôt que d'énumérer toutes les nouvelles possibilités, voyons plutôt les tendances communes aux TIC, en particulier concernant la question des données.

6.1.1 L'ÉMERGENCE DU PHÉNOMÈNE DES *BIG DATA*

On entend par *big data* (ou données massives), une façon de collecter, de conserver et de partager un très grand volume de données. Quatre caractéristiques accompagnent ces données. D'abord, le volume, car il devient à présent possible de générer et stocker une quantité gigantesque de données ; la vitesse, car les données sont traitées rapidement ; la variété, en raison de la diversité des données récoltées et du caractère brut à format différent (texte, image, chiffre, etc.) ; et enfin, la valeur[28], les données possèdent une plus-value, par ailleurs un des aspects de ces données massives est la possibilité d'établir des prédictions. Des exemples concrets seraient le traitement des photographies publiées sur un réseau social, le traitement des requêtes écrites dans un moteur de

[28]Certains n'ajoutent pas la valeur comme caractéristique des *big data*, mais c'est le cas du PFPDT.

recherche, le décodage rapide du génome humain, etc. A l'heure où l'information est une denrée recherchée, les *big data* offrent des nouvelles possibilités que ce soit au niveau politique, économique, social ou scientifique.

Les *big data* sont des données factuelles et anonymes, dès lors, elles ne permettent pas d'identifier une personne et donc ne rentrent pas dans la définition d'une « donnée personnelle ». Cependant, selon le PFPDT, la possibilité de ré-identification est possible[29]. Certains chercheurs affirment qu'une anonymisation totale est impossible (Mayer-Schönberger et Cukier 2014, p. 188) ; par exemple, aux Etats-Unis, il a été possible d'identifier une personne en croisant les données de locations de films sur Netflix (entreprise proposant des films et séries en location) à ses préférences en matière de cinéma (au moins six films favoris, qui ne soit pas les plus connus) sélectionnées sur le site IMDb (*Internet Movie Database*) (*ibid*., p. 187). C'est un exemple qui illustre la possibilité de croiser des données brutes, apparemment sans lien, pour ré-identifier un individu. Ce sont alors les principes au cœur de la LPD qui sont alors bafoués ; c'est pourquoi le PFPDT estime qu'une évaluation est nécessaire « pour déterminer si les principes essentiels que sont l'assignation d'un but précis, le consentement des personnes concernées et la transparence peuvent être respectés lors de l'utilisation de données massives »[30]. Par ailleurs, il précise que la *privacy by design* serait une réponse à cette explosion de la génération et de l'utilisation des données, grâce à l'intégration dès le développement des principes de protection.

6.1.2 « INTERNET DES OBJETS »

Par l'expression « Internet des objets », on entend l'intégration d'outils permettant de récolter des données dans la réalité de la vie quotidienne. Poullet parle d' « *ubiquitous computing* » (2009, p. 61) « où les terminaux peuvent être placés partout et dès lors enregistrer les faits les plus anodins de notre vie quotidienne, nos déplacements, nos hésitations, notre consommation domestique ». Ces technologies se

[29] http://www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=fr
[30] *ibid*.

concrétisent notamment sous forme de puces et capteurs. Les nouvelles technologies de l'*ubiquitous computing* possèdent quatre caractéristiques (Langheinrich 2001, p. 6 – 7) : la première est justement l'ubiquité, la captation de données peut se réaliser partout sur toute une série d'objets variés ; la deuxième est l'invisibilité, la technologie se miniaturise, on ne voit rien lorsqu'il y a un traitement de données ; la troisième est la capacité de collecter des données toujours plus variées et précises (par exemple, Langheinrich prévoit qu'il sera possible de capter des émotions, [2001, p. 6]) ; la quatrième est la capacité de mémorisation accrue, ce que nous avons déjà vu avec les *big data*. En somme, toutes les données récoltées par ces nouveaux biais pourront alors se trouver être « le gros fournisseur en *big data* de demain » (Rapport d'activité du PFPDT 2013/2014, p. 8).

Nous allons à présent détailler deux exemples emblématiques.

6.1.2.1 EXEMPLE 1 : LA TECHNOLOGIE RFID

Un exemple illustrant cette emprise du réseau et de la question des données sur notre quotidien est celui de la radio-identification (*radio frequency identification*, plus connue sous le sigle RFID). Les technologies RFID se concrétisent en deux appareils : l'étiquette RFID et le lecteur RFID. Les premières – qui peuvent apparaître sous forme de puce – contiennent des informations qui peuvent être ensuite lues par des lecteurs. La particularité de cette technologie est que les données mémorisées dans une étiquette peuvent être lues grâce à des ondes radio, donc à distance. Actuellement, l'utilisation de cette technologie existe dans un grand nombre de domaines, par exemple :

- les antivols dans les magasins
- certaines cartes de transport public
- puces sous-cutanées pour les animaux, voire les êtres humains[31]
- aide à la traçabilité des produits
- passeports, avec des données biométriques
- etc.

[31] Ce fut le cas en 2004 notamment dans une boîte de nuit barcelonaise ; les clients avaient la possibilité de s'implanter une puce RFID qui servait alors de porte-monnaie électronique.

Les possibilités sont larges et augmenteront encore dans les années à suivre.

Évidemment, les risques d'abus par rapport à la protection des données sont présents. Par exemple, il est possible alors que les étiquettes puissent être lues à l'insu de l'utilisateur[32]. Pour l'instant, le PFPDT rappelle la technologie RFID est liée à un système de réseaux et qu'il incombe aux gérants de ces systèmes d'y intégrer les principes essentiels de la protection des données (voir Rapport d'activités 2009/2010 du PFPDT, p. 34 – 36).

6.1.2.2 EXEMPLE 2 : LES COMPTEURS ÉLECTRIQUES INTELLIGENTS

Un autre exemple précis de l'utilisation de capteurs dans la vie quotidienne est celui des compteurs électriques intelligents. Il fait notamment l'objet d'une étude par la promotrice initiale de la *privacy by design* (voir Cavoukian 2009) et peut aisément être extrapolé à d'autres appareils.

Un compteur électrique intelligent est un système permettant d'analyser la consommation d'électricité d'un ménage. L'apparition de ce type d'outils vient avant tout de la libéralisation du marché de l'électricité ; c'est le cas en Europe et en Suisse. Dans notre pays, le marché de l'électricité est partiellement libéralisé depuis 2009 ; les grands consommateurs d'énergie – soit 100 MWH – peuvent choisir librement le fournisseur d'électricité. Il est prévu que cette libéralisation se poursuit et s'étendent aux PME et aux ménages, mais ce ne sera pas le cas avant 2016[33]. Si la réforme passe, « le client aura à l'avenir un exploitant de réseau et un fournisseur d'électricité ; le premier lui sera imposé, mais il pourra choisir le second »[34]. De ce fait, les fournisseurs, afin de s'adapter à l'offre et la demande, devront alors savoir au mieux quelles sont les habitudes de consommation des ménages ; c'est là que les compteurs intelligents se mettent place. Avec une analyse détaillée

[32] http://www.edoeb.admin.ch/dokumentation/00153/00215/00258/index.html?lang=fr (rapport activités 2009/2010)

[33] http://www.rts.ch/info/suisse/5525164-pas-de-liberalisation-totale-du-marche-suisse-de-l-electricite-avant-2016.html

[34] http://www.edoeb.admin.ch/datenschutz/00121/00916/index.html?lang=fr

de la consommation, ils permettront aux fournisseurs une adaptation de leurs tarifs. Mais cette analyse n'est pas sans risque d'un point de vue de la protection des données. Selon le PFPDT :

> « Du fait de leur conception technique, les compteurs numériques permettent en principe d'enregistrer les données nécessaires à la facturation, mais aussi le profil de consommation d'énergie du ménage ou de l'entreprise. Ces données plus détaillées contiennent des informations qui peuvent s'avérer précieuses pour le client en lui indiquant sa consommation d'énergie et donc aussi des gisements d'économies d'énergie, mais elles recèlent aussi des informations sur ses activités professionnelles, ses processus de production, ses activités personnelles, l'organisation de ses journées, des absences maladie, etc. »[35]

Parmi, les recommandations du PFPDT, on peut notamment trouver l'exigence du respect des principes de bases de la protection des données, l'importance aux fournisseurs d'expliquer comment les données récoltées seront traitées (notamment s'il y a transfert à des tiers), l'impossibilité de réaliser des observations en temps réel, notamment.

La dynamique est la même dans l'UE. En 2009, le troisième paquet « climat-énergie » adopté par le Parlement européen prévoyait l'installation de compteurs intelligents dans 80 % des ménages (Cavoukian 2009, p. 7). Cette volonté correspond aux objectifs de la Commission européenne d'atteindre les objectifs 20/20/20, « la réduction de 20% des émissions de gaz à effet de serre de l'Union Européenne par rapport à 1990, une part 20% d'énergies renouvelables dans la consommation d'énergie totale, et la réduction de 20% de la consommation énergétique européenne par rapport à l'augmentation tendancielle »[36]. La Suisse devra également tenir compte des évolutions dans l'UE dans ce domaine.

---

[35] *ibid*.

[36] http://www.developpement-durable.gouv.fr/IMG/pdf/05-_les_objectifs_europens_nergie-climat.pdf

6.1.3 LES TECHNOLOGIES AU SERVICE DE LA VIE PRIVÉE

Par rapport à la protection des données, l'évolution technologie se perçoit avant tout comme une menace, comme le montrent entre autres les exemples cités au-dessus. D'aucuns nominent ces technologies comme étant des *privacy-invasive technologies* (PIT). Certaines nouvelles technologies, lorsqu'elles sont utilisées correctement par des individus, permettent au contraire de renforcer la protection de leurs données. On parle alors de *privacy-enhancing technologies* (PET). Ces dernières permettent d'anonymiser les données, en utilisant principalement les méthodes de cryptographie (Morin 2012, p. 10). Nombre de ces technologies concernent Internet et le web ; il existe par exemple des sites ou programmes cryptant la navigation sur la Toile, voire les contenus postés sur les réseaux sociaux (*ibid*., p. 10). De nouveaux services respectant au maximum la protection de la vie privée sont lancés, par exemple des moteurs de recherche, des navigateurs, des réseaux sociaux alternatifs. Nous pouvons également l'initiative du World Wide Web Consortium (W3C)[37], qui cherche à mettre en place un moyen d'uniformiser les politiques de *privacy* sur Internet avec un certificat intitulé « *Platform for Privacy Preferences Project* » (P3P) qui serait appliqué à l'ensemble du web. Bien que des possibilités de crypter ses données ou d'user de logiciels garantissant la protection des données, elles ne sont pas forcément utilisées et ont un succès très relatif par rapport aux produits proposés par les géants de l'informatique.

6.2 ATTENTES ET COMPORTEMENTS DES INDIVIDUS

Le rapport d'évaluation de la LPD a réalisé une enquête sur la population suisse afin d'en connaître plus sur sa sensibilité quant à la question des données. Nous présenterons ici les principaux résultats, qui seront alors mis en perspective en les comparant à d'autres enquêtes similaires. L'enquête a été faite auprès de 1014 personnes sur l'ensemble du territoire suisse en respectant la représentativité de la population. Elle

[37] Le W3C est une organisation à but non lucratif qui émet les normes de standardisation du web, comme l'utilisation des langages HTML et CSS pour la structure des sites web. L'organisation est présidée par Tim Berners-Lee, fondateur du WWW. Les standards qu'elle met en place deviennent universels.

porte sur plusieurs aspects de la protection des données, dont les comportements sur Internet, la manière de se protéger ou la responsabilité de la protection.

6.2.1 LES RÉSULTATS DU RAPPORT D'ÉVALUATION

Une première donnée intéressante est la position des personnes interrogées sur l'échange d'informations et la collecte des données : il leur a été demandé de dire si elles étaient d'accord ou non avec les deux affirmations suivantes : 1) « L'échange d'informations est une bonne chose » (aspect positif) et 2) « La récolte des données peut effrayer » (aspect négatif) (OFJ 2011, p. 47 – 48). Suite aux réponses, il a été possible de créer quatre catégories de personnes. Premièrement, on retrouve la catégorie des « ambivalents », soit les personnes étant d'accord avec les deux affirmations ; c'est le groupe le plus représenté (50 % des interviewés). Deuxièmement, on retrouve le groupe des « pessimistes », soit les personnes pas d'accord avec la première proposition et en accord avec la deuxième ; 24 % des personnes y font partie. Troisièmement, le groupe des « insouciants » représente 15 % des interrogés ; il s'agit du groupe de ceux qui sont d'accord avec la première affirmation et pas d'accord avec la deuxième. Enfin, le groupe des « indifférents » obtient 6 % des réponses, ils ne sont pas d'accord avec les deux affirmations. Le groupe majoritaire des « ambivalents » et le petit groupe des « indifférents » montrent un certain paradoxe dans la vision de la population sur l'échange des données : il est à la fois une « bonne chose » et « effrayant ».

Une autre forme de paradoxe peut être vue à la question sur la responsabilité de la protection des données. Les personnes interrogées devaient dire si elles étaient d'accord avec les deux affirmations suivantes : 1) « On peut soi-même bien se contrôler » et 2) « Un organe indépendant est nécessaire » (*ibid.*, p. 49 – 50). Encore une fois, quatre groupes apparaissent en fonction des réponses. Premièrement, ceux qui ont répondu par l'affirmative aux deux affirmations forment le groupe des « délégants » ; ils sont représentés à 55 %. Deuxièmement, les personnes qui ne sont pas d'accord avec la première affirmation et approuvent la deuxième forment le groupe des « exigeants » à 20 %.

Troisièmement, le groupe des « responsables » prend en compte les gens qui sont d'accord avec la première affirmation et refusent la deuxième ; ils représentent 14 % du total. Enfin, ceux qui refusent les deux affirmations forment le groupe des ceux prônant un « refus fondamental » à 5 %. Le groupe majoritaire des « délégants » sont ambivalents en raison d'une confiance en eux-mêmes et une importance signalée d'avoir un organisme indépendant. Les experts interrogés en marge du questionnaire ne sont pas convaincus par cet apparent optimisme quant à une régulation personnelle des données, arguant notamment qu'il y a un manque de connaissances dans les possibilités techniques (*ibid*., p. 50).

Les personnes interrogées ont un avis différent sur le traitement des données en fonction de la nature et l'origine des données récoltées. Quand on leur demande quelles sont les données qui valent une protection (*schützenwerte Angabe*), les résultats montrent, dans l'ordre, les données médicales (86%), le revenu (83%), les photographies (81%), l'adresse (69%), les sites visités (65%), l'opinion politique (47%) et les achats (41 %) (*ibid*., 52 – 53). Quant aux types de traitement de données, 94 % des personnes pensent que la publication de photos est problématique, 84 % estiment que l'*adressbroking* (marketing direct) est également problématique, 54 % par rapport au « *Street View* » effectué par Google et 31 % par rapport aux caméras de vidéo-surveillance (*ibid*., p. 53).

L'enquête de l'OFJ a également cherché à voir si les comportements des personnes sur Internet changeaient pour des raisons de protection des données. Lorsqu'on cherche à savoir si les gens se passeraient d'une prestation commerciale pour des raisons de protection des données (la question exacte est « *Bei Wettbewerben, Kundenkarten oder auch anderen Dienstleitungen muss man zum Mitmachen manchmal weiter gehende Informationen über die eigene Personen angebem (z.B. Geburtsdatum, Geschlecht, Beruf oder auch Hobbies). Ist es schon einmal vorgekommen, dass Sie wegen solchen Angabem auf eine Dienstleistung verzichtet haben ?* ») (*ibid*., p. 58) : 17 % répondent souvent, 25 % occasionnellement, 6 % une fois, 11 % l'ont considéré, 38 % ne l'ont pas considéré et 3 % ne savent pas ou ne donnent pas de

réponse. On voit que près de la moitié ne l'ont jamais fait (les 38 et 11%) et seuls 17 % accordent une importance à la protection des données au point de se passer souvent de certaines prestations commerciales.

Sur les 822 personnes affirmant utiliser Internet au moins plusieurs fois par années, 84 % utilisent Internet pour des prestations commerciales et 16 % ne le font pas, parmi lesquelles 10 en raison de protection des données. Quant à l'utilisation d'un réseau social, 41 % des sondés en sont membres et 58 % ne le sont pas, parmi lesquels 23 en raison de protection des données et 35 pour d'autres raisons (*ibid*., p. 59 – 60).

Quant à l'utilisation des moyens de protections, la plupart des personnes interrogées (les 822 utilisant Internet régulièrement) affirment se protéger techniquement sur leur ordinateur (par exemple avec un antivirus ou un *firewall*) contre les éventuelles intrusions. Par contre, quand il s'agit spécifiquement de se protéger en allant sur le web (surf anonyme, outils de cryptage), seulement 34 % affirment le faire (*ibid*., p. 62 – 63).

Des différences significatives de réponses sont observées dans les différents groupes sociaux interrogés. Les catégories identifiées sont le sexe, l'âge, la région linguistique, le niveau d'études, le revenu et l'utilisation du web. Les différences significatives sont à relever principalement pour la région linguistique et l'âge. Les répondants du Tessin se montrent moins soucieux que les Romands et les Alémaniques par rapport à la protection des données et exigent un organisme indépendant. Par rapport à l'âge, les plus jeunes (15 à 34 ans) se sentent moins méfiants face à la technologie et plus confiants quant à leurs capacités à faire preuve d'un comportement responsable que les plus âgés (*ibid*., p. 56 - 57).

6.2.2 MISE EN PERSPECTIVE DES RÉSULTATS

Globalement, l'enquête montre que la population porte un intérêt envers les questions de protection des données, tout en étant à la fois intéressée aux nouvelles possibilités qu'offre la collecte de données. Et malgré les possibilités de renforcer la protection des données, surtout sur Internet, peu de personnes les utilisent, bien qu'une majorité se dise responsable de sa protection de ses données.

La sociologie des données personnelles fait état d'un paradoxe qui règne chez les individus par rapport à leurs données. Ce phénomène appelé « paradoxe de la vie privée » montre que les individus accordent beaucoup d'importance à la protection des données, mais n'agissent pas activement en faveur de cette idée (par exemple en divulguant des informations personnelles sur Internet). Une étude de la Commission européenne (Compañó et Lusoli 2009) sur les comportements des individus de 15 à 25 ans a été réalisée en France, Allemagne, Royaume-Uni et en Espagne. Il s'agit d'un questionnaire sur les comportements concernant la gestion de l'identité dans les environnements digitaux. Avec un total de 5265 réponses, quatre « paradoxes » qui illustrent un comportement supposé « irrationnel » des individus ont pu être soulevés.

Premièrement, le paradoxe de la vie privée, comme évoqué précédemment, montre que les personnes sont relativement bien informées des potentiels risques, mais divulguent leurs informations. Le besoin d'apparaître, notamment sur les réseaux sociaux, est mis en avant. Deuxièmement, le paradoxe de contrôle montre que les personnes interrogées ont conscience des outils – et leur efficacité – permettant un contrôle et une protection de leurs données (par exemple, les outils permettant une minimisation des données), mais ne les utilisent pas. Troisièmement, les répondants ne font confiance ni à eux-mêmes, ni à l'Etat pour la gestion de leurs données personnelles. Malgré les outils existants, ils considèrent ne pas avoir les connaissances nécessaires pour les utiliser. C'est le paradoxe de responsabilité. Enfin, le paradoxe de la conscience montre que les sondés connaissent très peu la législation sur la protection des données et ne l'apprécient pas. Même s'ils en apprennent plus sur la législation, leur comportement ne varie pas.

Certains auteurs relativisent cette apparente irrationalité comportementale. Kaplan (2010) relève que ces paradoxes peuvent aussi trouver leur origine chez les régulateurs peinant à trouver des solutions adéquates aux attentes des utilisateurs. Un autre argument est celui des changements de valeurs chez les individus. Certaines données autrefois jugées sensibles par certains le sont moins à leurs yeux (mais pas dans la loi !), par exemple l'orientation sexuelle dans la société occidentale contemporaine (Kaplan 2010, p. 23).

6.2.3 LA CONNAISSANCE DE LA LPD ET DU PFPDT

L'enquête menée par l'OFJ s'est intéressée également à la perception des individus de LPD et de leurs droits en matière de protection des données. Il apparaît en premier lieu que 30 % des sondés ne connaissent pas la LPD ; parmi les 70 % restants, 26 % connaissent les moyens de recours, 42 % affirment devoir s'informer et 2 % ne connaissent pas les moyens de recours (OFJ 2011, p. 77 – 82).

21 % des personnes (208) ont eu le sentiment d'avoir subis un abus sur leurs propres données personnelles. Dans 134 cas, il s'agissait de données concernant leur adresse, et 57 cas se classent dans la catégorie « autre » ; viennent ensuite les données comme les photos et les vidéos (25). La majorité des personnes s'étant senties victimes n'ont rien fait, et une petite minorité s'est tournée vers la personne qui abusait de leurs données. Lorsqu'on demande aux individus ce qu'ils feraient en cas d'atteinte à leurs données, les réponses indiquent qu'ils se tourneraient soit vers la police, soit directement vers la « source » du problème et un nombre non négligeable de gens se tournerait vers le tribunal ; un nombre similaire d'interrogés disent ne pas savoir ce qu'elles feraient. Mais dans les faits, ceux qui sont concrètement subis un tort ne réagissent tout simplement pas (plus de 50%). Le recours au PFPDT n'est pratiquement pas mentionné.

Par rapport au PFPDT (OFJ 2011, p. 159 – 160), la moitié des sondés ne connaissent pas le préposé ; et dans l'autre moitié, seuls 29 % connaissent les activités de conseil du PFPDT.

7 POSSIBILITÉS D'APPLICATION DE LA *PRIVACY BY DESIGN*

Nous allons à présent nous intéresser à l'application concrète de la *privacy by design* dans la loi suisse. Pour rappel, nous avons déjà montré un aperçu du cadre normatif de la protection des données, avec la mise en évidence de la LPD et ses deux ordonnances et du cadre européen avec la Conv. 108, la Directive 95/46/CE et le projet de règlement européen. Nous avons identifié le problème, qui est la (future) inadéquation de la LPD dans la société, pour cause d'évolution technologie et sociétale. Et nous allons à présent développer les différentes possibilités d'intervention dans les dispositions de la législation et les exigences qu'elles requièrent. Puis nous nous intéresserons à l'opérationnalisation de la *privacy by design*. Nous porterons enfin notre regard sur des considérations générales sur l'adoption de nouvelles dispositions.

Trouver la politique adéquate pour atteindre un objectif fixé n'est pas une mince affaire. Un grand éventail de possibilités existe, avec une mise en œuvre et des effets différents. La question est cruciale pour la protection de la vie privée dès la conception, car elle fait intervenir une toute autre logique qui est celle de la prévention, ce qui change radicalement la façon dont se conçoit la protection des données. De plus, celle-ci s'inscrit dans un contexte marqué par une permanente évolution technologique, ce qui rend la mise en place de nouvelles dispositions délicate ; il s'agit de prendre des mesures qui ne seront pas trop vite dépassées. L'une des idées majeures est de faire en sorte que la loi puisse façonner ou du moins encadrer l'évolution des techniques. A ce propos, Lawrence Lessig (cité dans Cavoukian 2011b, p. 12) écrit :

> *« For citizens of cyberspace, . . . code . . . is becoming a crucial focus of political contest. Who shall write that software that increasingly structures our daily lives? As the world is now, code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed. They are the ones*

> *who set its nature. Their decisions, now made in the interstices of how the Net is coded, define what the Net is. »*

En extrapolant, on entend par le « Net » tout système traitant des données. Avec la *privacy by design* et son degré d'implémentation, de grandes implications sur le futur des nouvelles technologies peuvent avoir lieu.

Parallèlement à la promotion des principes de *privacy by design*, Cavoukian propose également les moyens de les rendre opérationnels. Trois approches sont décrites : l'approche traditionnelle de correction des abus constatés, l'approche de nouvelle génération, qui se décline en une reprise – sectorielle ou générale – des principes dans la loi ou par l'adoption de codes de conduite et l'approche organisationnelle qui décrit les instruments liés à l'application de la *privacy by design* (Cavoukian 2011b, p. 14). D'un point de vue économique plus général, selon Rochelandet (2010), les modalités de gestion de la protection des données sont le « laissez-faire », l'autorégulation et la régulation contraignante. Pour Krebs (2013), trois approches sur l'introduction de la *privacy by design* peuvent se confronter : la première est l'introduction de la *privacy by design* dans la loi avec un niveau de détail élevé (précisant les outils technologiques à utiliser) ; la deuxième est l'introduction du principe comme principe général dans la loi ; enfin la dernière est l'autorégulation par les organismes traitant les fichiers, ce qui correspond à faire de la *privacy by design* un guide pratique avant tout. Nous nous inspirons de cette typologie pour proposer deux possibilités d'intervention, que nous présenterons par ordre de contrainte envers les responsables de traitement. Pour chacune des possibilités, nous évaluerons la justification, les conséquences d'une telle approche et sa mise en œuvre, avec plus ou moins de détails selon leur pertinence.

La première est la solution non contraignante, soit l'application de la *privacy by design* comme une « simple » recommandation. L'idée principale de cette approche est la *promotion* du principe chez les responsables de traitement.

La deuxième intervention est une solution contraignante. La *privacy by design* s'applique comme nouveau principe dans la LPD, avec des dispositions supplémentaires nécessaires à sa mise en œuvre.

Nous omettons à dessein de détailler une solution qui consisterait à faire appliquer la *privacy by design* avec un niveau de détail élevé, car cela agirait au contraire du principe non formel de neutralité technologique de la loi suisse, qui a permis de faire de la LPD une loi efficace malgré les avancées technologiques, dont Internet, pendant 20 ans. Nous reviendrons brièvement sur ce point dans les considérations générales (point 7.4.5).

7.1 INTERVENTION N°1 : LA *PRIVACY BY DESIGN* COMME RECOMMANDATION

La première option possible est de faire de la *privacy by design* un principe non contraignant. La principale justification d'une telle démarche est d'ordre économique. L'introduction de la *privacy by design* dans la loi suisse correspond donc à effectuer une régulation dont le groupe-cible est la personne privée ou l'organe fédéral (le maître du fichier). Dans beaucoup de domaines, il existe l'idée selon laquelle la régulation publique s'oppose au libre marché et empêche l'autorégulation. Cette dualité n'épargne pas le domaine de la protection des données. En effet, les données personnelles sont très liées aux intérêts économiques, surtout pour les personnes morales en l'occurrence. Dans son rapport sur l'évaluation de la LPD (MCF 2011), le Conseil fédéral écrivait alors : « Par ailleurs, le Conseil fédéral veillera, en examinant les mesures législatives souhaitables, à tenir compte du fait que les mesures prises au titre de la protection des données peuvent entrer en conflit avec d'autres intérêts. C'est pourquoi il s'efforcera d'intégrer dans sa réflexion, aux côtés des impératifs de la protection de la personnalité, tous les autres intérêts touchés, dont ceux de l'économie, la liberté d'opinion et d'information, ainsi que d'autres intérêts publics et privés » (p. 269). La révision de 2006 de la LPD avait également suscité une opposition des milieux économiques. La question des intérêts économiques des données personnelles se pose. Une solution non contraignante ferait ainsi la balance entre respect de la

protection des données et respect des intérêts des organisations. Nous allons détailler cet argument en deux points : tout d'abord nous reviendrons sur la critique générale de la régulation des données personnelles, puis nous aborderons les mécanismes d'autorégulation. Nous analyserons ensuite la mise en œuvre de cette solution.

7.1.1 LES CRITIQUES DE LA RÉGULATION

Comme nous l'avons vu, l'élaboration de la LPD s'est justifiée notamment par le fait d'ancrer le droit fondamental à la vie privée, inscrit à présent dans la Constitution. La loi protège contre les abus d'atteinte à la personnalité, un élément indispensable au fonctionnement d'une société démocratique. Malgré tout, de nombreuses critiques sur le concept même de protection des données existent. Deux principales critiques concernant à la fois les secteurs public et privé ressortent : la première est que la protection des données empêche le développement économique des entreprises ; la deuxième est qu'elle se heurte aux objectifs sécuritaires des Etats.

7.1.1.1 LES DONNÉES PERSONNELLES COMME RESSOURCE ESSENTIELLE POUR LES ENTREPRISES

L'intérêt de renforcer la protection des données peut soulever une opposition des intérêts économiques. Plusieurs entreprises ont fait savoir qu'une législation qu'ils considèrent trop restrictive serait un frein à l'innovation et aurait des conséquences économiques négatives. Pour beaucoup, une forme de régulation publique met une charge administrative sur le responsable du traitement du fichier de données. Un résumé de ces critiques se retrouve dans les théories de l'Ecole de Chicago (Rochelandet 2010, p. 29 – 37), qui, en économie, regroupe les célèbres économistes libéraux (Friedman, Posner, Stigler, entre autres). Dans les grandes lignes, la pensée de cette Ecole associe la protection des données à une dissimulation d'informations. Celles-ci sont, selon ces théoriciens, des atouts primordiaux dans une économie fonctionnant sur les principes d'offre et de demande. Une firme adapte ses produits et ses prix grâce à une collecte d'informations. De plus, la recherche d'informations est toujours possible par d'autres moyens, mais cela

génère un coût supplémentaire – tout autant que l'utilisation d'informations erronées.

Une telle approche a pu se développer aux Etats-Unis en partie car la philosophie de la *privacy* diffère fondamentalement de l'esprit européen. Elle évoque avant tout le droit d'être laissé tranquille et de se protéger contre les intrusions (Krebs 2013, §14 ; Rochelandet 2010, p. 90) ; la *privacy* n'est restrictive que dans certains domaines spécifiques comme la santé ou la protection des mineurs (Rochelandet 2010, p. 90).

Pour certains auteurs, une régulation publique ignore certains comportements de la part des utilisateurs en matière de données. Il n'est pas rare de voir les données personnelles désignées comme le « pétrole » du 21ème siècle. Derrière cette expression se cache les enjeux de l'économie dite de l'attention. Herbert Simon fut un des premiers chercheurs à l'avoir théorisée ; selon lui : « Dans un monde riche en information, l'abondance d'information entraîne la pénurie d'une autre ressource : la rareté devient ce qui est consommé par l'information. Ce que l'information consomme est assez évident : c'est l'attention de ses receveurs. Donc une abondance d'information crée une rareté d'attention et le besoin de répartir efficacement cette attention parmi la surabondance des sources informations qui peuvent la consommer » (1971, p. 40 – 41). Il s'agit d'un concept utilisé notamment dans le domaine du marketing comportemental, dont le rôle est d' « enregistrer l'ensemble des actions effectuées avec un ordinateur de manière à pouvoir créer des inférences et faire des suggestions d'achats ou afficher des publicités contextuelles » (Kessous 2012, p. 62).

Au cœur de ce qu'on peut appeler l'économie des données personnelles se trouve la personnalisation des prestations des entreprises à leurs (futurs) clients. Avec les informations contenues dans les données, une possibilité de personnaliser des produits est offerte aux employés. Selon Sackmann, Strüker et Accorsi (2006, cités dans Rochelandet 2010, p. 63), trois types de personnalisation de services existent :

– les services universels, ils se basent sur les données des individus pour offrir des prestations à tous ;

- les services individualisés, il s'agit par exemple utiliser une liste de course pour optimiser le chemin à parcourir dans le magasin ;
- les services personnalisés, ils demandent l'utilisation des données personnelles. Pour reprendre l'exemple du magasin, en fonction des achats du client et de ses caractéristiques, l'entreprise pourrait alors proposer des offres promotionnelles spécifiques, par exemple sur les écrans du magasin, en prenant en compte également la position du client (Sackmann, Strüker et Accorsi 2006).

L'adaptation au client est un point clé de l'économie. De même, la publicité ciblée est un élément majeur sur le web. En effet, les plus grandes entreprises informatiques reposent sur ce modèle. La publicité en ligne est divisible en trois catégories (CNIL 2009, p. 5) : la publicité personnalisée basée sur les caractéristiques des internautes ; la publicité comportementale se basant sur le comportement des internautes dans le temps et la publicité contextuelle, liée au contenu d'une page visitée. Les entreprises sont également capables de dresser des profils de la personnalité en fonction du comportement de l'individu sur un site web (et sa localisation avec son adresse IP) et en fonction des informations que la personne donne elle-même (*ibid*., p. 11).

7.1.1.2 AUTRES CRITIQUES SUR LA RÉGULATION DES DONNÉES

Une critique fait s'opposer protection des données et sécurité nationale. L'argument principal de cette critique est que l'intérêt public est prioritaire à l'intérêt privé dans certains cas. C'est aux Etats-Unis le *leitmotiv* au FISAA ou *Patriot Act*, dans l'objectif de lutte contre le terrorisme. Dans cette idée, la dissimulation de données essentielles, par exemple judiciaires ou médicales, est un obstacle à la sécurité publique. En Suisse, la voix de la Fédération suisse des fonctionnaires de police (FSFP) s'est fait entendre à ce propos (ATS 2012). Elle a organisé un congrès en juin 2012 sur la protection des données qu'elle considère comme étant un obstacle au travail quotidien de la police. Un exemple cité par la FSFP – via son secrétaire générale lors d'une émission à la radio[38] – était le cas d'un policier abattu par un homme barricadé dans son domicile ; selon la FSFP, si les policiers avaient eu accès aux

[38]http://sebastienfanti.ch/2012/06/21/protection-des-donnees-le-cauchemar-des-polices/

données médicales sur cet individu, ce qui avait été refusé, ils auraient pu avoir des informations cruciales sur son état psychologique.

Pour Rochelandet et Rallet, spécifiquement au web relationnel, une pratique comme la *privacy by design* ignorerait « le comportement actif des individus en matière de divulgation de données personnelles » (2011, p. 41). Selon l'auteur, le comportement de certains utilisateurs tendrait à dévoiler ses données (pour bénéficier des avantages d'un réseau social et par extension, profiter d'une prestation), ce qui va à l'encontre des objectifs de la protection des données dès la conception. Comme nous l'avions vu au point 6.2, une grande partie des utilisateurs d'Internet, bien qu'en ayant conscience des enjeux de protection des données, apprécient de profiter de certaines prestations dans la mesure où ils mettent à disposition leurs données.

Un autre argument vient mettre en question l'efficacité d'une régulation, il s'agit de la perte de responsabilité numérique. En effet, quand les utilisateurs d'un réseau social ont connaissance de l'existence d'un contrôle possible de leur part sur leurs données, ils sont plus enclin à livrer des données personnelles et vice-versa (Brandimarte, Acquisti et Loewenstein, 2011). Selon cette théorie, une sensibilisation et une responsabilisation des utilisateurs seraient plus efficaces.

7.1.2 LES MÉCANISMES D'AUTORÉGULATION

Chez les entreprises, plusieurs mesures d'autorégulation existent ; il s'agit par exemple d'avoir des guides de bonne gouvernance, un niveau de déontologie ou encore une indication de management de qualité. C'est également possible dans le domaine de la protection des données. En effet, certains auteurs affirment que la protection des données donne un avantage concurrentiel aux entreprises, cela prend par ailleurs en contre-pied les critiques de la notion de *privacy*. « Face à un univers global et décentralisé comme le sont les environnements numériques, la loi a un intérêt évident à s’en remettre à ceux-là même qui traitent des données personnelles. Il s’agit de jouer sur l’image positive et sur l’avantage concurrentiel que représente la protection de la vie privée » (Bondallaz 2008, §24). Les entreprises qui chercheraient à mieux protéger les données auraient la confiance des individus et ces derniers

se tourneraient vers elles. Un exemple est la rivalité qui a pu opposer les sociétés Google et Microsoft en 2008 lors du lancement de leurs deux nouveaux navigateurs respectifs[39]. Microsoft a cherché par mettre son avant les options de protection des données incluses dans son navigateur, contrairement à celui de son concurrent. L'avantage concurrentiel passe alors par la confiance des consommateurs ; il part du principe que la recherche de protection est un élément prioritaire. Il existe aujourd'hui une série de labels privés pouvant être attribués aux organisations ou aux produits respectant certains principes de protection des données. C'est le cas en Suisse : la certification est d'ordre privé pour des raisons de respect de l'économie libérale, mais encadrée dans la loi ; nous aborderons ce point en détail dans la mise en œuvre de l'application de la *privacy by design* au point suivant.

7.1.3 LA MISE EN ŒUVRE DE LA SOLUTION NON CONTRAIGNANTE : LA CERTIFICATION

En partant du principe que la régulation est une affaire privée et que l'introduction de la *privacy by design* relève des organisations elles-mêmes, la mise en œuvre doit renforcer les mécanismes d'autorégulation déjà présents. Il existe déjà deux dispositions de cette logique dans la loi. En effet, la révision de 2006 de la LPD a apporté deux manières de renforcer la protection des données et responsabiliser les responsables de traitement : il s'agit du recours à un conseiller à la protection des données et à la certification. La certification est un élément intéressant pour intégrer la *privacy by design* de façon non contraignante, car les organisations désirant se doter de mécanismes visant à mieux protéger les données peuvent recevoir un label. Cela peut avoir plusieurs conséquences positives pour l'organisation, comme une amélioration de son image, de la confiance inspirée, etc.

Nous allons à présent décrire le processus de certification, afin de déceler les potentielles améliorations possibles, dont le fait d'intégrer la *privacy by design*, puis proposer des réformes possibles.

[39] http://www.journaldunet.com/solutions/expert/31091/ie-8-contre-google-chrome---premieres-impressions-des-avocats-de-la-vie-privee.shtml

7.1.3.1 LE PROCESSUS ACTUEL DE CERTIFICATION

Le processus de certification délie actuellement un maître du fichier de son devoir de déclaration au registre des fichiers (art. 11a, al. 5 let. f LPD). La procédure est expliquée à l'art. 11 LPD :

> « 1. Afin d'améliorer la protection et la sécurité des données, les fournisseurs de systèmes de logiciels et de traitement de données ainsi que les personnes privées ou les organes fédéraux qui traitent des données personnelles peuvent soumettre leurs systèmes, leurs procédures et leur organisation à une évaluation effectuée par des organismes de certification agréés et indépendants. »
>
> « 2. Le Conseil fédéral édicte des dispositions sur la reconnaissance des procédures de certification et sur l'introduction d'un label de qualité de protection des données. Il tient compte du droit international et des normes techniques reconnues au niveau international. »

L'al. 2 fait référence à l'OCPD. En vertu de cette dernière, la certification porte sur les structures d'organisation et les systèmes techniques utilisés par les exploitants. Pour implémenter la *privacy by design*, nous pourrions imaginer la mise en place d'une certification obligatoire pour les responsables intégrant ce principe dans leurs systèmes. Actuellement, deux modes de certification sont prévus dans l'ordonnance : la certification de l'organisation et de la procédure et la certification de produits (« *produits matériels et logiciels ou systèmes pour procédures automatisées de traitement de données* ») (art. 1 al. 2 OCPD).

La certification de l'organisation et de la procédure est détaillée à l'art. 4 OCPD. Elle porte sur « l'ensemble des procédures de traitement des données pour lesquelles un organisme est responsable » (art. 4 al. 1 let. a OCPD) et « des procédures de traitement déterminées » (art. 4 al. 1 let. b OCPD). Il s'agit d'une certification sur la gestion et non sur le traitement. L'al. 2 décrit quels sont les éléments qu'un système de gestion de la protection des données (SGPD) doit fournir pour une évaluation (soit une charte de protection des données, un document sur les objectifs et

mesures garantissant la protection des données et les moyens techniques nécessaires pour réaliser ces objectifs). Selon l'al. 3, le PFPDT prévoit des directives sur les exigences d'un SGPD qui doivent se baser sur les normes : « Il tient compte des normes internationales relatives à l'installation, l'exploitation, la surveillance et l'amélioration de systèmes de gestion, dont en particulier les normes ISO 9001:2000 [remplacée depuis par la norme ISO 9001:2008] et ISO/CEI 27001:2005 [remplacée par la norme ISO/CEI 27001:2013 depuis le 19 mars 2014] » (art. 4 al. 3 OCPD). Ces normes traitent respectivement du management de qualité et de la sécurité de l'information[40]. Quant aux directives[41], elles sont entrées en vigueur le 1er septembre 2008. Elles réinterprètent certaines dispositions des normes ISO et formulent neuf exigences minimales inspirées des principes de base de la LPD, dont 20 mesures, à savoir, pour les citer telles quelles, la licéité (motifs justificatifs, base légale, traitement de données par un tiers), la transparence (bonne foi, reconnaissabilité, obligation d'informer), la proportionnalité (traitement proportionnel), la finalité (spécification et modification de la finalité, limitations d'utilisation), l'exactitude (exactitude des données, rectification), la communication transfrontière (niveau de protection adéquat), la sécurité des données (confidentialité, intégrité, disponibilité, traitement des données par un tiers), l'enregistrement des fichiers (obligation de déclarer [avec les exceptions], inventaire des fichiers non déclarés) et le droit d'accès et de procédure (droit d'accès à ses propres données, prétentions et procédures). Un code de bonne pratique pour la gestion de la protection des données basé sur la norme ISO/CEI 27002 (sécurité de l'information) vient compléter les exigences minimales. Le PFPDT a adapté ses directives à la norme ISO/CEI 27001:2013 depuis le 19 mars 2014 (PFPDT 2014). En outre, le modèle SGPD doit se baser sur le modèle PCDA (*Plan*, *Do*, *Check*, *Act*) qui demande un contrôle régulier du système en vue de l'améliorer (Commentaire OCPD, consid. 4.1.2).

[40]Voir www.iso.org

[41]Directives du 16 juillet 2008 sur les exigences minimales qu'un système de gestion de la protection des données doit remplir.

La certification de produits est traitée à l'art. 5 OCPD. Cela concerne « les produits servant principalement au traitement de données personnelles ou générant, lors de leur utilisation, des données personnelles concernant notamment l'utilisateur » (art. 5 al. 1 OCPD). Cela concerne entre autres les navigateurs Internet, les logiciels gérant des serveurs, les systèmes reposant sur la technologie RFID, GPS (Commentaire OCPD, consid. 5.1), ou encore les logiciels de gestion du personnel, des patients ou les logiciels détectant les failles (Meier 2010, §1439). Selon l'art. 5 al. 2 OCPD, le produit doit satisfaire à des exigences de sécurité (let. a), des exigences de proportionnalité (let. b), des exigences de transparence (let. c) et mettre en œuvre des mesures techniques afin de satisfaire à ses exigences (let. d) (selon les termes utilisés par Meier 2010, §1440). Les directives devant être énoncées par le préposé en vertu de l'art. 5 al. 3 OCPD n'existent pas : au terme des discussions d'un groupe de travail en 2010, il a été décidé de geler les travaux pour des raisons de difficulté d'établir des directives précises sur la certification de produits, un constat qui était similaire en France et en Allemagne[42]. En attendant, les directives reprennent les normes de l'*Unabhängige Landeszentrum für Datenschutz (ULD*) du *Land* allemand de Schleswig-Holstein, qui sont reconnues comme précurseur en la matière (Belleil 2009, p. 149).

Deux problèmes majeurs de la certification existent. Premièrement, la certification garantit un respect des principes fondamentaux de la LPD seulement au moment de la certification (Meier 2010, §1416), aucune garantie n'est possible après la certification. Selon Meier (*ibid*.), « les standards à appliquer sont souvent vagues et leur respect n'est vérifié que sur le papier ». Deuxièmement, la certification est octroyée par un organisme de certification agréé et non par le PFPDT. Selon l'OFJ, cette option permet de soutenir l'initiative privée et de réduire la densité normative de l'ordonnance (Commentaire de l'OCPD, p. 1). La valeur de la certification diminue, sachant qu'il y a « autant de labels que d'organismes de certification » (Cottier 2007, p. 6), un environnement qui ne facilite pas la tâche du consommateur (Meier 2010, §1413).

[42]http://www.edoeb.admin.ch/datenschutz/00756/00757/index.html?lang=fr

7.1.3.2 INTÉGRER LA PRIVACY BY DESIGN DANS LA PROCÉDURE DE CERTIFICATION

Face à la multitude de labels, une première solution serait d'incomber la tâche au PFPDT de certifier des labels officiels. Cette solution exigerait une revue de l'OCPD par rapport à l'institution des organismes de certification et les dispositions qui les lient aux organisations. Une telle démarche existe en France par exemple où trois labels[43] sont délivrés par la CNIL comme le prévoit l'art. 11 al. 3 let. c Loi 17-78[44]. Le premier label « audit de traitement » est à destination des audits de traitement, qui examinent un traitement de données conforme à la loi française, et décrit les exigences sur les modalités de réalisation des audits. Le deuxième label « formation informatique et libertés » certifie les organismes proposant des formations de correspondants « informatique et libertés ». Le troisième label « coffre-fort numérique » est une certification instaurée en janvier 2014 (les deux autres furent instaurés en juin 2012) portant sur les produits ; elle se destine aux responsables de traitement et possède des exigences à propos des données traitées, de l'accès aux données, de la conservation de celles-ci, de l'information aux personnes concernées et des mesures de sécurité[45].

Il est possible d'imaginer l'introduction de labels officiels décernés par le PFPDT. Ceux-ci porteraient sur les questions d'organisation et sur les produits, comme c'est le cas actuellement. Concernant la *privacy by design*, c'est surtout par rapport aux produits que la démarche est intéressante, car elle traite des systèmes de traitement des données. De plus, sachant qu'il existe un gel des travaux sur les normes à utiliser par rapport à la certification de produits, ce serait l'occasion pour le PFPDT de créer ses propres normes. Ainsi, les responsables de traitement décidant d'inclure les principes de *privacy by design*, en plus du respect des autres principes de la LPD, pourraient recevoir un label directement du PFPDT.

[43] http://www.cnil.fr/linstitution/labels-cnil/
[44] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[45] http://www.cnil.fr/linstitution/actualite/article/article/un-nouveau-label-pour-les-services-de-coffre-fort-numerique/

Le PFPDT aurait alors deux nouvelles compétences : la capacité de créer un label, ce qui va plus loin que la formulation de directives sur les exigences minimales qui existent déjà, et la capacité à décerner le label. Cela exigerait premièrement une réforme du statut du PFPDT pour qu'il puisse faire partie des « organismes d'évaluation de la conformité publics suisses » tels que prévus dans l'OAccD (art. 4 al. 1 let. b). Cette nécessité découle du fait que la compétence d'accréditation relève du SAS, la création d'un label étant comparable à la création d'une marque déposée. L'OCPD devrait être revue en prenant compte du fait que le PFPDT est aussi un organisme de certification, ce qui a des conséquences sur les dispositions traitant des relations entre organisme de certification et le préposé (notamment sur le fait que l'organisme de certification doit informer le PFPDT en cas de manquement de l'organisation certifiée [art. 9 et 10 OCPD]). Deuxièmement, le PFPDT devrait intégrer des modalités de formulation de demande (par exemple un formulaire disponible en ligne) et les moyens de traiter les demandes pour accorder ou non, et sous quelles conditions, un label. L'ajout de ces nouvelles compétences aboutirait à une simplification du processus de labellisation ; les directives du PFPDT s'appliqueraient directement dans les labels sans qu'un contrôle soit nécessaire. Mais cela demanderait un plus grand travail du PFPDT, qui est déjà surchargé en l'état actuel (voir point 7.4.4). La question de l'existence de labels officiels et de labels privés peut se poser. Ces derniers pourront être perçus avec une valeur moindre que leurs homologues publics, car le contrôle sur les certifications privés est moins intense et car il en existe plus d'un ; cela pose la question de la nécessité de la coexistence d'un régime de certification privé et public.

Une telle solution paraît efficace dans le cadre de la promotion de l'autorégulation, mais le problème majeur de l'effectivité des pratiques demeure : une fois que la certification est attribuée, rien n'empêche à l'organisme de manquer à ses devoirs. De tels manquements ne seraient alors perçus que lors d'éventuels contrôles.

Une deuxième solution serait la création d'un label officiel sans donner la compétence au PFPDT de les décerner. Il s'agit d'une solution qui avait évoquée – mais écartée – lors de la réflexion sur un régime de

certification (Commentaire de l'OCPD, introduction). Les arguments en défaveur de cette solution étaient la grande densité normative que cela représenterait et l'introduction d'une activité étatique dans un secteur avant tout privé. Cette solution va moins loin que la précédente et ne modifie que peu l'état actuel de la législation. Aussi, elle peut manquer d'une certaine cohérence : pourquoi donner la compétence de créer un label sans pouvoir le décerner ? Un autre problème vient du fait qu'il n'y a pas de différence pour un organisme de certification à décerner un label public ou privé, si ce dernier est réalisé en fonction des directives du PFPDT et des normes ISO exigées.

Une dernière solution qui n'implique pratiquement pas de changement dans la législation actuelle est d'intégrer une nouvelle norme ISO dans les directives actuelles. Il serait possible de rattacher la certification à des normes qui concernent la *privacy by design*. Or c'est notamment le cas de la norme ISO 29000 « *Privacy Framework* » (Bensoussan 2014). La norme est également évoquée par l'initiatrice du concept de *privacy by design*[46]. La norme contient onze principes, dont la limitation de la collecte des données, la minimisation des données collectées, la limite de l'utilisation des données (Hoepman 2012, p. 7). Une telle approche devrait faire intégrer explicitement la mention d'une nouvelle norme ISO dans l'OCPD à l'art. 4 sur les certifications de gestion et dans les directives du PFPDT. Le régime de certification ne changerait pas, mais les nouveaux labels privés incluraient alors les principes de protection dès la conception.

7.1.4 ANALYSE DE L'APPROCHE AUTORÉGULATRICE

Introduire la protection de la vie privée dès la conception en promouvant des mécanismes d'autorégulation est une solution flexible qui tient compte des intérêts économiques et se base avant tout sur la responsabilité des individus. Avec un système de labels, ils pourraient être informés des pratiques de certaines organisations et de l'utilisation de certains produits. Cette dynamique va de pair avec la sensibilisation de la population quant aux conséquences de l'utilisation de certains outils. Elle part du principe que le développement d'outils

[46] http://saisa.eu/blogs/Guidance/?p=922

technologiques suivra son cours, permettant aux individus de se protéger eux-mêmes. Notons également qu'une logique similaire a cours dans d'autres domaines, notamment avec le développement des P3P (voir point 6.1.3) dans le monde du web. Si les travaux du W3C sur les paramètres de *privacy* aboutissent, il se pourrait qu'il y ait une généralisation de ce label dans l'ensemble du web, ce qui compléterait bien la dynamique de labels en Suisse, si c'est l'option suivie.

Un certain nombre de critiques peuvent être adressées à cette approche. Tout d'abord, elle ne répondrait que très partiellement au problème de l'inadéquation de la loi. Nous avons vu que l'évolution technologique implique la multiplication de moyens de capter des données et la multiplication des données captées. Dans un contexte généralisé de collecte des données, l'appel à la responsabilité individuelle est utopiste. Le recours à des labels permettrait d'orienter une personne, mais face à l'ubiquité des moyens de collecte, la tâche devient très difficile.

Une critique de l'autorégulation affirme que la protection des données deviendrait une option commerciale (Belleil 2009, p. 150), plutôt qu'un droit. Un consommateur pourrait se trouver devant un choix entre des prestations différenciées selon qu'elles respectent ou non la protection des données. On serait tenté d'accorder la priorité à une prestation apportant un confort d'utilisation en contre-partie d'une collecte pas forcément régulée. C'est en somme le problème de la capacité des individus à lire les paramètres de confidentialité d'un site, les moyens de collecte d'un appareil, la réputation d'un label, etc. Si cela devient trop coûteux en terme d'investissement, le contrôle préalable de l'individu n'est alors plus réalisé (Vila, Greenstadt et Molnar. 2003).

En outre, certains auteurs estiment que l'autorégulation est caractérisée par une instabilité (*ibid.*). Ils partent du principe que plus les entreprises ont tendance à renforcer leur protection des données, moins les consommateurs sont vigilants à ce sujet ; en conséquence, face au déclin d'attention des consommateurs sur l'utilisation de leurs données, les entreprises tendent alors à moins respecter la protection des données et à exploiter les données des clients, et ainsi de suite.

Enfin, notons qu'intégrer la *privacy by design* de manière non contraignante va à l'encontre des dynamiques internationales en cours. Que ce soit au niveau de l'Union européenne par les projets de règlement et de directive ou au niveau du Conseil de l'Europe, la *privacy by design* est perçue comme un principe essentiel. Sachant que la Suisse doit tenir compte des évolutions sur la question dans le contexte européen, l'introduction de la protection de la vie privée comme principe, soit une solution contraignante, paraît plus plausible. C'est ce dont nous allons traiter dans le point suivant.

7.2 INTERVENTION N°2 : LA *PRIVACY BY DESIGN* COMME NOUVEAU PRINCIPE APPLICABLE DANS LA LOI

La deuxième solution proposée est d'introduire la *privacy by design* de façon contraignante. Une telle application se justifie premièrement par le fait que les révisions européennes vont toutes dans ce sens. Les projets de règlement et de directive européens vont dans cette direction en incluant explicitement la protection de la vie privée dès la conception, de même que le projet de modernisation de la Conv. 108. De plus, déjà lors de la révision de 2006, malgré le renforcement et l'ajout de nouvelles dispositions, la doctrine juridique pointait du doigt le manque d'audace du législateur (voir par exemple Cottier 2007, Meier 2007, Bondallaz 2008), d'autant plus que le processus helvétique de réforme législative est lent. Le PFPDT montre également sa volonté d'intégrer la *privacy by design* de manière approfondie (Thür 2012, Walter 2012a).

Nous allons donc premièrement nous intéresser à l'intégration de la protection dès la conception en tant que principe dans la LPD, puis nous verrons les moyens de rendre l'application du principe efficace, c'est-à-dire intégrer au mieux la logique de prévention, l'essence du concept de *privacy by design*.

7.2.1 FAIRE DE LA *PRIVACY BY DESIGN* UN NOUVEAU PRINCIPE

L'intégration d'une disposition stipulant la *privacy by design* dans la législation suisse n'est pas simple. S'agissant d'un concept à portée générale et fondamental – c'est ainsi qu'il fut définit par son initiatrice –

on serait d'abord tenté de faire de la protection de la vie privée dès la conception un nouveau principe.

Comme nous l'avons vu, la LPD établit déjà une liste de principes dans son première section. La première idée est de savoir s'il est possible de faire de la protection de la vie privée dès la conception un principe en plus de ceux définis à l'art. 4 LPD (licéité, proportionnalité, bonne foi, reconnaissabilité, consentement). Cette perspective se heurte à deux problèmes.

Premièrement, la *privacy by design* ne peut s'ajouter aux principes dans la loi, car dans cette notion, il s'agit de faire respecter les principes essentiels *déjà définis* dans la loi dès la conception. En somme, elle se caractérise avant tout par le *déplacement dans le temps du respect des principes définis dans la loi* (en amont) et moins comme un principe supplémentaire. Deuxièmement, évoquer une protection de la vie privée dès la conception fait intervenir justement la « conception » d'un outil ou système traitant les données et non le traitement des données en lui-même. La création de nouveaux systèmes traitant les données et le traitement réalisé par un maître du fichier sont deux opérations à distinguer.

L'intégration d'un principe de *privacy by design* pourrait se faire dans la section de la LPD « Dispositions générales de protection des données », sans pour autant figurer dans l'art. 4 LPD, au même titre que l'art. 5 et l'art. 7 LPD sur l'exactitude et la sécurité des données. Sachant que le maître du fichier est « la personne privée ou l'organe fédéral qui décide du but et du contenu du fichier » (art. 3 LPD let. i), la protection de la vie privée dès la conception lui incombera ; il s'agirait alors d'une nouvelle responsabilité du maître du fichier.

Voici une proposition pour article intitulé « Protection de la vie privée dès la conception » :

> *1. Le maître du fichier applique le principe de protection de la vie privée dès la conception.*
>
> *2. Il applique les mesures et procédures techniques et organisationnelles appropriées en tenant compte :*

a. des techniques les plus récentes ;

b. des coûts liés à leur mise en œuvre.

Cette proposition s'inspire grandement de la définition de la protection dès la conception apparaissant dans les propositions de directive (art. 19) et de règlement (art. 23) européennes, adaptées de telle sorte à ne contenir qu'une idée par alinéa. Une telle proposition intègre directement la notion de protection des données la conception, ce qui demanderait alors une définition du terme « conception » dans l'art. 3 LPD. Les « mesures et procédures techniques et organisationnelles » est suffisamment large pour englober tout un panel d'outil et fait référence au fait que la technique permet de résoudre les enjeux de la *privacy by design*. Sachant que la technologie ne permet pas forcément de résoudre un problème, l'ajout des « mesures organisationnelles » permet d'autres possibilités.

La question de la définition d'un tel principe peut être discutée, car la protection des données dès la conception est une forme de proportionnalité : il s'agit en somme de prévoir dès la conception l'adéquation d'un moyen de traitement à un but défini et ce principe existe déjà dans la LPD. L'enjeu sera de savoir si la mention explicite d'une protection en amont est nécessaire. Si l'on suit la logique de responsabilisation des maîtres du fichier, cette mention sera utile.

Quoiqu'il en soit, l'ajout du principe de *privacy by design* ne suffit pas. Une simple mention du principe ne change pas essentiellement la logique qui doit passer à celle de la protection à celle de la *prévention* qui est le concept au cœur de la *privacy by design*. De ce fait, il devrait être possible de contrôler sa mise en place. L'ajout d'un principe ne garantit pas son respect, le PFPDT devrait avoir un moyen de contrôler l'application de ce nouveau principe. C'est ce dont il sera question dans le point suivant.

7.2.2 INTÉGRER LA LOGIQUE DE PRÉVENTION

Prévoir une protection dès la conception exige l'existence d'une possibilité de contrôler qu'un système soit créé dans le respect de ce principe. La révision de 2006 de la LPD a apporté deux manières de

renforcer la protection des données et responsabiliser les responsables de traitement : il s'agit du recours à un conseiller à la protection des données et à la certification. S'ils sont actuellement incitatifs et non obligatoires, nous allons voir comment ils peuvent faire en sorte d'assurer la protection dès la conception.

7.2.2.1 LE RECOURS À UN CONSEILLER À LA PROTECTION DES DONNÉES[47]

Mettre en place une disposition de *privacy by design* correspond à réaliser une intervention sur une entreprise (ou un organe fédéral, dans une moindre mesure) susceptible de développer de nouveaux outils traitant les données. Si le législateur désire utiliser la contrainte sur l'entreprise, un suivi doit pouvoir être effectué. Cela peut être possible grâce à un conseiller à la protection des données.

Le projet de directive de l'UE fait mention d'un nouveau rôle que pourrait avoir le « délégué à la protection des données à caractère personnel » évoqué dans la Directive 95/46/CE. Par rapport à la *privacy by design*, on peut lire à l'art. 32 du projet de directive que « les États membres prévoient que le responsable du traitement ou le sous-traitant confie au délégué à la protection des données au moins les missions suivantes »:

> [...]
>
> *(b) contrôler la mise en œuvre et l'application des règles internes en matière de protection des données à caractère personnel, y compris la répartition des responsabilités, la formation du personnel participant aux traitements, et les audits s'y rapportant;*
>
> *(c) contrôler la mise en œuvre et l'application des dispositions adoptées conformément à la présente directive, notamment en ce qui concerne les exigences relatives à la protection des données dès la conception, à la protection des données par défaut et à la sécurité des données, ainsi que l'information des personnes concernées et l'examen des demandes présentées*

[47] Nous utiliserons les deux termes de conseiller et délégué.

> *dans l'exercice de leurs droits au titre des dispositions adoptées conformément à la présente directive;*
>
> [...]

Un tel délégué existe déjà dans plusieurs pays européens. C'est le cas de la France, la Suède, les Pays-Bas, le Luxembourg et l'Allemagne. Pour cette dernière, contrairement aux autres, la nomination d'un délégué est obligatoire pour les secteurs privé et public, avec certaines conditions. La France l'a mis en place depuis 2004 (« correspondant informatique et libertés », CIL) et il existe une formation spécifique à ce poste depuis sept ans[48]. Selon Cottier, « [cet organe] a contribué efficacement au développement de la protection des données au sein des collectivités publiques et des entreprises privées » (2007, p. 6). L'Association française des correspondants à la protection des données (AFCDP) estime par ailleurs que le correspondant informatique et liberté est le garant de l'application de la protection dès la conception : « le CIL intervient en amont de tout projet de traitement de données ; et pour mener à bien sa mission doit procéder à une analyse des conséquences du projet sur la vie privée et les libertés individuelles des personnes concernées. C'est à partir de cette analyse qu'il va indiquer au responsable de traitements si le projet nécessite l'intégration de certaines fonctionnalités au stade même de la conception. Le DPO [*Data Protection Officer]* joue donc un rôle clé dans le processus de « Privacy by Design » et du « Security by Design » » (AFCDP 2004).

En Suisse, une solution analogue peut être envisagée. La LPD introduit le conseiller interne à la protection des données à l'art. 11a. Selon l'article, les personnes privées « sont tenues de déclarer leurs fichiers » (art. 11a al. 3 LPD) si « elles traitent régulièrement des données sensibles ou des profils de la personnalité » (art. 11a al. 3 let. a LPD) et si « elles communiquent régulièrement des données personnelles à des tiers » (art. 3 al. 3 let. b LPD). Les fichiers sont tenus dans un registre du PFPDT en ligne. L'al. 5 LPD expose les dérogations pour lesquelles « le maître du fichier n'est pas tenu de déclarer son fichier », parmi lesquelles figure la désignation d'un « un conseiller à la protection des

[48] http://www.informatique-et-libertes-formation.fr/

données indépendant chargé d'assurer l'application interne des dispositions relatives à la protection des données et de tenir un inventaire des fichiers » (art. 11a al. 5 let. e LPD)[49].

Les dispositions concernant le conseiller à la protection des données sont définies dans l'OLPD. Actuellement, les tâches du conseiller à la protection des données sont les suivantes (art 12b al. 1 OLPD) :

« a. contrôler les traitements de données personnelles et de proposer des mesures s'il apparaît que des prescriptions sur la protection des données ont été violées;

*b. dresser l'inventaire des fichiers gérés par le maître du fichier mentionné à l'art. 11*a*, al. 3, LPD et de le tenir à la disposition du préposé ou des personnes concernées qui en font la demande. »*

Si les tâches de contrôle des traitements et de proposition de mesures évoquées ci-dessus sont des actions effectuées *a posteriori*, le contrôle est supposé avoir déjà lieu plus en amont dans la réalisation des projets d'une entreprise « même si l'ordonnance ne le prévoit pas expressément » (Commentaire OLPD, consid. 7.1.2). Il s'agit de conseils et de formation du personnel sur les aspects de protection des données.

---

[49] Les dispositions prévoyant une dérogation sont les suivantes :
a. « si les données sont traitées par une personne privée en vertu d'une obligation légale »;
b. « si le traitement est désigné par le Conseil fédéral comme n'étant pas susceptible de menacer les droits des personnes concernées »;
c. « s'il utilise le fichier exclusivement pour la publication dans la partie rédactionnelle d'un média à caractère périodique et ne communique pas les données à des tiers à l'insu des personnes concernées »;
d. « si les données sont traitées par un journaliste qui se sert du fichier comme un instrument de travail personnel » ;
e. « s'il a désigné un conseiller à la protection des données indépendant chargé d'assurer l'application interne des dispositions relatives à la protection des données et de tenir un inventaire des fichiers »;
f. « s'il s'est soumis à une procédure de certification au sens de l'art. 11, a obtenu un label de qualité et a annoncé le résultat de la procédure de certification au préposé ».

En outre, « il donnera son avis sur tous les projets qui touchent la protection des données, ce qui implique qu'il doit être consulté par le maître du fichier avant la mise en œuvre de tout nouveau traitement. Il fera également régulièrement rapport au maître du fichier sur son activité. » (Commentaire OLPD, consid. 7.1.2). Ces tâches ne figurent pas dans l'ordonnance, de ce fait, la question d'un caractère obligatoire ou non de ces tâches est « controversée » selon Meier (2010, note 1416).

L'art. 12 al. 2 OLPD stipule que le conseiller doit disposer des moyens nécessaires à l'exercice de ses tâches et des compétences requises. Parmi ces compétences, le PFPDT recommande notamment de bien connaître l'entreprise, d'avoir une formation juridique (ou bénéficier d'une formation interne ou encore d'avoir travaillé six mois dans le domaine de la protection des données) et d'avoir les compétences techniques spécialisées nécessaires selon le type d'entreprise (par exemple des connaissances de programmation)[50]. Selon les termes du PFPDT, il s'agit d'une indépendance sur le plan matériel.

La désignation du conseiller relève de la compétence du maître du fichier. Aux termes de l'art. 12a OLPD, ce dernier « peut désigner un collaborateur ou un tiers en qualité de conseiller à la protection des données ». Le maître du fichier a le choix, mais la désignation d'un tiers est une garantie d'indépendance supplémentaire (Cottier 2007, p. 6 ; Meier 2010, §1452). Quand il s'agit d'un collaborateur interne, un certain nombre de critères doivent être respectés afin d'éviter les conflits d'intérêts. Il ne peut être à la fois conseiller à la protection des données et membre de la direction, collaborateur RH ou encore avoir des fonctions dans l'administration des systèmes d'information. Il peut en revanche faire partie du service de sécurité informatique ou du service juridique (Commentaire OLPD, consid. 7.1.1).

La responsabilité du traitement de données repose sur le maître du fichier, soit l'entreprise, et non sur le conseiller à la protection des données, même si le maître du fichier a suivi les directives de son conseiller (Meier 2010, §1457 ; Cottier 2007, p. 6).

[50] http://www.edoeb.admin.ch/datenschutz/00626/00743/00874/01051/index.html?lang=fr

Le conseiller n'a pas un pouvoir « coercitif » sur l'entreprise si cette dernière ne suit pas ces recommandations. L'OFJ explique : « Il convient enfin de relever que ni la loi ni l'ordonnance ne confèrent au conseiller à la protection des données le droit de porter l'affaire devant le préposé si ses recommandations ne sont pas suivies. Il peut par contre dans l'exercice de ces tâches demander conseil au préposé, conformément à l'article 28 LPD » (Commentaire OLPD, consid. 7.1.2). Il paraît difficile à concevoir qu'un conseiller qui est un collaborateur interne saisisse le PFPDT sans que cette action entraîne des conséquences pour sa personne (ici, la question de l'indépendance fait surface). S'il y a violation manifeste des principes de protection des données, aucune conséquence « directe » n'a lieu. Une violation ne pourra être détectée que postérieurement. Le PFPDT explique que dans un tel cas, la seule conséquence est que l'image de l'entreprise sera dégradée[51].

7.2.2.2 RENFORCER LA FONCTION DE CONSEILLER À LA PROTECTION DES DONNÉES

En ayant considéré tous ces aspects, la protection de la vie privée dès la conception exigerait alors :

- l'obligation pour les entreprises de faire appel à un conseiller aux données personnelles
- l'instauration d'une nouvelle tâche à ce conseiller, consistant à avoir un regard sur tout nouveau projet de nouvel outil traitant des données
- la permission pour lui de porter une affaire devant le PFPDT

Cela exigerait premièrement de détacher l'institution d'un conseiller à la protection des données de l'idée d'allègement administratif. Un tel conseiller ne serait plus une option, mais une obligation. Vient ensuite la question du critère qui détermine la nécessité d'avoir à faire appel à un conseiller. Le projet de règlement européen en propose trois ; la désignation d'un délégué à la protection des données a lieu si l'organisme est public, s'il s'agit d'une entreprise employant plus de 250 personnes et enfin si « les activités de base du responsable du traitement ou du sous-traitant consistent en des traitements qui, du fait de leur

[51] http://www.edoeb.admin.ch/datenschutz/00626/00743/00874/01051/index.html?lang=fr

nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique des personnes concernées » (art. 35 al. 1 let. c de la proposition de règlement). Le texte adopté le 12 mars 2014 par le Parlement européen propose de remplacer le critère de grandeur d'une entreprise par le fait qu'elle réalise un traitement portant sur plus de 5000 personnes concernées et sur une période de douze mois consécutifs et ajoute le critère du traitement de données « sensibles » (selon la dénomination helvétique).

En Suisse, une adaptation similaire est possible. Ce type de critères que nous venons d'évoquer existe pour le moment dans la LPD par rapport à l'obligation des maîtres du fichier à déclarer les fichiers au préposé (art. 11a LPD). Ce devoir de déclarer à lieu s'il s'agit d'un organe fédéral, si un traitement régulier de données sensibles a cours et si les entreprises communiquent régulièrement des données à des tiers. Des dispositions analogues – ainsi que les exceptions – peuvent être adaptées pour une obligation de désigner un conseiller. Reste à savoir si le critère de taille de l'entreprise peut être retenu. A notre avis, l'activité d'une entreprise est avant tout le critère pertinent. La taille d'une entreprise n'a pas d'incidence sur l'intensité d'un traitement de données.

Il paraît opportun de reprendre une disposition similaire à celle de l'art. 35 al. 1 let. c de la proposition de règlement européen (voir plus haut). Il s'agit d'une disposition très générale qui englobe toute une série d'activités possibles, dont la communication à des tiers par exemple.

Dans l'idée d'assurer la protection de la vie privée dès la conception, le conseiller à la protection des données devrait posséder une nouvelle tâche, en plus de son contrôle du traitement et de la tenue de l'inventaire des fichiers qu'il est en mesure d'effectuer actuellement. La proposition de règlement européen prévoit qu'il puisse « contrôler la mise en œuvre et l'application du présent règlement, notamment en ce qui concerne les exigences relatives à la protection des données dès la conception, à la protection des données par défaut et à la sécurité des données, ainsi que l'information des personnes concernées et l'examen des demandes présentées dans l'exercice de leurs droits au titre du présent règlement » (art. 37 al. 1 let. c de la proposition de règlement). Si la loi suisse prévoit d'ajouter la *privacy by design* comme principe, alors il sera possible de

l'évoquer explicitement dans une nouvelle tâche du conseiller. Il serait en mesure de certifier un produit de l'entreprise s'il respecte les principes de protection des données (Mouchard 2013, p. 24).

Si le conseiller peut émettre des recommandations sur un projet d'une entreprise, il faut que cette dernière soit obligée de les suivre, sinon le principe de *privacy by design* n'aurait aucune portée. Ce n'est pas le cas actuellement. Dans le cas où une entreprise refuserait de suivre les recommandations d'un conseiller, il n'y a aucun moyen d'action pour ce dernier, si ce n'est qu'il peut demander conseil au PFPDT en vertu de l'art. 28 LPD (Commentaire OLPD, consid. 7.1.2). Une réelle collaboration est nécessaire, similaire à ce que prévoit la proposition de règlement européen à l'art. 35 al. 1 let. g qui exige du délégué qu'il coopère avec l'autorité de contrôle à la demande de cette dernière ou de sa propre initiative. Mais comme nous l'évoquions précédemment, dans le cas où une entreprise décide délibérément de refuser des recommandations du conseiller, celui peut difficilement agir « contre » l'entreprise qui l'emploie aux risques de représailles éventuelles, surtout si le conseiller est à l'origine un employé de l'entreprise et non un tiers. Le risque de violation du secret des affaires existe également (Meier 2010, §1452). Se pose alors la question de l'indépendance du conseiller : afin qu'il puisse exercer son rôle au mieux et qu'il puisse coopérer avec le PFPDT, voire porter une affaire devant lui, il doit pouvoir être indépendant. Un tiers désigné comme conseiller répond plus à ces exigences. Un dilemme se pose alors. Soit on imagine que le maître du fichier soit obligé de désigner un tiers comme conseiller, ce qui est une charge très importante pour l'entreprise et une « ingérence » importante de l'Etat dans son fonctionnement, mais une pratique qui garantit une plus grande indépendance du conseiller et ainsi une meilleure efficacité dans son rôle ; soit il est laissé aux maîtres de fichier la possibilité de nommer un collaborateur de l'entreprise, ce qui lui laisse une certaine liberté, mais qui risque d'affecter l'effectivité d'une protection dès la conception.

Une autre difficulté sera de déterminer le profil du conseiller. Les tâches qu'il possède se situent entre le droit et les éléments purement techniques. Dans le cas d'une obligation de désigner un conseiller, il sera

opportun de définir les modalités entendues comme « compétences professionnelles nécessaires » (art. 12a al. 2 OLPD).

Les expériences nationales quant à la question du délégué à la protection des données sont globalement positives. L'institution d'un tel acteur est similaire dans les grands principes d'un pays à l'autre (voir AFCDP 2009a et 2009b pour une comparaison détaillée des cas de la Suède, de l'Allemagne, du Luxembourg, de la Suisse, de la France et des Pays-Bas). Parmi les points importants, nous citerons premièrement la désignation obligatoire des délégués en Allemagne. Les modalités de désignation sont définies aux art. 4f, 4g de la *Bundesdatenschutzgesetz* (BDSG[52]). Les conditions de la désignation sont différentes selon qu'il s'agisse du secteur privé, du secteur public fédéral ou du secteur public des *Länder* et dépend également du mode de traitement (automatisé ou manuel). Concernant les conditions d'exercice, les Pays-Bas et l'Allemagne confèrent un statut protégé au délégué ; aux Pays-Bas, il dispose en plus de compétences étendues de contrôle administratif[53] comme un pouvoir d'investigation, d'accès aux documents, voire même une demande d'assistance de la police. Dans le cadre des relations entre le délégué et l'autorité de protection des données, la tenue d'un registre des délégués a cours aux Pays-Bas et en Suède ; la liste des organisations ayant recours à un délégué est publié sur le site web de l'autorité de contrôle aux Pays-Bas, tandis qu'en Suède, le rapport annuel fait figurer les délégués. Au-delà du registre, les relations entre les délégués et les autorités de protection des données sont étroites avec la possibilité pour le délégué de saisir l'autorité en cas de doute ou de non suivi de recommandations ; à l'inverse, la saisie du délégué par l'autorité est possible en Suède et en Allemagne lorsque l'autorité souhaite recevoir des informations. Notons enfin l'existence d'une association professionnelle des délégués existant aux Pays-Bas (cela a même abouti à la création d'un syndicat[54]) et en Allemagne.

[52]Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist.

[53]http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/etude-de-droit-compare-sur-les-correspondants-a-la-protection-des-donnees/

[54]*ibid*.

Le retour sur l'efficacité des délégués est difficile à réaliser en Allemagne, car il n'existe pas de registre officiel des délégués et une grande diversité de conditions pour lesquelles la désignation d'un délégué est obligatoire. Il est difficile de savoir si la pratique a réellement lieu ; elle peut être perçue comme un obstacle et un fardeau bureaucratique[55]. Aux Pays-Bas et en Suède, de nouvelles revendications sur une amélioration de ce système apparaissent[56] : elles demandent notamment l'organisation de journées de rencontre entre délégués et organisées par l'autorité de protection des données, la mise en place d'un système de formation (c'est le cas en France), un meilleur suivi des délégués ou encore un renforcement des liens entre délégué et autorité, notamment par la mise en place d'une *hotline* spéciale, d'un accès réservé aux délégués à une partie du site web de l'autorité et l'instauration d'une personne de contact pour les délégués. L'idée sous-tendant le renforcement du suivi du délégué est qu'il puisse avoir les moyens de « tenir tête » à l'organisation pour laquelle il travaille en cas de conflit, « ils se sentent mieux armés pour défendre des positions parfois impopulaires auprès de la direction de leur organisation »[57].

7.2.3 ANALYSE DE LA SOLUTION CONTRAIGNANTE

La solution d'intégrer la *privacy by design* comme nouveau principe, en garantissant sa mise en place avec un conseiller obligatoire à la protection des données, paraît une option plausible, au vu des développements en cours. De plus, la solution est à même de répondre aux problèmes déjà définis. Obliger les responsables de traitement à se responsabiliser quant au traitement des données à long terme permet aux individus de se mouvoir dans un environnement en toute confiance. Ces exigences techniques et organisationnelles pourraient par contre être mal perçues par les personnes privées, car il s'agit de faire porter sur elles une charge importante, mais c'est pour les défenseurs d'une telle solution un « mal nécessaire » pour faire respecter les droits fondamentaux des citoyens.

---

[55] *ibid.*
[56] Le résumé des revendications a été réalisé par la CNIL : *ibid.*
[57] *ibid.*

Le renforcement de la procédure d'institution de délégués à la protection des données permet non seulement de mettre en place le principe de protection de la vie privée dès la conception, mais également garantit un contrôle sur d'autres aspects du traitement de données, comme la communication transfrontière ou le principe de transparence. Un délégué obligatoire aurait un impact fort qui demanderait un nouveau rôle de supervision du PFPDT, tâche supplémentaire, qui paraît difficile à mettre en place actuellement au vu des ressources actuelles du PFPDT ; nous aborderons ce point en détail au point 7.4.4. La création d'un nouveau régime dans lequel une nouvelle profession de délégué à la protection des données se mettrait en place serait un signal fort pour mettre en lumière les enjeux de la protection des données dans la société et responsabiliser les maîtres du fichier sur la question.

La question de l'utilité du registre des fichiers se pose également. Du moment que la désignation d'un délégué devient obligatoire, l'allègement administratif qui existe en contre-partie devient obsolète. Une suppression semble plausible, car il est peu utilisé dans les faits (OFJ 2011) et elle avait déjà été évoquée lors de l'avant-projet de la révision de 2008, concernant les personnes privées (Meier 2010, §1468). En cas d'abrogation des dispositions sur l'obligation de déclarer des fichiers, il faudra néanmoins tenir compte des modalités pour réaliser un droit d'accès efficace, ce qui est l'un des buts du registre.

7.3 LES APPLICATIONS DE LA *PRIVACY BY DESIGN*

Dans ce point, nous allons traiter de l'application concrète de la *privacy by design*. Nous retiendrons deux facettes : le principe d'utilisation économe des données et la *privacy by default*. L'objectif d'atteindre une protection des données dès la conception d'un système est en réalité très lié à faire respecter le principe de proportionnalité. En effet, un système traitant les données devrait être construit de façon à utiliser uniquement les informations qui lui sont utiles et pas davantage. Le principe d'utilisation économe des données est l'élément technique permettant d'atteindre ce but, il s'agit donc d'une « une concrétisation du principe de proportionnalité [...] qui instaure une protection préventive » (Bondallaz 2007, §793). Quant à la *privacy by default*, elle permet de proposer des

systèmes avec un haut niveau de protection comme standard minimum, ce qui correspond bien à la philosophie de *privacy by design* ; de plus, si l'utilisateur d'un produit désire qu'il lui soit laissé la possibilité d'accepter une utilisation de ces données, cela est toujours possible, il s'agit consentement explicite.

Nous verrons enfin l'instrument précis à même de concevoir des systèmes protégés : l'étude d'impact.

7.3.1 L'UTILISATION ÉCONOME DES DONNÉES

L'utilisation économe des données est un concept qui ne fait pas partie explicitement de la LPD. Il figure en revanche dans la loi allemande dans les termes de « *Datenvermeidung* » (évitement des données) et de « *Datensparsamkeit* » (minimisation des données) (§ 3a BSGD). Ces deux principes doivent être pris en compte dans la conception de nouveaux systèmes (Meier 2010, §633 ; Bondallaz 2008, §28). Selon Meier, ces deux notions relèvent respectivement de la proportionnalité de principe et la proportionnalité matérielle (2010, §673).

Selon la proportionnalité de principe, un traitement de données répond à un besoin effectif. La notion est liée à la bonne foi et à la finalité. Un exemple est celui de la transmission de données sur la santé d'un individu à une assurance maladie ; une demande d'informations peut être faite par un assureur dans le cadre d'une assurance complémentaire, mais ce n'est pas une nécessité dans le cas d'une assurance de base, comme le veut la loi (*ibid*., §674).

La proportionnalité matérielle fait référence, selon Meier, au choix du mode traitement, à l'étendue des données traitées, à leur nature et aux modalités de communication à des tiers (*ibid*., §676). Ces critères doivent être analysés afin de prévoir le traitement le plus adapté au but recherché. Il s'agit d'éliminer le « superflu » et de ne garder que le strict nécessaire. Pour illustrer la minimisation des données, prenons l'exemple d'une transaction commerciale sur Internet : un vendeur a seulement besoin de savoir quel objet est acheté et si la transaction a été effectuée, sans connaître l'identité de l'acheteur, ni son adresse ; la banque de ce dernier réalise le versement sur le compte du vendeur,

mais elle n'a pas la nécessité de savoir quel article a été acheté, etc. (Dewarte et Gambs, 2010).

Les moyens techniques pour éviter et minimiser les données sont l'anonymisation ou la pseudonymisation, lesquelles sont notamment possibles grâce à la cryptographie et aux PET. L'intensité de l'anonymisation peut varier et être totale ou partielle, cela dépend des moyens à fournir pour ré-identifier une personne. Le PFPDT propose déjà un guide détaillé sur l'utilisation de ces moyens techniques pour anonymiser les données[58].

Cependant, comme nous l'avions déjà vu précédemment, l'anonymisation des données n'est plus une garantie suffisante, car il est possible de les croiser pour ré-identifier une personne (voir point 6.1.1). A l'heure du *data mining*, où les techniques pour explorer les données se perfectionnent, une protection supplémentaire est requise. Il s'agit de faire en sorte que les données ne circulent pas et restent confinées à une structure spécifique : c'est la localisation des données (Langheinrich 2001, p. 13). Par exemple, des données collectées pour le compte d'une entreprise resteraient accessibles seulement pour l'entreprise en question. Le principe est de réguler au maximum la transmission de données ; une telle pratique doit être justifiée.

7.3.2 LA PRIVACY BY DEFAULT

La privacy by default indique que tout système doit être paramétré de façon à garder le plus haut niveau de protection de données. Deux options de paramétrage existent : l'*opt-out* et l'*opt-in*. La première indique qu'un système, par exemple un site web, est par défaut paramétré de façon à traiter les données personnelles ; l'utilisateur doit activement faire part, s'il le souhaite, de son opposition. C'est un consentement implicite au traitement. L'*opt-in* inverse le rapport : l'utilisateur consent par défaut à ce que le traitement des données soit le plus strict possible. Son consentement est requis pour traiter des données personnelles. La mise en place de systèmes *opt-in* permet de garantir alors un haut niveau de protection des différents outils tout en laissant la

[58] Le guide est téléchargeable sur : http://www.edoeb.admin.ch/datenschutz/00628/00629/00636/index.html?lang=fr

possibilité de laisser la possibilité de prélever certaines données consenties.

Ce principe assez puissant en matière de protection des données fait partie des sept facettes de la privacy by design selon Cavoukian (2011a). Il est en étroit lien avec le principe de minimisation des données, mais intègre tout de même la possibilité d'effectuer un traitement au-delà du minimum requis si un individu le désire. Il peut être utilisé dans les situations dans lesquelles il y a un contrat à signer ou une charte à accepter, par exemple sur le web, et conviendrait particulièrement bien à la protection des mineurs, l'un des objectifs édictés par le Conseil fédéral par rapport à la protection des données, eux qui ne sont pas forcément au courant des implications de leurs actions dans l'usage des NTIC. Le risque qui existe toutefois est la proposition de prestations différenciées qualitativement en fonction du consentement ou non d'une personne concernée à être la cible d'un traitement de données.

7.3.3 LA PLACE DE DES PRINCIPES D'ÉCONOMICITÉ DES DONNÉES ET DE LA *PRIVACY BY DEFAULT* DANS L'ORDRE JURIDIQUE

La question se pose par rapport au degré de précision sur la façon dont les outils que nous venons d'évoquer devraient figurer dans les dispositions. Dans le cadre de la neutralité technologique, les termes d'économie des données, d'anonymisation, de pseudonymisation, de *privacy by default* sont à préférer par rapport aux termes plus spécifiques tels que le chiffrement des données, par exemple, car ils sont plus généraux. Sachant qu'ils découlent du principe de proportionnalité, l'intégration de ce principe dans la législation possède deux possibilités : soit ils sont intégrés sous un nouveau principe d'économicité des données figurant dans la deuxième section de la LPD, ce qui marque une orientation claire au maître du fichier, ce risque toutefois d'être redondant par rapport au principe de proportionnalité déjà évoqué, soit ils figurent dans l'OLPD, précisant les concepts de proportionnalité et de protection dès la conception, au risque que leur efficacité soit moindre par rapport à la responsabilisation du maître du fichier.

7.3.4 UN OUTIL PRATIQUE DE MISE EN ŒUVRE DE LA *PRIVACY BY DESIGN* : L'ÉTUDE D'IMPACT

Un outil qui permettrait au conseiller à la protection des données une évaluation efficace des nouveaux outils développés par une entreprise serait l' « évaluation d'impact sur la vie privée » (EIVP, aussi appelée analyse d'impact). La réalisation d'une EIVP consiste à évaluer les risques potentiels d'un nouvel outil ; il se passe en amont d'un projet, ce qui correspond parfaitement à la *privacy by design*. Comme il l'indique dans son dernier rapport d'activités (2013 – 2014), le PFPDT a par ailleurs mis en place un tel outil[59], qui répond selon lui au besoin de sensibilisation aux questions relatives à la protection des données et à la « tendance actuelle du « *privacy by design* » » (p. 67). Le G29 justifie également son utilisation : « L'un des aspects de la prise en compte du respect de la vie privée dès la conception consiste à déterminer les risques du traitement au début du processus pour pouvoir les atténuer » (G29 2012, p. 33). Il est soutenu par d'autres homologues européens du préposé comme la CNIL (Guérin-François 2012). L'EIVP est également prévue dans le projet de règlement européen aux art. 33 et 34 ; la proposition de règlement explique que la réalisation de l'EIVP incombera au responsable de traitement ou à un éventuel sous-traitant.

Selon le G29 qui a notamment réalisé une EIVP sur les puces RFID (G29 2011), cette méthode consiste en deux étapes. Premièrement, la phase d'analyse préalable doit déterminer s'il y a lieu de faire une EIVP ou non et dans le cas où elle apparaît nécessaire, savoir s'il s'agira d'une EIVP complète ou partielle (traitement de données ou non, traitement de données sensibles ou non sensibles, étendue du traitement, etc.). Deuxièmement, en fonction des résultats de la première étape, il s'agira de réaliser l'étude. Pour Oetzel et Spierkerman, qui étudient les analyses d'impact dans le cadre de la *privacy by design*, la réalisation de l'étude peut se diviser en six étapes (2012, p. 6) :

– décrire les caractéristiques du système traitant les données
– définir les cibles (personnes concernées) du système
– évaluer le degré de demande de protection pour chaque cible

[59] Disponible sur https://www.apps.edoeb.admin.ch/dsfa/fr/index.html

- identifier les menaces et leur probabilité pour chaque cible
- identifier et recommander l'application des contrôles existants ou futurs adéquats pour protéger les cibles de ces menaces
- évaluer les risques résiduels

Les modalités de réalisation peuvent varier, mais restent similaires dans les grandes étapes[60]. L'idée majeure dans la volonté d'intégrer la *privacy by design* serait de faire des EIVP l'outil indispensable des conseillers à la protection des données. Reste à savoir si les EIVP doivent être recommandés ou obligatoires. Sachant qu'il s'agit de l'outil le mieux adapté pour évaluer un futur système traitant des données, une obligation paraît pertinente. Une telle démarche exigerait d'intégrer dans une ordonnance les procédures liées à la mise en pratique d'une telle analyse, soit la planification de l'analyse (quand par rapport au développement d'un nouvel outil), la désignation des personnes compétentes à diriger l'évaluation (dans notre proposition, le conseiller à la protection des données), etc.

7.4 CONSIDÉRATIONS GÉNÉRALES

Nous traiterons ici d'autres éléments plus généraux dont il faudra tenir compte afin d'intégrer la *privacy by design*.

7.4.1 LA PRISE EN CONSIDÉRATION DU PROJET DE RÈGLEMENT EUROPÉEN EN SUISSE

Comme le précise le Conseil fédéral, un renforcement de la LPD se fait à la lumière des travaux européens sur la question de la protection des données. L'évolution dans ce domaine aura une influence sur la façon d'intégrer la *privacy by design*, parmi d'autres normes, en Suisse. Dans un premier temps, par sa ratification de la Conv. 108, la Suisse devra intégrer les modifications du texte en cours. Actuellement, selon Mader et Hilti (2012), les dispositions prévues ne sont pas plus contraignantes que ce qui existe déjà en Suisse, une adaptation matérielle paraît donc

[60] L'*Information Commissioner* du Royaume-Uni a réalisé un document complet sur les analyses d'impact, encore différent de celui proposé par le G29. Il est disponible sur http://ico.org.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

peu envisageable. En revanche, si la nouvelle Conv. 108 est adoptée avant la fin des travaux en Suisse, cela exigerait de cette dernière une accélération de ses procédures (*ibid*., p. 3). Dans un second temps, la reprise du futur règlement européen se pose. Pour la Commission européenne, le règlement est un développement de l'acquis de Schengen (Proposition de règlement, consid. 137), mais cet avis n'est pas partagé par le Conseil de l'UE. Si la version de ce dernier est reconnue, « la Suisse serait probablement considérée comme un pays tiers au sens du chapitre V de la proposition » (Mader et Hilti 2012, p. 3), ce qui aurait des conséquences par rapport à l'échange de données entre les parties qui demande un niveau de protection équivalent. Si l'avis de la Commission prime, trois possibilités prévues dans les accords de Schengen/Dublin s'offrent alors à la Suisse (*ibid*., p. 3). En premier lieu, elle peut reprendre seules les dispositions couvertes par les accords, comme ce fut le cas avec la Directive 95/46/CE, qui a provoqué la révision des domaines relavant de l'ancien premier pilier de l'UE, et la Décision-cadre 2008/977/JAI, qui a agi au niveau de la coopération policière et judiciaire en matière pénale. En deuxième lieu, la Suisse reprend la totalité des normes, elle deviendrait ainsi très euro-compatible, avec pour risque une perte de marge de manœuvre (du fait que, par exemple, la définition de certaines modalités de traitement de données incombe à la Commission européenne dans son projet de règlement) ou encore une remise en question des préposés cantonaux, le projet de règlement ne prévoyant pas d'autre autorité de surveillance qu'une autorité nationale (*ibid*., p. 5). Enfin, et même si cela paraît peu probable, la Suisse peut refuser complètement une reprise du règlement européen, ce qui compromettrait les accords de Schengen/Dublin

.Les travaux en cours dans l'UE ou le Conseil de l'Europe auront une influence certaine sur l'agenda suisse en matière de protection des données, mais il est encore difficile de se prononcer précisément, tant il existe encore des inconnues à ce sujet.

7.4.2 LA PORTÉE LIMITÉE DE L'APPLICATION DE CERTAINES DISPOSITIONS À LA SEULE ÉCHELLE NATIONALE

Lorsque nous évoquons les nouvelles technologies comme potentielles menaces à la protection des données, cela englobe une grande diversité

d'outils. Internet et ce qui en découle – applications pour *smartphones*, réseaux sociaux, messagerie, navigation web – en fait partie. Or dans ce domaine, une très nette domination des logiciels non suisses – surtout américains – a cours et la LPD ne s'applique que sur le territoire suisse. Le Conseil fédéral avait signalé cette limite de la LPD dans sa réponse à l'interpellation de Jean-Christophe Schwaab le 8 mai 2013 – avant l'affaire PRISM – sur les conséquences du FISAA[61] (voir note 16) :

> « La marge de manœuvre de la Suisse est limitée face à des violations du droit de la protection des données par des entreprises étrangères n'ayant pas de siège dans notre pays. En raison du principe de territorialité, des violations de la LPD ne peuvent être sanctionnées qu'en présence d'un rattachement suffisant avec la Suisse ».

C'est également l'avis du TF dans l'affaire *Google Street View* (ATF 138 II 346)[62]. Dans ce cas, il y avait bel et bien un « rattachement suffisant avec la Suisse », car Google collectait des données en Suisse pour son service *Street View*.

Le poids des géants américains d'Internet tels que Google, Apple, Facebook ou Amazon (les *GAFA* ou *Big Four*), entre autres, est considérable. Pesant à eux quatre quelques centaines de milliards de dollars en termes de chiffre d'affaire, ces géants du numérique dominent le monde et leurs secteurs d'activités se multiplient. Côté suisse ou même européen, on ne peut réguler leurs pratiques concernant le traitement des données personnelles. Ainsi, appliquer la *privacy by design* n'est possible que sur le territoire national. Concernant les géants américains, deux solutions sont possibles. Premièrement, il s'agirait de faire en sorte que la mise à disposition de certaines prestations respectent le droit suisse, donc intègrent une protection dès la

[61] « Comment protéger les données personnelles des citoyens suisses détenues par des entreprises américaines? » (13.3033 – Interpellation).

[62] Google avait fait recours au TF suite à la décision du TAF, qui avait été saisi par le PFPDT suite à des recommandations non suivies, qui lui demandait de respecter la LPD à propos de la collecte de données (photographies) et l'anonymisation partielle – donc insuffisante – de ces dernières. Dans son arrêt, le TF a admis qu'une anonymisation totale était impossible, mais a émis des conditions à Google. Ce fut une solution qui a pu satisfaire à la fois Google et le PFPDT (Manaï 2012).

conception ; cette solution est très exigeante et a pour risque majeur de se couper des prestations de ces entreprises si elles refusent ces conditions (imaginons par exemple que le moteur de recherche Google ne soit plus disponible sur le territoire suisse[63]). Cette solution hautement improbable doit se réaliser au moins à plus grande échelle – en coordination avec l'UE par exemple – pour avoir un plus grand impact et doit partir du principe que ces entreprises renonceraient à traiter plus qu'il n'en faut des données personnelles – c'est possible si la *privacy* devient un argument commercial pour les entreprises. Deuxièmement, il s'agirait de renforcer la sensibilisation et la responsabilité des personnes dans leur utilisation des services proposés par les géants d'Internet. Cette pratique déjà en cours, bien que non contraignante et à portée limitée, favorise par exemple l'utilisation d'outils suisses, qui eux, respectent *a priori* la loi suisse et, dans le cadre de la *privacy by design*, seront conçus en fonction des principes de la loi. Nous le voyons : intégrer la protection dès la conception a une limite nationale qu'il sera possible de pallier grâce à d'autres moyens d'intervention.

7.4.3 L'APPLICATION DE LA *PRIVACY BY DESIGN* AUX OUTILS DÉJÀ EXISTANTS

Une application des principes de *privacy by design* aurait un effet sur tous les nouveaux systèmes de traitement des données créés. Mais qu'en sera-t-il des outils déjà existants ? Une réflexion devra se poser sur l'adaptation de ces outils aux nouvelles normes, ce qui serait un travail non négligeable pour les responsables de traitement. Certains auteurs évoquent le concept de *privacy by redesign* (Mouchard 2013, p. 26) ; comme son nom l'indique, il s'agit de repenser les systèmes déjà existants en fonction du principe de protection dès la conception. Une réflexion devra être faite sur l'adaptation à des nouveaux principes, notamment sur le temps laissé aux organisations afin d'atteindre ce but,

[63] C'est le cas dans plusieurs pays, par exemple en Allemagne par rapport à *Google Street View*. Ce service a failli disparaître du territoire suisse (voir http://ntdroit.wordpress.com/2012/10/02/google-street-view-larret-du-tribunal-federal-qui-satisfait-toutes-les-parties-1c-230-2011/).

tout en prenant en compte les possibilités et moyens des responsables de traitement.

7.4.4 LES RESSOURCES DU PFPDT

Les deux solutions que nous avons imaginées exigent que le PFPDT ait de nouvelles compétences ou du moins approfondisse ses rôles de supervision. Dans le domaine privé, il a pour l'instant surtout un rôle de conseiller, mais il est indéniable qu'il sera amené à dépasser ce rôle dans le futur. Toutefois, en l'état, le PFPDT n'est pas en mesure de travailler plus. Ce constat a notamment été établi dans le rapport d'évaluation de la LPD (OFJ 2011, p. 200 – 204). Son budget, qui s'élève à 5,5 millions de francs pour l'année 2013, doit être négocié avec la Chancellerie fédérale, dont il dépend[64] ; il ne dispose pas de budget propre, ce qui affaiblit son autonomie. Selon Walter, il doit « être en mesure d'anticiper les problèmes et d'intervenir en amont, de répondre aux attentes des individus, de développer des solutions de protection des données concertées avec les différentes acteurs impliqués, de sensibiliser les utilisateurs actuels et futurs des technologies d'information et de contrôler plus systématiquement le respect des dispositions légales, les ressources et les effectifs du préposé fédéral à la protection des données devraient être sérieusement renforcés, sans quoi face à l'évolution actuelle de la société d'information et de surveillance, sa fonction pourrait devenir qu'un pur alibi »[65]. Une des raisons de ce manque de ressources pourrait également venir du statut d'autorité indépendante du PFPDT qui est un concept assez peu fréquent dans l'administration helvétique (Cottier 2011, p. 36).

Pour relativiser ce constat assez alarmant quant à l'avenir, notons que la situation n'est pas forcément meilleure dans les autres pays (*ibid*., p. 37) où les mêmes manquements sont pointés du doigt. Par exemple, en France, la CNIL fait face au même problème et accumule les dossiers en retard (Rochelandet 2010, p. 110). Elle avait par ailleurs évoqué l'idée d'une taxe à destination des entreprises pour améliorer son financement. En Suisse, la question de la gestion du budget du PFPDT devra être

[64] http://www.edoeb.admin.ch/datenschutz/00628/00665/00672/index.html?lang=fr
[65] *ibid*.

étudiée, afin de lui donner les moyens d'exercer ses futurs nouveaux rôles.

7.4.5 LA QUESTION DE LA NEUTRALITÉ TECHNOLOGIQUE

Intégrer la *privacy by design* pose la question de la future neutralité technologique de la loi. Nous l'avons dit, la neutralité qui caractérise la LPD actuellement est une raison de sa relative efficacité actuelle ; la loi a su épouser les fulgurantes innovations de ces dernières années. De ce fait n'apparaissent pas de dispositions sur les puces RFID, les données biométriques, le web, la vidéosurveillance, etc. Dans l'intérêt de garder l'efficacité de la loi, il paraît donc nécessaire de garder un tel principe. Ainsi, les dispositions ne seront pas vite dépassées ou contournées et la loi garderait une certaine clarté avec un nombre d'articles assez restreints.

Toutefois, si l'intégration générale de la *privacy by design* doit se faire en respectant ce principe ; selon Meier, quelques encarts à la règle pourraient avoir un effet positif (2007, p. 167). L'utilisation de termes trop généraux est vue ici comme une solution qui peut se révéler sans grande implication. Dans cette idée, les applications de la *privacy by design* que nous évoquions au point 7.3 (principe d'économicité des données, anonymisation des données, localisation, *privacy by default*) demanderaient une référence explicite dans la loi, sans quoi ils risquent de n'être que des vœux pieux. Dans l'intérêt d'améliorer au mieux la LPD, un subtil équilibre se situant quelque part entre une trop grande densité normative et des dispositions à faible portée devra être trouvé.

Une solution intermédiaire serait de mettre dans les dispositions d'une nouvelle législation une obligation pour les responsables de traitement de respecter les normes inscrites dans des directives que rédigerait le PFPDT. Cette idée est inspirée de ce que propose le projet de règlement européen où la Commission dispose de compétences en la matière. L'avantage d'une telle démarche est la combinaison du degré de précision des obligations légales et la facilité de les mettre à jour par le préposé, sans qu'il faille modifier toute la loi.

8 CONCLUSION

En conclusion, nous pouvons dire que la protection de la vie privée dès la conception représente en soi un grand bouleversement et se trouve être l'une des mesures phares de la protection des données, répondant à l'objectif du Conseil fédéral de rendre la LPD plus adéquate aux évolutions technologiques et sociétales actuelles. Au cours des dernières années, la notion s'est invitée dans les réflexions et les débats sur la protection des données. Nous avons pu voir avec ce travail que la mise en place de la *privacy by design* en Suisse s'opérationnalise principalement de deux manières différentes. Il existe deux solutions répondant à la question de recherche : l'autorégulation privée et la réglementation contraignante.

Premièrement, l'autorégulation se base sur le principe de responsabilité individuelle et part du principe qu'une régulation des responsables de traitement est trop restrictive et que, finalement, il incombe aux personnes intéressées de se responsabiliser quant à leurs comportements en utilisant par exemple des outils de protection déjà existants. L'introduction de la *privacy by design* résulterait d'initiative privée : les organisations décelant un avantage en terme d'image et de compétitivité à mettre en avant une meilleure protection des données adapteraient leurs nouveaux systèmes. Pour aider le citoyen à se retrouver, le PFPDT pourrait mettre en place des labels officiels, une pratique se trouvant être dans le prolongement des dispositions actuelles.

Deuxièmement, au vu des attitudes paradoxales des individus quant à leur vision et gestion des données personnelles, du manque de connaissance de la loi et surtout des évolutions technologiques qui parfois semblent sortir de l'imagination de célèbres auteurs de science-fiction, la solution contraignante veut obliger les responsables de traitement à respecter la protection des données dès la conception en mentionnant explicitement le principe dans la loi sous forme de nouvelle disposition. Comme nous l'avons vu, l'intégration du principe de *privacy by design* de façon contraignante ne compte que si un contrôle de son application est réalisé ; c'est pourquoi, la figure du délégué à la protection des données personnelles se démarque. Souvent évoqué en

relation avec la protection des données dès la conception, il ne manquera pas de marquer le paysage politique et économique européen et suisse. Il est encore tôt pour évaluer le réel impact des délégués dans les organisations, mais il sera très intéressant dans un futur proche de connaître leur réelle influence dans les affaires d'une entreprise (ou d'une institution étatique) et comment ils travaillent avec les organisations pour faire respecter les principes de protection des données.

A l'avenir, il sera intéressant d'étudier la solution la plus apte à répondre au problème public en se basant sur plusieurs critères tels que l'effectivité du droit, les attentes des citoyens et les intérêts des milieux de l'économie.

L'option choisie dépendra de l'importance accordée aux divers intérêts en jeu qui s'opposent. Au-delà de cette problématique vient se greffer la question des développements européens en la matière. Si beaucoup d'inconnues quant aux futurs projets de l'Union européenne et du Conseil de l'Europe, et à leur portée en Suisse, demeurent, leur influence n'en est pas moins marquante ; d'autant plus que l'UE est plus que déterminée à adopter une législation forte en matière de protection des données, une manière d'envoyer un signal – aux Etats-Unis notamment – montrant l'importance des libertés publiques. En suivant les futurs développements, il sera intéressant d'étudier sous l'angle de l'internationalisation des politiques publiques l'impact réel de la reprise du droit européen en Suisse par rapport à une série d'aspects tels que la marge de manœuvre de la Suisse, la question des préposés cantonaux, etc. Aussi, dans les années à venir, quoi que soit le chemin choisi, le PFPDT sera confronté à une série de nouveaux défis : il devra à la fois renforcer sa communication et la sensibilisation générale à la question de la protection des données et travailler à la mise en œuvre de très probables nouvelles dispositions.

Terminons par l'idée qu'au-delà du dilemme issu du choix d'une solution restrictive ou non, il s'agit peut-être de dépasser la pensée à la mode affirmant que toute forme de vie privée est vouée à disparaître ou au contraire que le droit doit agir en défenseur de tout traitement de données, vu comme une menace uniquement. Il s'agit de développer l'idée que « [l]es individus ne se préoccupent pas seulement (quand ils

s'en préoccupent) de défendre leur vie privée, il est tout aussi important pour eux de constituer, d'affirmer, d'exploiter leur identité publique dans un monde en réseau » (Kaplan 2010, p. 69). L'enjeu futur sera alors de permettre aux individus d'être autonomes, pleinement informés en matière de gestion de leurs données personnelles et être aptes à exercer un droit effectif à l'autodétermination informationnelle.

9 BIBLIOGRAPHIE

Sources juridiques

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28.I.1981, STE n°180

Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (Journal officiel de l'Union européenne L 350/60)

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (*Journal officiel n° L 281 du 23/11/1995 p. 0031 - 0050)*

Loi fédérale du 19 juin 1992 sur la protection des données (LPD), RS 235.1

Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD), RS 235.11

Ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD), RS 235.13

Ordonnance du 17 juin 1996 sur le système suisse d'accréditation et la désignation de laboratoires d'essais et d'organismes d'évaluation de la conformité, d'enregistrement et d'homologation (Ordonnance sur l'accréditation et la désignation, OAccD), RS 946.512

Proposition de Directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012) 10 final

Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces

données (règlement général sur la protection des données), COM(2012) 11 final

Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, Strasbourg, 8.XI.2001, STE n° 181

Documents officiels

Avis 9/2011 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID) adopté le 11 février 2011 (00327/11/FR WP 180, G29 2011)

Avis 01/2012 sur les propositions de réforme de la protection des données adopté le 23 mars 2012 (00530/12/FR WP 191, G29 2012)

Commentaire de l'Office fédéral de la justice à l'appui de l'ordonnance du 14 juin 1993 (état au 1er janvier 2008) relative à la loi fédérale sur la protection des données (OLPD, RS 235.11)

Commentaire l'Office fédéral de la justice concernant l'ordonnance du 28 septembre 2007sur les certifications en matière de protection des données (OCPD, RS 235.13)

CNIL. 2009. « La publicité ciblée en ligne ». Communication présentée en séance plénière le 5 février 2009

Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988 (MCF 1988, FF 1988 II 421)

Message relatif à une nouvelle Constitution fédérale (MCF 1996, FF 1997 I 155)

Message relatif à la révision de la loi fédérale sur la protection des données (LPD) et à l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données du 19 février 2003 (MCF 2003, FF 2003 I 1915)

Message relatif à l'arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'Union européenne sur la reprise de la décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale du 11 septembre 2009 (MCF 2009, FF 2009 6091)

OFJ. 2011. « Evaluation des Bundesgesetzes über den Datenschutz. Schlussbericht ». Office fédéral de la justice, Berne.

PFPDT. 2006. Explications sur les modifications du 17 décembre 2004 et du 24 mars 2006 de la loi fédérale sur la protection des données (LPD)

PFPDT. 2014. Commentaire explicatif sur les modifications du 19 mars 2014 des « Directives sur les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir» »

Rapport d'activités 2013/2014 du PFPDT

Rapport d'activités 2009/2010 du PFPDT

Rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données du 9 décembre 2011 (MCF 2011, FF 2012 255)

Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n°108)

Rapport explicatif du Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181)

Ouvrages généraux, doctrine, articles

AFCDP. 2004. « Contribution de l'AFCDP à la Consultation de la Commission Européenne «Une Approche Globale de la Protection des Données à caractère Personnel dans l'Union Européenne» »

AFCDP. 2009a. « Tableau comparatif des délégués à la protection des données à caractère personnel en Europe ». Tableau réalisé par Me Pascale Gelly (Cabinet Gelly), assistée d'E. Quillatre, à

l'occasion des 5èmes Assises du Correspondant Informatique & Libertés (Paris – 10 juin 2009).

AFCDP. 2009b. « Tableau comparatif des délégués à la protection des données à caractère personnel en Europe ». Tableau réalisé par Me Pascale Gelly (Cabinet Gelly), assistée d'E. Quillatre, à l'occasion des 5èmes Assises du Correspondant Informatique & Libertés (Paris – 10 juin 2009).

Belleil, Arnaud. 2009. « La régulation économique des données personnelles ? » in *Legicom*, vol. 1, n° 42, p. 143 – 151.

Bensoussan, Alain. 2014. « Privacy By Design ». Présentation PowerPoint de l'AFDIT. URL : http://www.afdit.fr/media/pdf/20%20mars%202014/Privacy%20by%20Design_Alain%20Bensoussan,%20Alain%20Bensoussan%20Avocats%2020%2003%202014.pdf.

Bondallaz, Stéphane. 2007. *La protection des personnes et de leurs données personnelles dans les télécommunications*. Thèse de doctorat sous la direction de Zufferey, Jean-Baptiste, Université de Fribourg.

Bondallaz, Stéphane. 2008. « Le « droit à une télécommunication protégée » ou la nécessité de reconsidérer la protection de la vie privée dans les environnements numériques » in *Jusletter*, 25 janvier 2008.

Brandimarte, Laura, Alessandro Acquisti et George Loewenstein. 2011. « Misplaced Confidences : Privacy and the Control Paradox » in : *Ninth Annual Workshop on the Economics of Information Security (WEIS)*. Harvard University, Cambridge.

Cavoukian, Ann. 2009. « SmartPrivacy for the Smart Grid : Embedding Privacy into the Design of Electricity Conservation ». Information Privacy Commissionner, Ontario, Canada.

Cavoukian, Ann. 2011a. « La protection intégrée de la vie privée. Les sept principes fondamentaux ». Commissaire à l'information et à la protection de la vie privée , Ontario, Canada .

Cavoukian, Ann. 2011b. « Privacy by Design in Law, Policy and Practice. A White Paper for Regulators, Decision-makers and Policy-makers ». Information Privacy Commissionner, Ontario, Canada.

Compañó, Ramón et Wainer Lusoli. 2009. « The Policy Maker's Anguish : regulating personal data behaviour between paradoxes and dilemmas ». Eighth Workshop on the Economics of Information Security (WEIS 2009), 24 – 25 juin 2009, Londres.

Cottier, Bertil. 1994. « La surveillance de droit public » in Gaillard, Nicolas (éd.). *La nouvelle loi fédérale sur la protection des données*, p. 207 – 226. Cedicac, Lausanne.

Cottier, Bertil. 2007. « La révision de la loi fédérale sur la protection des données: mieux vaut tard que jamais » in *Jusletter*, 17 décembre 2007.

Cottier, Bertil. 2011. « L'indépendance du Préposé fédéral à la protection des données à l'aune des modèles étrangers » in *plaidoyer*, p. 34 – 37.

Dewarte, Yves et Sébastien Gamps. 2010. « Protection de la vie privée : principes et technologies ». *Cahiers du CRID (Centre de Recherches Informatique et Droit)*, éditeur Daniel Le Métayer, Bruylant.

Guérin-Francois, Alexandra. 2012. « Encadrements juridiques et champs d'application de la Privacy by Design. D'où l'on vient.... Vers quoi se dirige-ton ? ». CNIL, Service des affaires juridiques.

Hoepman, Jaap-Henk. 2012. « Privacy Design Strategies ». *arXiv*.

Langheinrich. Marc. 2001. « Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems », ETH Zurich.

Mader, Luzius et Martin Hilti. 2012. « « Europarechtliche Vorgaben im Bereich Datenschutz : Implikationen für die Schweiz » in Epiney, Astrid et Tobias Fasnacht (éd.). 2012. Le développement du droit européen en matière de protection des données, p.69 – 86. Schulthess, Zürich, Bâle, Genève.

Mahon, Pascal. 2010. *Droit constitutionnel II. Droits fondamentaux.* Faculté de Droit de l'Université de Neuchâtel.

Manaï, Dominique. 2012. « La protection des données au miroir de la jurisprudence actuelle » in Epiney, Astrid et Tobias Fasnacht (éds.). *Le développement du droit européen en matière de protection des données et ses implications pour la Suisse*, p. 101 – 124. Schulthess, Zürich, Bâle, Genève.

Mayer-Schönberger, Viktor et Kenneth Cukier 2014. *Big data, la révolution des données est en marche*. Robert Laffont, Paris.

Meier, Philippe. 2007. « La nouvelle loi fédérale sur la protection des données : pragmatique ou lacunaire ? » in *medialex*, 4/2007, p. 165 – 167.

Meier, Philippe. 2010. *Protection des données. Fondements, principes généraux et droit privé*. Stämpfli, Berne.

Mouchard, Emilie. 2013. « La protection de la vie privée dès la conception ou l'intégration de la *Privacy by Design* comme mécanisme du régime général sur la protection des données en droit Européen » in *Lex Electronica*, vol. 18, n° 2.

Morin, Jean-Henry. 2012. « L'utilisation des moyens techniques en vue d'une amélioration de la protection des données » in Epiney, Astrid et Tobias Fasnacht (éds.). *Le développement du droit européen en matière de protection des données et ses implications pour la Suisse*, p. 1 – 13. Schulthess, Zürich, Bâle, Genève.

Kaplan, Daniel. 2010. *Informatique, libertés, identités*. FYP éditions, Limoges.

Kessous, Emmanuel. 2012. *L'attention au monde. Sociologie des données personnelles à l'ère numérique*. Armand Colin, Paris.

Krebs, David. 2013. « "Privacy by Design": Nice-to-have or a Necessary Principle of Data Protection Law ? » in *JIPITEC* 2, para. 1.

Oetzel, Marie Caroline et Sarah Spiekerman. 2012. « Privacy-by-design through systematic privacy impact assessment – a design science approach ». Publié lors du 20ème *European Conference on Information Systems* (ECIS 2012), Barcelone, juin 2012 .

OFJ. 2008. *Guide de législation « module loi »*. Office fédéral de la justice, Berne.

Rochelandet, Fabrice. 2010. *Economie des données personnelles et de la vie privée*. La Découverte, Paris.

Rochelandet, Fabrice et Alain Rallet. 2011. « La régulation des données personnelles face au web relationnel : une voie sans issue ? » in *Réseaux*, vol. 3, n° 167, p. 17 – 47.

Pedrazzini, Mario M. 1994. « Les grandes options du législateur » in Gaillard, Nicolas (éd.). *La nouvelle loi fédérale sur la protection des données*, p. 17 – 39. Cedicac, Lausanne.

Poullet, Yves. 2005. « Pour une troisième génération de réglementations de protection des données » in *Jusletter*, 3 octobre 2005.

Poullet, Yves. 2009. « La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ? » in *Legicom*, vol. 1, n°42, p. 47 – 69.

Sackmann, Stefan, Jens Strüker et Rafael Accorsi. 2006. « Personalization in Privacy-Aware Highly Dynamic Systems ». Institute of Computer Science and Social Studies, Department of Telematics, University of Freiburg, Germany .

Simon, Herbert A. 1971. « Designing Organizations for an Information-Rich World », in Martin Greenberger. *Computers, Communication, and the Public Interest*, The Johns Hopkins Press, Baltimore.

de Terwangne, Cécile. 2012. « La modernisation de la Convention 108 du Conseil de l'Europe » in Epiney, Astrid et Tobias Fasnacht (éds.). *Le développement du droit européen en matière de protection des données et ses implications pour la Suisse*, p. 23 – 67. Schulthess, Zürich, Bâle, Genève.

Thür, Hanspeter. 2012. « Zum Reformsbedarf des Datenschutzgesetzes aus Sicht des Eidgenössischen Datenschutzbeauftragten » in Epiney, Astrid et Tobias Fasnacht (éds.). *Le développement du droit européen en matière de protection des données et ses implications pour la Suisse*, p. 87 – 99. Schulthess, Zürich, Bâle, Genève.

Vila, Tony, Rachel Greenstadt et David Molnar. 2003. « Why we cannot be bothered to read privacy policies : models of privacy economics as lemon markets », *Proceedings of the 5th International Conference of Electronic Commerce*, Harvard University.

Walter, Jean-Philippe. 1988. *La protection de la personnalité lors du traitement de données à des fins statistiques*. Editions universitaires, Fribourg.

Walter, Jean-Philippe. 1994. « Le droit public matériel » in Gaillard, Nicolas (éd.). *La nouvelle loi fédérale sur la protection des données*, p. 41 – 83. Cedicac, Lausanne.

Walter, Jean-Philippe. 2009. « Communication de données personnelles à l'étranger » in Epiney, Astrid et Patrick Hobi (éds.). *La révision de la Loi sur la protection des données*. Schulthess, Zurich, Bâle, Genève.

Walter, Jean-Philippe. 2012a. « Vingt ans de législation sur la protection des données, rétrospectives et perspectives », in *Jusletter*, 25 juin 2012.

Walter, Jean-Philippe. 2012b. « La loi fédérale sur la protection des données, versus secteur privé ». Présentation PowerPoint. URL : www.ge.ch/ppdt/doc/Presentation-WALTER.pptx.

Walter, Jean-Philippe. 2012c. « L'évolution du droit de la protection des données : perspectives ». Conférence publique « Vingt ans de législation sur la protection des données », 27 avril 2012, Bellinzone.

Articles de journaux (en ligne)

ATS. 2012. « « La protection des données empêche le travail de la police » / 240 policières / et policiers tiennent congrès à Lugano ». *ATS*, 21 juin 2012. URL : http://www.presseportal.ch/fr/pm/100019942/100720584/-la-protection-des-donn-es-emp-che-le-travail-de-la-police-240-polici-res-et-policiers-tiennent

Kallenborn, Gilbert. 2013. « Comment les Etats-Unis légitiment la cybersurveillance mondiale ». *01Net*, 21 janvier 2013. URL : http://www.01net.com/editorial/584637/comment-les-etats-unis-legitiment-la-cybersurveillance-mondiale/

Mattatia, Fabrice. 2013. « Les amendements au projet de règlement européen sur les données personnelles ». *01Business*, 6 décembre 2013. URL : http://pro.01net.com/editorial/609798/les-amendements-au-projet-de-reglement-europeen-sur-les-donnees-personnelles/

Säemann, Stefan. 2014. « La nécessité d'une meilleure protection des données en Suisse ». *La Voix des Consommateurs*, 10 mars 2014.

URL : http://fr.comparis.ch/comparis/konsumentenstimme/2014-1/datenvertrauens-index.aspx

Sites web

www.admin.ch

www.afapdp.org

www.apps.edoeb.admin.ch

www.bj.admin.ch

www.cnil.fr

www.comparis.ch

www.curia.europa.eu

www.developpement-durable.gouv.fr

www.edoeb.admin.ch

www.europa.eu

www.europarl.europa.eu

www.hebdo.ch

www.ico.org.uk

www.informatique-et-libertes-formation.fr

www.iso.org

www.journaldunet.com

www.ntdroit.wordpress.com

www.oecd.org

www.parlament.ch

www.privacybydesign.ca

www.rts.ch

www.saisa.eu

www.sebastienfanti.ch

In der gleichen Reihe
Dans la même collection

N°	Autoren, Titel und Datum – Auteurs, titres et date
275	**SOGUEL Nils, MUNIER Evelyn** Vergleich 2011 der Kantons- und Gemeindefinanzen Comparatif 2011 des finances cantonales et communales
276	**HUGUENIN Jean-Marc** Data Envelopment Analysis (DEA)
277	**PINSON Joël** Analyse des réseaux sociaux appliquée à l'organisation d'événements sportifs
278	**HUGUENIN Jean-Marc** Data Envelopment Analysis (DEA)
279	**DUPUIS Johann, KNOEPFEL Peter** Institutional regimes, policy networks and their effects on the management of contaminated sites. The case of Bonfol industrial landfill in Switzerland
280	**STADELHOFER Julie-Antoinette** Die Organisation von Rechtsdiensten in der Bundesverwaltung
281	**BONOLI Giuliano, CHAMPION Cyrielle** La réinsertion professionnelle des bénéficiaires de l'aide sociale en Suisse et en Allemagne
282	**EGGLI Sophie** L'exercice des droits politiques des membres de la Cinquième Suisse: quelles différences avec les Suisses de l'intérieur?
283	**SOGUEL Nils, MUNIER Evelyn** Vergleich 2012 der Kantons- und Gemeindefinanzen Comparatif 2012 des finances cantonales et communales
284	**ROUD Guillaume** État des lieux et potentiel de l'agriculture urbaine en Suisse
285	**SOGUEL Nils, MUNIER Evelyn** Vergleich 2013 der Kantons- und Gemeindefinanzen Comparatif 2013 des finances cantonales et communales
286	**SCHMID Silvio** Regulierungen an der Schnittstelle zwischen den Ressourcen Wald und Klima. Einflussfaktoren auf die Inwertsetzung der CO2-Senkenleistung des Waldes
287	**PRIGIONI Mina-Claire** Le management de juridiction: Analyse comparative de l'organisation et du fonctionnement managérial de cinq juridictions du pouvoir judiciaire à Genève
288	**DAYER Alexande** L'hôpital public sous l'ère de la nouvelle gouvernance. Une «camisole de force» pour le personnel soignant?.

L'IDHEAP en un coup d'œil

Champ

Intégré au 1er janvier 2014 dans la Faculté de droit, des sciences criminelles et d'administration publique, l'IDHEAP poursuit dans un environnement académique élargi et fertile ses missions d'enseignement dans les programmes de base, de formation continue, de recherche et d'expertise qui lui ont permis d'atteindre un rayonnement national et international.

Ainsi recomposée, la Faculté de droit, des sciences criminelles et d'administration publique développe un profil totalement inédit en Suisse, propice aux échanges interdisciplinaires, dans la ligne adoptée de longue date par l'UNIL.

L'IDHEAP se concentre sur l'étude de l'administration publique, un champ interdisciplinaire visant à développer les connaissances scientifiques sur la conduite des affaires publiques et la direction des institutions qui en sont responsables. Ces connaissances s'appuient sur plusieurs disciplines des sciences humaines et sociales, adaptées aux spécificités du secteur public et parapublic. L'IDHEAP est le seul institut universitaire suisse totalement dédié à cet important champ de la connaissance.

Vision

À l'interface entre théorie et pratique de l'administration publique, l'IDHEAP est le pôle national d'excellence contribuant à l'analyse des mutations du secteur public et à une meilleure gouvernance de l'Etat de droit à tous ses niveaux, en pleine coopération avec ses partenaires universitaires suisses et étrangers.

Mission

Au service des étudiants, du secteur public et de la société dans son ensemble, l'IDHEAP a une triple mission qui résulte de sa vision :

- **Enseignement universitaire** au niveau master et post-master, ainsi que formation continue de qualité des élus et cadres publics ;
- **Recherche fondamentale et appliquée** en administration publique reconnue au niveau national et international, et valorisée dans le secteur public suisse ;
- **Expertise et conseil indépendants** appréciés par les organismes publics mandataires et enrichissant l'enseignement et la recherche.

Principales prestations

1. Enseignement : former les élus et cadres actuels et futurs du secteur public

- Doctorat en administration publique
- MPA (Master of Advanced Studies in Public Administration-MPA)
- Master PMP (Master of Arts in Public Management and Policy)
- CEMAP (Certificat exécutif en management et action publique)
- CAS en administration publique avec spécialisation dans une douzaine de domaines (Certificate of Advanced Studies in Public Administration)
- SSC (Séminaire pour spécialistes et cadres)

2. Recherche : ouvrir de nouveaux horizons pour l'administration publique

- Projets de recherche fondamentale ou appliquée
- Direction de thèse de doctorat en administration publique
- Publications scientifiques (ouvrages et articles)
- Colloques et conférences scientifiques
- Cahiers et Working Papers de l'IDHEAP

3. Expertise et conseil : imaginer de mettre en œuvre des solutions innovatrices

- Mandats d'expertise et de conseil auprès du secteur public et parapublic

4. Services à la cité : contribuer à la connaissance du service public

- Bibliothèque spécialisée en administration publique
- Sites badac.ch, gov.ch, ivote.ch
- Manuel de l'administration publique
- Renseignement aux collectivités publiques
- Interventions médiatiques
- Articles et conférences de vulgarisation

La loi fédérale sur la protection des données (LPD) en vigueur en Suisse depuis 1993 ne sera bientôt plus adaptée à notre société, en raison des évolutions technologiques rapides que cette dernière connaît. Parmi les améliorations de la loi proposées, la mise en place d'une protection de la vie privée dès la conception (privacy by design) des outils traitant les données est évoquée. Cette idée propose un changement de paradigme quant à l'exploitation des données ; elle est également présente dans les débats européens. Ce travail fait une revue générale de la LPD et propose d'examiner les modalités d'intégration de la privacy by design en son sein et les implications que cela suppose.

The Federal Act on Data Protection (FADP) in force in Switzerland since 1993 will soon be unfitted for our society which knows major technological changes. Among the proposed improvements for the law, the implementation of the "privacy by design" concept is discussed. This idea offers a paradigm shift towards the use of data ; it is also debated in the European context. This work proposes a general review of the FADP and analyses integration modalities of the "privacy by design" in it and its implications.