



Collection lausannoise  
CEDIDAC

Sylvain Métille  
(éditeur)

# L'informatique en nuage

*Unil*



Stämpfli Editions





Collection lausannoise  
CEDIDAC

Sylvain Métille  
(éditeur)

**L'informatique en nuage**



Collection lausannoise  
**CEDIDAC**

**Volume 90**

Comité éditorial

Hansjörg Peter; Damiano Canapa, Robert J. Danon,  
Anne-Christine Favre, Andrew M. Garbarski, Eva Lein

Volumes 1 à 72 publiés dans la collection Recherches juridiques  
lausannoises

Sous-collection CEDIDAC (volume 118) dirigée par Damiano Canapa,  
fondée par François Dessemontet sous le titre Publication CEDIDAC et  
continué par Jean-Marc Rapp et Edgar Philippin

Le CEDIDAC bénéficie du soutien de la Fondation pour le Centre du  
droit de l'entreprise de l'Université de Lausanne (CEDIDAC)



Stämpfli Editions



Collection lausannoise  
CEDIDAC

# L'informatique en nuage

Édité par

**Sylvain Métille**

Professeur à l'Université de Lausanne, avocat



Stämpfli Editions

© Stämpfli Editions SA Berne

---

Information bibliographique de la Deutsche Nationalbibliothek

La Deutsche Nationalbibliothek a répertorié cette publication dans la Deutsche Nationalbibliografie; les données bibliographiques détaillées peuvent être consultées sur Internet à l'adresse <http://dnb.d-nb.de>.

Tous droits réservés, en particulier le droit de reproduction, de diffusion et de traduction. Sans autorisation écrite de l'éditeur, l'œuvre ou des parties de celle-ci ne peuvent pas être reproduites, sous quelque forme que ce soit (photocopies, par exemple), ni être stockées, transformées, reproduites ou diffusées électroniquement, excepté dans les cas prévus par la loi.

© Stämpfli Editions SA Berne · 2022  
[www.staempfliverlag.com](http://www.staempfliverlag.com)

Print ISBN 978-3-7272-4456-8

Dans notre librairie en ligne [www.staempflishop.com](http://www.staempflishop.com),  
la version suivante est également disponible :

E-Book ISBN 978-3-7272-4437-7

printed in  
switzerland



© Stämpfli Editions SA Berne

---

## Avant-propos

L'informatique en nuage (*cloud* ou *cloud computing*) est aujourd'hui omniprésente. Cet accès à distance et sur demande à des ressources informatiques (hébergement, machines virtuelles, services, *etc.*) fournies par un tiers et généralement mises en commun pour de nombreux utilisateurs soulève de nombreuses questions. Comme le relève Alexandre JOTTERAND, la qualification juridique d'un contrat d'informatique en nuage n'est pas évidente. Elle est pourtant essentielle, car elle détermine les règles applicables, y compris à la sortie du contrat, une étape très souvent négligée au moment de la négociation du contrat.

L'informatique en nuage est un cas classique d'externalisation ou de délégation de traitement, un cas bien connu en droit de la protection des données. Les questions que cela soulève sont pourtant encore nombreuses, en particulier lorsqu'interviennent des sous-traitants étrangers (ou une communication de données à l'étranger) ou des données protégées par des secrets. Philipp FISCHER et Sébastien PITTET s'y intéressent sous l'angle des responsables du traitement privés, alors que Daniel DZAMKO aborde la question pour les administrations fédérale, cantonales et communales.

Si le droit pose des conditions assez complexes, il est intéressant de regarder les réponses concrètes. Nicolas SAVOY, Mélanie GARCIA, Ludivine EPINEY et Catherine PUGIN s'intéressent à la situation au sein de l'administration vaudoise. Ils présentent non seulement les limites juridiques applicables, mais aussi la manière concrète d'y répondre. Quant à Aurélien ROCHER, il analyse une initiative privée des fournisseurs, le Code de conduite CISPE des Fournisseurs d'Infrastructures Cloud relatif à la Protection des Données.

Pour conclure, Frédéric ÉRARD traite de plusieurs questions en lien avec le dossier électronique du patient, alors que Susanne VERGNOLLE s'interroge sur le rôle de la territorialité pour des prestations par nature dématérialisées.

L'informatique en nuage est un sujet qui ne se résout ni en un colloque, ni en un ouvrage. Néanmoins, et modestement, il doit contribuer à clarifier l'utilisation conforme de l'informatique en nuage et réconcilier, autant que possible, les exigences légales, les possibilités techniques, et les besoins des utilisateurs.

Je profite également de remercier chaleureusement les auteurs sans qui cet ouvrage n'existerait pas, ainsi que Enzo BASTIAN, assistant doctorant au CEDIDAC et Margot SUTTER, assistante étudiante au CEDIDAC pour leur relecture attentive et la mise en forme du présent ouvrage.

Sylvain Métille





---

# Sommaire

<b>Avant-propos</b> .....	V
<b>Table des principales abréviations</b> .....	XI
<b>Contrats <i>cloud</i> : qualification, gestion des données et sortie de la relation</b> .....	1
<i>ALEXANDRE JOTTERAND</i>	
<b>L'utilisation de services <i>cloud</i> par des responsables du traitement privés</b> .....	35
<i>PHILIPP FISCHER</i> <i>SÉBASTIEN PITTET</i>	
<b>Überlegungen zu Recht und Risiko bei behördlicher Cloudnutzung</b> .....	83
<i>DANIEL DZAMKO-LOCHER</i>	
<b>L'informatique en nuage à l'État de Vaud – État des lieux, enjeux et solutions</b> .....	119
<i>NICOLAS SAVOY</i> <i>MÉLANIE GARCIA</i> <i>LUDIVINE ÉPINEY</i> <i>CATHERINE PUGIN</i>	
<b>Le Code de conduite CISPE des fournisseurs d'infrastructures Cloud relatif à la protection des données</b> .....	201
<i>AURÉLIEN ROCHER</i>	
<b>Le dossier électronique du patient : révolution ou désillusion ?</b> .....	219
<i>FRÉDÉRIC ERARD</i>	
<b>Cloud et territoire</b> .....	243
<i>SUZANNE VERGNOLLE</i>	



---

## Table des principales abréviations

a.a.O	<i>am angegebenen Ort</i>
Abs.	<i>Absatz</i>
ACV	Administration cantonale vaudoise
<i>ad art./par.</i>	À l'article/au paragraphe
Aff.	Affaire
AIMP	Accord intercantonal des 25 novembre 1994/15 mars 2001 sur les marchés publics, RO 2003 196
AIPD	Analyse d'impact relative à la protection des données
AISBL	Association internationale sans but lucratif
AJP	<i>Aktuelle Juristische Praxis</i>
al.	Alinéa
AMP	Accord international révisé du 15 avril 1994 sur les marchés publics, RS 0.632.231.422
APDI	Autorité de protection des données et de droit à l'information du Canton de Vaud
API	<i>Application Programming Interface</i>
Art.	<i>Artikel</i>
art.	Article
ASB	Association suisse des banquiers
ASP	<i>Application Service Provider</i>
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
AWS	<i>Amazon Web Services</i>
B2C	<i>Business to Consumer</i>
BB1	<i>Bundesblatt</i>
BCR	<i>Binding Corporate Rules</i>
BGE	<i>Bundesgerichtsentscheid</i>
BGer	<i>Schweizerisches Bundesgericht</i>
BGÖ	<i>Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung, SR 152.3</i>
BJ	<i>Bundesamt für Justiz</i>
BLV	Base législative vaudoise
BO CE	Bulletin officiel du Conseil des États
BO CN	Bulletin officiel du Conseil national

BPDV	<i>Verordnung vom 22. November 2017 über den Schutz von Personendaten des Bundespersonals, SR 172.220.111.4</i>
BPG	<i>Bundespersonalgesetz vom 24. März 2000, SR 172.220.1</i>
BPV	<i>Bundespersonalverordnung vom 3. Juli 2001, SR 172.220.111.3</i>
BSK	<i>Basler Kommentar</i>
Bspw.	<i>Beispielsweise</i>
Bstb.	<i>Buchstabe</i>
BV	<i>Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101</i>
BWIS	<i>Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit, SR 120</i>
BYOE	<i>Bring Your Own Encryption</i>
BYOK	<i>Bring Your Own Key</i>
bzw.	<i>beziehungsweise</i>
c.	<i>contre</i>
CARA	Association intercantonale regroupant les cantons de Genève, du Valais, de Vaud, de Fribourg et du Jura
CCM	<i>Cloud Controls Matrix</i>
CCTF	<i>Task force du Code de conduite</i>
CdC	Centrale de compensation
CDS	Conférence des directrices et directeurs cantonaux de la santé
CE	Commission européenne
CEDN	Comité d'experts délégués au numérique
CEO	<i>Chief Executive Officer</i>
CEPD	Comité européen de la protection des données
cf.	<i>confer</i>
CH	Suisse
ch.	Chiffre(s)
CHUV	Centre Hospitalier Universitaire Vaudois
CID	<i>Client-identifying data</i>
Cir.	<i>Circular</i>
CISP(s)	<i>Cloud Infrastructure Service Provider(s)</i>
CISPE	<i>Cloud Infrastructure Service Providers Europe</i>
CJUE	Cour de justice de l'Union Européenne
CLDN	Conférence latine des directeurs du numérique
<i>Cloud</i>	Informatique en nuage

<i>CLOUD</i>	<i>Clarifying Lawful Overseas Use of Data</i>
<i>CLOUD Act</i>	<i>Clarifying Lawful Overseas Use of Data Act</i>
CN	Conseil national
CNIL	Commission nationale de l'informatique et des libertés (France)
CO	Loi fédérale du 30 mars 1911 complétant le Code civil suisse (Livre cinquième : Droit des obligations), RS 220
coll.	Collection
cons./c.	Considérant(s)
Corp.	<i>Corporation</i>
CP	Code pénal suisse du 21 décembre 1937, RS 311.0
CSA	<i>Cloud Security Alliance</i>
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101
Cst.-VD	Constitution du Canton de Vaud du 14 avril 2003, BLV 131.231
CSV	<i>Comma-separated values</i>
CyrV	<i>Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung, SR 120.73</i>
d.h.	<i>das heißt</i>
<i>DaaS</i>	<i>Desktop as a Service</i>
<i>DBaaS</i>	<i>Database as a Service</i>
DBG	<i>Bundesgesetz vom 14. Dezember 1990 über die direkte Bundessteuer, SR 642.11</i>
DEP	Dossier électronique du patient
DFJC	Département de la formation, de la jeunesse et de la culture
DGNSI	Direction générale du numérique et des systèmes d'information
DIRH	Département des infrastructures et des ressources humaines
DOJ	<i>Department of Justice</i> (États-Unis d'Amérique)
DRP	<i>Disaster Recovery Plan</i>
DSFA	<i>Datenschutz-Folgenabschätzung</i>
DSG	<i>Bundesgesetz vom 19. Juni 1992 über den Datenschutz, SR 235.1</i>
DSGVO	<i>Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), JO L 119 vom 4. Mai 2016, p. 1 ss</i>
E.	<i>Erwägungsgrund</i>
<i>e.g.</i>	<i>Exempli gratia</i>

E-ID	Moyen d'identification électronique
éd.	Édition
éd/éds/édit.	Éditeur(s)
EDPB	<i>European Data Protection Board</i>
EDPL	<i>European Data Protection Law Review</i>
EDPS	<i>European Data Protection Supervisor</i>
EDÖB	<i>Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter</i>
EEE	Espace Économique Européen
EF	Expert Focus
ég.	Également
EHDS	<i>European Health Data Space</i>
Eidg.	<i>Eidgenössisch</i>
EMRK	<i>Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten, SR 0.101</i>
EMS	Établissements médico-sociaux
ENISA	<i>European Network and Information Security Agency</i>
EPD	<i>Elektronisches Patientendossier</i>
EPDV	<i>Verordnung vom 22. März 2017 über das elektronische Patientendossier, SR 816.11</i>
ESTV	<i>Eidgenössische Steuerverwaltung</i>
et al.	<i>Alius</i>
<i>etc.</i>	<i>et cætera</i>
EU	<i>European Union</i>
EuGH	<i>Gerichtshof der Europäischen Union</i>
EuZ	<i>Zeitschrift für Europarecht</i>
EWS	<i>Europäisches Wirtschafts- und Steuerrecht</i>
ex.	Exemple
f.	<i>Folgende Seite</i>
FAQ	Foire aux questions
fév.	Février
FF	Feuille fédérale
ff.	<i>Folgende Seiten</i>
FHE	<i>Fully Homomorphic Encryption</i>
FINMA	Autorité fédérale de surveillance des marchés financiers
FMH	<i>Foederatio Medicorum Helveticorum</i>
Fn.	<i>Fussnoten</i>

GDPR	<i>Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 199, 4 May 2016, p. 1 ff.</i>
GE	Canton de Genève
GEVER-Verordnung	<i>Verordnung vom 3. April 2019 über die elektronische Geschäftsverwaltung in der Bundesverwaltung, SR 172.010.441</i>
ggf.	<i>Gegebenenfalls</i>
grds.	<i>Grundsätzlich</i>
Hinw.	<i>Hinweis</i>
HK	<i>HandKommentar</i>
Hrsg.	<i>Herausgeber</i>
HYOK	<i>Hold Your Own Key</i>
<i>i.e.</i>	<i>id est, c'est-à-dire</i>
<i>i.e.S.</i>	<i>Im engeren Sinne</i>
<i>i.K.</i>	<i>Inkrafttreten</i>
<i>i.S.</i>	<i>Im Sinne</i>
<i>i.S.v.</i>	<i>Im Sinne von</i>
<i>i.V.m.</i>	<i>In Verbindung mit</i>
<i>IaaS</i>	<i>Infrastructure as a Service</i>
IAPP	<i>International Association of Privacy Professionals</i>
<i>Ibid.</i>	<i>Ibidem, même endroit</i>
IBM	<i>International Business Machines Corporation</i>
ID	<i>Identification</i>
IDG	<i>Informations- und Datenschutzgesetz des Kanton Zürich</i>
IKS	<i>Internes Kontrollsystem</i>
IKT	<i>Informations- und Kommunikationstechnik</i>
<i>in</i>	<i>dans</i>
<i>in fine (i.f.)</i>	<i>à la fin</i>
<i>infra</i>	<i>plus bas</i>
<i>inkl.</i>	<i>inklusive</i>
<i>insbes.</i>	<i>Insbesondere</i>
IP	<i>Internet Protocol</i>
ISB	<i>Informatiksteuerungsorgan des Bundes</i>

ISchV	<i>Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes, SR 510.411</i>
ISG	<i>Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund, BBl 2017 3077</i>
ISO	<i>International Organization for Standardization</i>
ITSL	<i>Center for Information Technology, Society, and Law</i>
JCP	Juris-Classeur Périodique
JdT	Journal des tribunaux
JO L	Journal officiel de l'Union européenne
JSON	<i>JavaScript Object Notation</i>
JU	Canton du Jura
KPI	<i>Key Performance Indikator</i>
LAMal	Loi fédérale du 18 mars 1994 sur l'assurance-maladie, RS 832.10
LB	Loi fédérale du 8 novembre 1934 sur les banques et les caisses d'épargne, RS 952.0
LCart	Loi fédérale du 6 octobre 1995 sur les cartels et autres restrictions à la concurrence, RS 251
LDA	Loi fédérale du 9 octobre 1992 sur le droit d'auteur et les droits voisins, RS 231.1
LDEP	Loi fédérale du 19 juin 2015 sur le dossier électronique du patient, RS 816.1
let.	Lettre
LIHD	Loi fédérale du 14 décembre 1990 sur l'harmonisation des impôts directs des cantons et des communes, RS 642.14
LI	Loi cantonale vaudoise du 4 juillet 2000 sur les impôts cantonaux, BLV 642.11
LIFD	Loi fédérale du 14 décembre 1990 sur l'impôt fédéral direct, RS 642.11
LInfo	Loi cantonale vaudoise du 24 septembre 2002 sur l'information, BLV 170.21
LMP-VD	Loi cantonale vaudoise du 24 juin 1996 sur les marchés publics, BLV 726.01
LNCS	<i>Lecture Notes in Computer Science</i>
LNE	Laboratoire national de métrologie et d'essai (France)
LPD	Loi fédérale du 19 juin 1992 sur la protection des données, RS 235.1
LPGA	Loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales, RS 830.1



LPrD	Loi cantonale vaudoise du 11 septembre 2007 sur la protection des données, BLV 172.65
LRH	Loi fédérale du 30 septembre 2011 relative à la recherche sur l'être humain, RS 810.30
LSI	Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération, RS 128
LSR	<i>Life Science Recht</i>
m.E.	<i>meines Erachtens</i>
MLAT	<i>Mutual Legal Assistance Treaties</i>
N	Numéro(s) marginaux
N°/n°/n./No/no/Nr.	Numéro
NB	<i>Nota bene</i>
nDSG	<i>Bundesgesetz vom 25. September 2020 über den Datenschutz, Inkrafttreten am 1. September 2023, BBl 2020 7639</i>
NIST	<i>National Institute of Standards and Technology</i>
nLPD	Loi fédérale du 25 septembre 2020 sur la protection des données, entrée en vigueur le 1 <sup>er</sup> septembre 2023, FF 2020 7397
NOYB	<i>None Of Your Business</i>
oct.	Octobre
ODEP	Ordonnance du Conseil fédéral du 22 mars 2017 sur le dossier électronique du patient, RS 816.11
ODEP-DFI	Ordonnance du Conseil fédéral du 22 mars 2017 du DFI sur le dossier électronique du patient, RS 816.111
OFJ	Office fédéral de la justice
OLPD	Ordonnance du Conseil fédéral du 14 juin 1993 relative à la loi fédérale sur la protection des données, RS 235.11
OPDo	Ordonnance du Conseil fédéral du 31 août 2022 sur la protection des données
OMC	Organisation mondiale du commerce
Ord.	Ordonnance
p.	Page(s)
p. ex.	Par exemple
<i>PaaS</i>	<i>Platform as a Service</i>
par.	Paragraphe(s)
PCA	Plan de continuité des activités
PDF	<i>Portable Document Format</i>
FPFDT	Préposé fédéral à la protection des données et à la transparence
PII	<i>Personal Identifiable Information</i>

PIIEC	Projet important d'intérêt européen commun
PJA	Pratique juridique actuelle
PK	<i>Praxiskommentar</i>
PME	Petites et moyennes entreprises
pp.	Pages
privatim	Conférence des préposé(e)s suisses à la protection des données
PSI	Plan de secours informatique
Pub. L. No.	<i>Public Law number</i>
RCDIP	Revue critique de droit international privé
RDS	Revue de droit suisse
REAS	Centre du droit de la responsabilité civile, des assurances privées et sociales
RGPD	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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 et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4 mai 2016, p. 1 ss
RIC	Règlement cantonal vaudois du 21 janvier 200 relatif à l'informatique cantonale, BLV 172.62.1
RLMP-VD	Règlement cantonal vaudois du 7 juillet 2004 d'application de la loi cantonale vaudoise du 24 juin 1996 sur les marchés publics, BLV 726.01.01
RLPers-VD	Règlement cantonal vaudois du 9 décembre 2002 d'application de la loi du 12 novembre 2001 sur le personnel de l'État de Vaud, BLV 172.31.1
RMA	Revue de la protection des mineurs et des adultes
RO	Recueil officiel du droit fédéral
RRB	<i>Regierungsratsbeschluss</i>
RS	Recueil systématique du droit fédéral
RSDA	Revue suisse de droit des affaires et du marché financier
RSJ	Revue suisse de Jurisprudence
RTD Eur.	Revue trimestrielle de droit européen
RVOG	<i>Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997, SR 172.010</i>
RVOV	<i>Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998, SR 172.010.1</i>
Rz.	<i>Randziffer</i>
S.	<i>Seite</i>

S./Sect.	Section(s)
s.	Suivant(e)
<i>SaaS</i>	<i>Software as a Service</i>
SCA	<i>Stored Communications Act</i>
SCC	<i>Standard Contractual Clauses</i>
SECO	Secrétariat d'État à l'économie
Seq.	<i>Sequentia</i>
SFR	Société Française du Radiotéléphone
SI	Système d'information
SICAV	Société d'investissement à capital variable
SIK	<i>Schweizerische Informatikkonferenz</i>
SJ	Semaine Judiciaire
SLA	<i>Service Level Agreement</i>
Sog.	<i>sogenannte</i>
Spéc.	Spécialement
SR	<i>Systematische Rechtsammlung</i>
ss	Suivante(e)s
<i>STaaS</i>	<i>Storage as a Service</i>
Stat.	<i>Statutes</i>
StGB	<i>Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0</i>
StHG	<i>Bundesgesetz vom 14. Dezember 1990 über die Harmonisierung der direkten Steuern der Kantone und Gemeinden, SR 642.14</i>
<i>supra</i>	au-dessus
SUVA	Caisse nationale suisse d'assurance en cas d'accidents
SWIPO	<i>Switching Cloud Providers and Porting Data</i>
SZW	<i>Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht</i>
TAF	Tribunal administratif fédéral
TC	Tribunal cantonal
TEE	<i>Trusted Execution Environment</i>
TF	Tribunal fédéral
TIC	Technologies de l'information et de la communication
Trad.	Traduit
TREX	<i>Der Treuhandexperte</i>
u.a.	<i>unter anderem</i>

U.S.	<i>United States of America</i>
U.S.C.	<i>United States Code</i>
u.U.	<i>unter Umständen</i>
UE	<i>Union européenne</i>
UPIC	<i>Unité de pilotage informatique de la Confédération</i>
URL	<i>Uniform Resource Locator</i>
v/v./vs	<i>versus</i>
V.	<i>Voir</i>
v.	<i>version</i>
VD	<i>Canton de Vaud</i>
VDSG	<i>Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz, SR 235.11</i>
VDTI	<i>Verordnung vom 25. November 2020 über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung, SR 172.010.58</i>
Vgl.	<i>Vergleiche</i>
vol.	<i>Volume</i>
VPN	<i>Virtual Private Network</i>
XaaS	<i>Everything as a Service</i>
XML	<i>Extensible Markup Language</i>
z.B.	<i>zum Beispiel</i>
ZD-Aktuell	<i>Zeitschrift für Datenschutz</i>
Ziff.	<i>Ziffer</i>
Zit.	<i>Zitiert</i>
ZSR	<i>Zeitschrift für Schweizerisches Recht</i>

---

# Contrats *cloud* : qualification, gestion des données et sortie de la relation

ALEXANDRE JOTTERAND  
Avocat, étude id est avocats Sàrl  
CIPP/E, CIPM

## Table des matières

<b>I. Introduction .....</b>	<b>2</b>
<b>II. Notions et caractéristiques .....</b>	<b>4</b>
A. Définition du <i>cloud computing</i> .....	4
B. Modèles de services <i>cloud</i> .....	4
C. Modèles de déploiement .....	5
D. Caractéristiques retenues.....	6
<b>III. La résiliation des contrats <i>cloud</i> .....</b>	<b>7</b>
A. Introduction.....	7
B. Qualification juridique du contrat <i>cloud</i> .....	8
C. La résiliation en tout temps sans motif .....	11
1. Application de l'art. 404 CO ?.....	11
2. Excursus : la résiliation selon les règles du contrat de maintenance et d'outsourcing .....	12
D. Résiliation des contrats de durée pour justes motifs .....	13
E. Résiliation pour imprévision ( <i>clausula rebus sic stantibus</i> ).....	15
F. Résiliation des contrats pour inexécution .....	16
<b>IV. Les enjeux pratiques et techniques liés à la sortie des contrats <i>cloud</i> .....</b>	<b>17</b>
A. La continuité des opérations et la réversibilité.....	17
B. Le phénomène du « <i>Vendor Lock-In</i> ».....	18
C. L'accès aux données et leur portabilité.....	19
1. Notions.....	19
2. Le droit d'accès contractuel.....	21
3. Le droit d'accès légal.....	22
a) Introduction .....	22
b) L'obligation de restitution dans les contrats de service .....	23
c) Législation sur la protection des données .....	26
aa) Droit d'accès .....	26
bb) Droit à la portabilité des données .....	27

4. Excursus : le projet de règlement européen sur les données (« Data Act ») .....	29
a) Introduction .....	29
b) Droit de sortie (« <i>switching right</i> ») .....	30
<b>V. Conclusion</b> .....	<b>31</b>
<b>VI. Bibliographie</b> .....	<b>32</b>
A. Ouvrages et articles .....	32
B. Documents .....	33

## I. Introduction

L'informatique en nuage, ou « *cloud computing* »<sup>1</sup>, a connu ces dernières années un essor fulgurant en raison des nombreux avantages qu'on lui reconnaît. Le *cloud* permet des économies d'investissement importantes, puisqu'il n'est plus nécessaire d'acquérir le matériel et les logiciels nécessaires à l'exploitation de l'infrastructure informatique. Le principe du paiement à la demande (*pay-as-you-go*) permet de rapidement accroître son utilisation des ressources quand (et uniquement quand) cela devient nécessaire (phase dite de *scaling*). Les craintes liées aux risques en matière de sécurité et, dans une certaine mesure, de conformité légale se sont au demeurant réduites<sup>2</sup>.

Ces arguments ont poussé de nombreuses entreprises et organisations à se tourner vers des solutions *cloud*. Durant le processus d'acquisition, les problématiques juridiques liées à l'exploitation de la solution *cloud* sont en principe dûment analysées (ou devraient l'être) dans le cadre d'une « stratégie *cloud* ». Il est par contre plus rare que les problématiques liées à la sortie de la relation fassent l'objet d'une analyse approfondie. Or, une sortie de la relation *cloud* n'est ni hypothétique ni simple. La sortie d'une relation *cloud* pose en effet toute une série de problèmes, à la fois juridiques et pratiques/techniques. Toute stratégie *cloud* devrait en conséquence prendre en considération les problématiques liées à la sortie de la relation (l'« *exit* »). Sans cela, il peut s'avérer difficile de « corriger le tir » par la suite.

Fondamentalement, un client peut poursuivre deux objectifs dans le cadre de la sortie d'un service *cloud* : changer de prestataire ou réintégrer l'infrastructure à l'interne (ou sur une solution contrôlée par lui). S'agissant de ce second

---

<sup>1</sup> Par simplification, nous nous référons simplement au « *cloud* » dans cet article pour désigner l'informatique en nuage.

<sup>2</sup> La validation du *cloud* dans le secteur bancaire est un exemple parlant : cf. ASB, Guide *cloud*.

scénario, il peut paraître contre-intuitif à l'ère du « *cloud first* » d'imaginer un tel retour en arrière. Le recul dont on dispose désormais sur le *cloud* nous offre toutefois une image plus complète du cycle de vie du *cloud* et de son impact sur l'entreprise. Il semblerait ainsi que si le *cloud* tient clairement ses promesses économiques au début du parcours d'une entreprise (phase de croissance), la pression qu'il exerce sur les marges peut commencer à l'emporter sur les avantages à mesure que l'entreprise évolue et que sa croissance ralentit. Cette tendance du *cloud* à être de moins en moins avantageux économiquement sur le long terme a été désignée le « paradoxe du *cloud* »<sup>3</sup>.

C'est semble-t-il, le motif qui a poussé la société *Dropbox* (qui fournit la solution de stockage en ligne du même nom) à rapatrier en 2016/2017 la majorité des données de ses utilisateurs depuis les serveurs d'*Amazon Web Services* où elles étaient hébergées vers des serveurs contrôlés par *Dropbox*. Ce rapatriement aurait permis à la société d'économiser 75 millions de dollars américains sur deux ans<sup>4</sup>. Au-delà de cet exemple, il est évalué que le rapatriement du *cloud* vers des solutions sur site (ou contrôlées) peut entraîner une réduction représentant d'un tiers à la moitié du coût d'exécution sur le *cloud*<sup>5</sup>. Ainsi, les motifs économiques qui ont poussé l'organisation à se diriger vers le *cloud* pourraient donc bien, à terme, être ceux qui conduisent à décider de le quitter. Une sortie du *cloud* est en tout état de cause moins hypothétique que ce qui pourrait être intuitivement envisagé.

Après avoir introduit les notions et concepts importants du *cloud* en lien avec la présente thématique (*infra* II.), nous nous focaliserons dans cette contribution sur les problématiques liées à la résiliation des contrats *cloud* (*infra* IV.). Pour ce faire, il est tout d'abord nécessaire de s'arrêter sur la qualification juridique du contrat (*infra* III.), puis sur les problématiques liées à l'accès et au portage des données, enjeu fondamental de cette thématique (*infra* IV.C.).

---

<sup>3</sup> WANG/CASADO.

<sup>4</sup> Le rapatriement représentait 600 pétabits de données clients. Voir WANG/CASADO et <<https://www.geekwire.com/2018/dropbox-saved-almost-75-million-two-years-building-tech-infrastructure/>> (consulté le 20 avril 2022).

<sup>5</sup> WANG/CASADO.

## II. Notions et caractéristiques

### A. Définition du *cloud computing*

Conformément à la définition du *US National Institute of Standards and Technology* (NIST)<sup>6</sup>, le *cloud* est un modèle qui permet un accès réseau pratique et sur demande à des ressources informatiques configurables (par exemple le stockage, le traitement, la mémoire, la bande passante du réseau, les machines virtuelles, des applications ou des services) qui sont mises en commun pour nombreux utilisateurs. L'accès à ces ressources est rapide et ne requiert pas d'interaction formelle avec le prestataire de services.

Le *cloud* peut se présenter selon trois modèles de services et quatre modèles de déploiement différents.

### B. Modèles de services *cloud*

Les trois modèles « classiques » de services *cloud* sont les suivants :

- *Software as a Service (SaaS)* : dans le cadre du modèle *SaaS* (p. ex. *Zoom*, *Dropbox*, *Office 365*, *Salesforce*), le client a principalement accès à distance aux fonctionnalités d'une application. Cette situation se rapproche de la licence qui est concédée pour l'utilisation d'une application téléchargée sur le poste ou le réseau de l'utilisateur. La suite logicielle de Microsoft peut par exemple être soit téléchargée en local – auquel cas une licence d'utilisation « classique » est accordée (*Office 2021*) – soit utilisée sur le *cloud* (*Office 365*)<sup>7</sup>. Dans le cadre du *SaaS*, le client exploite sa propre infrastructure informatique pour accéder au service, qui est distincte de celle sur laquelle le prestataire fait fonctionner l'application<sup>8</sup>. Le modèle *SaaS*

---

<sup>6</sup> Disponible sous : <<https://csrc.nist.gov/publications/detail/sp/800-145/final>> (consulté le 20 avril 2022).

<sup>7</sup> En droit américain, une distinction fondamentale est apportée entre le téléchargement de l'application sur le poste de l'utilisateur, qui implique l'octroi d'une licence, de l'accès à distance via un réseau aux fonctionnalités du logiciel, qui ne requiert pas de licence mais un droit d'accès et d'utilisation. Cette distinction nous semble moins pertinente en droit suisse, compte tenu du large cadre des droits exclusifs de l'auteur prévus à l'art. 10 de la loi fédérale du 9 octobre 1992 sur le droit d'auteur et les droits voisins (LDA), RS 231.1.

<sup>8</sup> Le prestataire est responsable de l'application et des serveurs, réseaux, systèmes d'exploitation et de la capacité de stockage.



impliquera en règle générale un hébergement des données chez le prestataire de services<sup>9</sup>. Le modèle correspond à ce qui était auparavant appelé ASP (*Application Service Provider*)<sup>10</sup>.

- *Platform as a Service (PaaS)* : dans le cadre du modèle *PaaS* (p. ex. *Microsoft Azure App Services, AWS Elastic*), le client déploie sur l'infrastructure *cloud* ses propres applications, dont il assume la responsabilité. Le prestataire reste cependant responsable de l'infrastructure sur laquelle l'application est déployée (réseaux, serveurs, systèmes d'exploitation et stockage). Ce modèle de service est principalement utilisé par des prestataires informatiques qui veulent déployer sur le *cloud* leurs propres applications.
- *Infrastructure as a Service (IaaS)* : dans le modèle *IaaS* (p. ex. *Microsoft Azure, Amazon Web Services, Google Compute Engine*), le prestataire de services fournit la puissance de calcul, l'espace de stockage, les réseaux et d'autres ressources informatiques fondamentales (qui sont, dans le *cloud public*<sup>11</sup>, partagées entre tous les utilisateurs). Le client exploite par-dessus cette infrastructure ses propres systèmes d'exploitation et applications, dont il assume la responsabilité.

Ces trois modèles ont donné lieu par la suite à la tendance du *XaaS* ou *everything as a service*. Initialement, cette notion désigne toute fonctionnalité qui est fournie à distance (*as a service*) via une infrastructure *cloud*. Sans exhaustivité, citons le *Desktop as a Service (DaaS)*, le *Database as a Service (DBaaS)* ou encore le *Storage as a Service (STaaS)*. Si certains usages sont légitimes, car concrétisant des fonctionnalités nouvelles, d'autres ont une portée uniquement marketing et non juridique, parfois complètement déconnectée de l'informatique en nuage. Ainsi, le *Hardware as a Service* sera en principe une simple location de matériel.

L'univers du *XaaS* est ainsi infini et peut recouvrir des concepts très différents. Nous nous limiterons dans cette contribution aux trois modèles de service *cloud* classiques décrits ci-avant. S'agissant des autres modèles de services, une analyse au cas par cas sera nécessaire.

## C. Modèles de déploiement

Conformément à sa définition classique, le *cloud* peut être déployé de différentes manières. Le modèle de déploiement « standard » du *cloud* est le **cloud public**, dans le cadre duquel un prestataire met à disposition d'un grand

---

<sup>9</sup> Pour le détail, voir ANCELLE/FERDJANI, p. 139.

<sup>10</sup> DE WERRA, Contrats, p. 114 ; JACCARD/ROBERT, p. 101-102.

<sup>11</sup> *Infra* II.C.

nombre de clients une infrastructure *cloud*. *Microsoft*, *Google* et *Amazon* offrent tous trois des *cloud* publics.

Par opposition, une organisation peut elle-même exploiter (ou faire exploiter) sa propre infrastructure *cloud* au moyen d'un **cloud privé**. Il existe ainsi des différences majeures entre le *cloud* public et privé. En particulier, à la différence du *cloud* privé, le *cloud* public implique de confier certaines activités à un prestataire externe ; il s'agit donc d'une forme d'*outsourcing*<sup>12</sup>.

Enfin, il existe des modèles de **cloud hybrides**, mélangeant *cloud* privé et public<sup>13</sup>. Le *cloud* hybride permet de rechercher les avantages respectifs des autres modèles, par exemple en conservant ses données ou activités sensibles sur un *cloud* privé, tout en bénéficiant de l'élasticité du *cloud* public pour ses autres activités.

La notion de *cloud* hybride doit être distinguée de celle de **multicloud**, qui fait référence au choix de recourir aux services de différents prestataires *cloud* au lieu d'un seul. Le *multicloud* permet notamment de limiter le risque de « *vendor lock-in* » qui sera discuté ci-après<sup>14</sup>.

## D. Caractéristiques retenues

Il ressort des explications ci-avant que la notion de « contrat *cloud* » regroupe en réalité différents modèles de services et de déploiement, qui peuvent couvrir une large variété de prestations.

Nous relevons toutefois les caractéristiques suivantes :

- Caractéristique 1 : tous les contrats *cloud* impliquent l'accès à distance à une infrastructure informatique, en particulier à des applications, des serveurs, de la puissance de calcul et des espaces d'hébergement. Cette infrastructure n'est pas en tant que telle *mise à disposition* du client, car le prestataire en conserve la maîtrise et la possession exclusive. Le prestataire met à disposition ses fonctionnalités (notamment la capacité de traiter et stocker l'information), sous une forme gérée et modulable. L'élément fondamental est ainsi moins la location de machines et d'espaces de stockage, que la responsabilité de leur gestion sûre et efficiente<sup>15</sup>.

---

<sup>12</sup> Cf. *infra* II.D, caractéristique 2.

<sup>13</sup> À noter que d'autres modèles peuvent exister, p. ex. le *cloud* communautaire.

<sup>14</sup> *Infra* IV.B.

<sup>15</sup> Le client qui recherche uniquement à stocker des données pourra faire l'acquisition à moindre coût d'un espace de stockage. Ce qu'il recherche en optant pour le *cloud* est un service (complexe) qui comprend le stockage des données, l'accessibilité des données, ainsi que la gestion flexible et sûre de la fonctionnalité.

- Caractéristique 2 : le client va *externaliser* la gestion et le contrôle de cette infrastructure à un tiers. Le *cloud* est ainsi une forme d'*outsourcing*<sup>16</sup>.
- Caractéristique 3 : les fonctionnalités qui sont mises à disposition comprendront non seulement du matériel (puissance de calcul et espace de stockage), mais également le droit d'accès et d'utilisation des fonctionnalités de logiciels informatiques (licence)<sup>17</sup>. Schématiquement, l'on peut retenir que cette composante de licence sera en règle générale prépondérante dans le modèle *SaaS* et plus secondaire dans les modèles *PaaS* et *IaaS*. Une analyse au cas par cas sera toutefois nécessaire.
- Caractéristique 4 : le prestataire fournira toute une série de services. Certains services feront partie intégrante de la prestation principale (caractéristique 1), comme la maintenance de l'infrastructure et son raccord aux réseaux internet et électrique. D'autres services pourront être fournis de manière plus indépendante, comme le support (*helpdesk*), la migration de données, l'implémentation, la configuration, ou des formations, *etc.*
- Caractéristique 5 : les contrats *cloud* seront en principe conclus pour une certaine durée, qui peut être déterminée ou indéterminée. Suivant les circonstances, cette durée aura un intérêt pour les deux parties. Le client aura en effet intérêt à s'assurer que le prestataire ne puisse pas résilier du jour au lendemain le contrat<sup>18</sup>.
- Caractéristique 6 : la confiance entre les parties jouera un rôle plus ou moins important en fonction des circonstances. Le client externalisera en effet potentiellement la gestion de données sensibles (au sens large du terme) et/ou des fonctions importantes pour son activité, ce qui implique une certaine confiance du client envers son prestataire.
- Caractéristique 7 : les contrats *cloud* peuvent faire l'objet d'accord de niveaux de services (SLA) pour mesurer la conformité du prestataire avec ses obligations<sup>19</sup>.

### III. La résiliation des contrats *cloud*

#### A. Introduction

Un contrat peut toujours être résilié conformément aux règles qui y sont stipulées (résiliation conventionnelle des contrats). Cet aspect ne pose

---

<sup>16</sup> ANCELLE/FERDJANI, p. 140. Sauf en cas de modèle de *cloud* purement privé (*Supra* II.C).

<sup>17</sup> Plus spécifiquement, il s'agit généralement dans le modèle *SaaS* de la mise à disposition des fonctionnalités du logiciel, auxquelles l'utilisateur accède à distance.

<sup>18</sup> *Infra* IV.A.

<sup>19</sup> Sur les contrats SLA, voir : DE WERRA, Contrats ; GILLIÉRON.

guère de problème. L'on relèvera uniquement que le contrat peut prévoir une courte durée de résiliation (p. ex. 30 jours, voire en tout temps sans préavis) ou au contraire un long délai de résiliation (une ou plusieurs années), ou encore une durée initiale du contrat durant laquelle le contrat ne peut pas être résilié<sup>20</sup>.

Lorsque le délai de résiliation contractuel est long, il devient utile de rechercher s'il est possible de mettre fin de manière anticipée au contrat en raison d'un motif juridique impératif. Ces motifs juridiques dépendront en partie de la nature du contrat et de sa qualification juridique, qu'il est donc nécessaire de rechercher. Les contrats pourront toutefois souvent être résiliés pour des motifs juridiques indépendants du rattachement du contrat à un contrat nommé, raison pour laquelle les tribunaux renoncent parfois à sa qualification précise<sup>21</sup>.

## B. Qualification juridique du contrat *cloud*

Les contrats *cloud* entrent dans la catégorie plus générale des *contrats informatiques*. Ce terme fait toutefois référence à la technologie sous-tendant ce type de convention et peut s'appliquer à des relations juridiques très variées. La qualification juridique d'un contrat informatique dépendra donc des circonstances particulières de chaque cas et une classification *in abstracto* n'est pas possible<sup>22</sup>.

Il ressort de la jurisprudence topique que les contrats portant sur des prestations informatiques sont le plus souvent qualifiés de contrats innommés<sup>23</sup> et plus spécifiquement de contrats mixtes (*gemischten Verträge*) lorsqu'ils combinent plusieurs contrats nommés, respectivement de contrats *sui generis* (*Verträge eigener Art*) lorsqu'ils prévoient des prestations qui n'existent pas dans la législation<sup>24</sup>.

Il n'existe à notre connaissance pas de décision portant spécifiquement sur la qualification et le régime de résiliation de contrats *cloud*. Les tribunaux se sont par contre prononcés sur des thématiques qui s'en rapprochent :

- Le contrat intitulé « Hébergement Infogéré » ayant pour objet la mise à disposition de logiciels (par l'intermédiaire de licences *Microsoft*) dans un serveur virtuel, la mise à disposition d'une infrastructure matérielle et la mise à disposition d'un espace de stockage a été qualifié en première instance

---

<sup>20</sup> Selon l'expérience de l'auteur, la durée des contrats *cloud* a plutôt tendance à se raccourcir.

<sup>21</sup> Notamment : TF, arrêts 4A\_573/2020 et 4A\_575/2020 du 11 octobre 2021, c. 4.2.

<sup>22</sup> ATF 124 III 456 c. 4, JdT 2000 I 172.

<sup>23</sup> Cf. les références citées ci-après et HEUSLER/MATHYS, p. 254-255.

<sup>24</sup> JACCARD/ROBERT, p. 98.

de contrat de licence<sup>25</sup>. En appel, le Tribunal cantonal vaudois semble considérer que bien que la première prestation remplisse les caractéristiques du contrat de licence, les deux autres impliquent plutôt une mise à disposition de serveurs et d'un espace de stockage, qui se rapprochent des prestations caractéristiques du bail<sup>26</sup>. Le Tribunal laisse toutefois la question de la qualification du contrat ouverte, la résiliation devant de toute manière être appréciée selon les règles des art. 97 ss CO<sup>27</sup>.

- Le contrat ayant pour objet l'installation, l'utilisation et la maintenance d'un système de divertissement pour un hôtel a été qualifié de contrat mixte réunissant les traits d'un *contrat de bail* (vu la cession de l'usage d'un important matériel sujet à restitution, moyennant paiement d'un forfait mensuel), d'un *contrat de licence* (eu égard à la remise sous licence de logiciels spécifiques), d'un *contrat d'entreprise* (impliquant l'installation du système dans les locaux de la cliente) et, enfin, d'un *contrat de maintenance sui generis* (réglementant l'assistance à fournir durant toute la durée du contrat)<sup>28</sup>.
- Un contrat portant sur la mise à disposition d'un espace physique de stockage (armoires informatiques) alimenté par courant électrique et muni d'une connexion VPN, permettant ainsi au client d'y stocker ses propres serveurs et d'accéder à distance aux données hébergées sur ceux-ci, a été qualifié de *contrat mixte* réunissant les traits d'un *contrat de dépôt* s'agissant de la mise à disposition de l'espace physique et d'un *contrat d'entreprise de durée* (contrat innommé) pour ce qui concerne la connectivité fournie. Selon la Cour de justice de Genève, la prestation principale ne relève en effet ni du contrat de bail « *compte tenu du fait qu'elle n'impliquait pas un transfert de possession, qui constitue un élément essentiel de ce type de contrat* », ni d'un contrat de mandat, en l'absence de relation de confiance particulière entre les parties<sup>29</sup>.
- Le contrat portant sur la livraison d'un système informatique composé de matériel et de logiciel doit être soumis aux règles du contrat de vente lorsque les prestations du prestataire ne comprennent ni l'élaboration de projets pour l'ensemble du système ni le développement des applications<sup>30</sup>. Les règles du contrat d'entreprise sont par contre applicables lorsque la

<sup>25</sup> Le jugement de première instance est résumé dans la partie « en fait » de TC/VD, arrêt HC/2018/1159 du 21 décembre 2018.

<sup>26</sup> TC/VD, arrêt HC/2018/1159 du 21 décembre 2018, c. 4.3.

<sup>27</sup> Sur ce sujet, cf. *infra* III.F.

<sup>28</sup> TF, arrêts 4A\_573/2020 et 4A\_575/2020 du 11 octobre 2021 (voir également CJ/GE, arrêt ACJC/1256/2020 du 1<sup>er</sup> septembre 2020, c. 2.3).

<sup>29</sup> CJ/GE, arrêt ACJC/1083/2020 du 14 juillet 2020, c. 2.2.

<sup>30</sup> ATF 124 III 456 c. 4, JdT 2000 I 172.

livraison comporte d'importantes adaptations et individualisations du logiciel<sup>31</sup>.

- Dans un cas concernant la conception et l'élaboration d'une plateforme informatique, la Cour civile du canton du Jura a renoncé à trancher entre la qualification de contrat d'entreprise ou de contrat de mandat, relevant que l'obligation de résultat était un indice fort de rapprochement avec le contrat d'entreprise, mais notant au passage que la rémunération sous forme de tarif horaire était également un indice fort de rapprochement avec le mandat<sup>32</sup>.

Ces jurisprudences donnent des pistes concernant la qualification des contrats *cloud*, mais pas des règles. Sur cette base, et conformément aux sept caractéristiques retenues ci-avant<sup>33</sup>, l'on retiendra que les contrats relatifs au *cloud* seront le plus souvent qualifiés de *contrats mixtes de durée*, qui contiendront, selon les circonstances concrètes du cas d'espèce : (i) des éléments du contrat de licence (droit d'utilisation des fonctionnalités d'un logiciel), (ii) du contrat d'entreprise<sup>34</sup> (en cas de prestation de projet avec obligations de résultat), du contrat de maintenance<sup>35</sup>, et du mandat (notamment pour les prestations de conseil et autres services sans obligation de résultat). Un rapprochement avec le contrat de bail (ou le bail à ferme) devra s'apprécier avec extrême réserve, du fait que le contrat de bail se caractérise par le transfert de possession d'une chose ; or, si l'informatique en nuage implique fondamentalement dans la chaîne de valeur du service l'utilisation de serveurs physiques, il n'y aura pas de transfert de la possession de ceux-ci<sup>36</sup>.

Lorsqu'on se trouve confronté à un contrat mixte, il n'est généralement pas possible d'en dégager un contrat type aux éléments spécifiques clairs, ni de dire une fois pour toutes à quelles normes légales il doit être soumis. Il faut au contraire déterminer pour chaque question litigieuse quelles règles légales appliquer, selon le « centre de gravité des relations contractuelles »<sup>37</sup>.

---

<sup>31</sup> TF, arrêt 4C.393/2006 du 27 avril 2007 c. 3.1.

<sup>32</sup> TC/JU, arrêt CC/97/2015 du 7 janvier 2016, c. 4.1.

<sup>33</sup> *Supra* II.D.

<sup>34</sup> Plus spécifiquement, un contrat d'entreprise de durée (*sui generis*).

<sup>35</sup> *Infra* III.C.2.

<sup>36</sup> Voir la caractéristique 2 (*Supra* II.D) ; arrêt précité ACJC/1083/2020, c. 2.2 ; JACCARD/ROBERT, p. 101-102 ; *contra* : MÉTILLE, p. 620, selon qui le contrat portant sur l'hébergement des données informatiques contre rémunération se rapproche *a priori* du contrat de bail à loyer, ou plus vraisemblablement du contrat de bail à ferme.

<sup>37</sup> ATF 131 III 528, c. 7.1.1.

## C. La résiliation en tout temps sans motif

### 1. Application de l'art. 404 CO ?

La loi autorise dans certains cas les cocontractants à mettre un terme au contrat sans motif, le plus souvent sans délai et sans devoir indemniser le cocontractant pour le dommage qui pourrait en résulter. On parle d'un « droit » de résilier le contrat. Ce droit existe notamment dans le contrat de mandat, pour autant que la résiliation n'intervienne pas en temps inopportun (art. 404 CO).

Le Tribunal fédéral maintient jusqu'à présent que la règle de l'art. 404 CO est de droit impératif<sup>38</sup>. La règle permet donc à chaque partie de résilier unilatéralement le contrat sans délai – cela même si les parties ont convenu d'une durée – sans motif et sans avoir à indemniser l'autre partie. Cette jurisprudence est d'autant plus importante que la loi confère au contrat de mandat un caractère supplétif : ainsi, « *les règles du mandat s'appliquent aux travaux qui ne sont pas soumis aux dispositions légales régissant d'autres contrats* » (art. 394 al. 2 CO).

Comme exposé ci-avant, les contrats *cloud* seront le plus généralement qualifiés de contrats mixtes, remplissant les caractéristiques de plusieurs contrats nommés (mandat, entreprise) ou *sui generis* (licence, maintenance). Sur le principe, une résiliation conformément aux règles de l'art. 404 CO est envisageable si le centre de gravité du contrat se rapproche du mandat. Le Tribunal fédéral a d'ailleurs retenu que l'art. 404 CO peut également s'appliquer de manière impérative aux contrats de service mixtes si les règles sur le mandat semblent appropriées compte tenu de l'engagement des parties dans le temps<sup>39</sup>. L'application des règles du mandat (en lien ici avec la question de la résiliation) présuppose toutefois une relation de confiance tellement intense entre les parties qu'il serait déraisonnable de maintenir le contrat lorsque la confiance fait défaut<sup>40</sup>.

La règle de l'art. 404 CO ne s'appliquera en revanche pas aux contrats d'entreprise de durée, contrats *sui generis* et non mixtes<sup>41</sup>. La qualification du contrat d'entreprise de durée s'imposera notamment si le lien de confiance entre les parties se rapproche du lien de confiance normal entre les parties d'un contrat

---

<sup>38</sup> Cette jurisprudence est critiquée. Il n'est donc pas impossible que le Tribunal fédéral saisisse l'opportunité d'une prochaine affaire qui lui serait soumise pour renverser sa jurisprudence. Pour une analyse détaillée de la position du Tribunal fédéral sur l'art. 404 CO et des controverses à ce sujet, voir CARRON, p. 225.

<sup>39</sup> TF, arrêt 4A\_141/2011 du 6 juillet 2011, c. 2.2. Ce critère fait écho aux caractéristiques 5 et 6 que nous avons retenues (*Supra* II.D).

<sup>40</sup> TF, arrêt 4A\_146/2016 du 18 juillet 2016, c. 4.4.

<sup>41</sup> ATF 120 V 299, c. 4b).

d'entreprise classique<sup>42</sup>. La règle de l'art. 404 CO ne s'appliquera pas non plus à notre avis aux relations *cloud* dont le centre de gravité se rapproche du contrat de licence<sup>43</sup>.

Il ressort de la casuistique ci-avant<sup>44</sup> que les tribunaux ont généralement tendance à exclure l'application de l'art. 404 CO aux contrats informatiques, niant l'existence un rapport de confiance particulier. Tout contrat *cloud* implique toutefois une certaine confiance du client en son prestataire, dont l'importance dépendra fortement des circonstances<sup>45</sup>. L'application de l'art. 404 CO devra donc être analysée au cas par cas, et ne saurait être d'emblée exclue.

## 2. *Excursus : la résiliation selon les règles du contrat de maintenance et d'outsourcing*

Les contrats *cloud* comprendront souvent des prestations qui se rapprochent du contrat de maintenance et du contrat d'*outsourcing*<sup>46</sup>. Ces deux contrats ayant fait l'objet de développements jurisprudentiels et doctrinaux, il convient d'en rappeler certains principes.

Le contrat de maintenance (ou d'entretien) désigne le contrat par lequel une partie s'engage à l'égard d'une autre, contre rémunération, à contrôler un objet et à le maintenir en état de fonctionner<sup>47</sup>. Dans la mesure où l'obligation d'exécuter l'ouvrage (la maintenance) ne s'éteint pas lorsqu'elle est accomplie, mais subsiste jusqu'à l'échéance du contrat, il s'agit d'un contrat d'entreprise ayant une durée indéterminée, qui est pour ce motif qualifié de contrat innommé *sui generis*<sup>48</sup>. Un tel contrat ne peut en principe être résilié ni selon l'art. 377 CO ni selon l'art. 404 CO<sup>49</sup>. Dans un arrêt récent, la Cour de justice du canton de Genève a rattaché au contrat de maintenance les prestations d'un *contrat forfaitaire de prestations informatiques* qui portaient notamment sur l'accès 24/7 à un *Service Desk*, le *monitoring* 24/7 des serveurs et des équipements de sécurité, l'assistance pour la maintenance et le dépannage des contrôles à distance et des interventions sur site, ainsi que la garantie de bon fonctionnement de bases de données<sup>50</sup>.

---

<sup>42</sup> Arrêt précité 4A\_146/2016, c. 4.4.

<sup>43</sup> Voir la caractéristique 3 (*Supra* II.D).

<sup>44</sup> *Supra* III.B.

<sup>45</sup> Voir la caractéristique 6 (*Supra* II.D).

<sup>46</sup> Voir les caractéristiques 2 et 4 (*Supra* II.D).

<sup>47</sup> TERCIER/BIERI/CARRON, N 3549.

<sup>48</sup> ATF 130 III 458, c. 4 ; CJ/GE, arrêt ACJC/585/2018 du 24 avril 2018, c. 4.1.

<sup>49</sup> TF, arrêt 4C.139/2005 du 29 mars 2006, c. 2.2 ; arrêt précité ACJC/1256/2020, c. 2.1.5.

<sup>50</sup> Arrêt précité ACJC/585/2018, c. 4.1.



L'*outsourcing* informatique – qui est une des caractéristiques du *cloud*<sup>51</sup> – consiste à confier la gestion de l'entier ou de portions du système d'information d'une entreprise à un prestataire externe. Le contrat d'*outsourcing* informatique conclu de manière durable pour des prestations récurrentes est qualifié de contrat mixte pouvant contenir des éléments du contrat de vente, du contrat d'entreprise, du mandat ou du contrat de bail (avec réserve selon nous sur ce dernier point)<sup>52</sup>. Les règles sur la résiliation de ce type de contrats se rapprochent typiquement du contrat de maintenance, excluant en principe (comme de manière générale tous les contrats d'entreprise de durée)<sup>53</sup> une résiliation selon la règle de l'art. 404 CO. Une solution opposée n'est par principe toutefois pas exclue en cas de rapport de confiance particulier<sup>54</sup>.

#### D. Résiliation des contrats de durée pour justes motifs

En dépit de l'absence de disposition générale sur la résiliation des contrats de durée dans le Code des obligations, le Tribunal fédéral a reconnu un droit de résiliation pour justes motifs, applicable à l'ensemble des contrats de durée, y compris aux contrats informatiques<sup>55</sup>. Ce droit permet de se départir du contrat avant le terme prévu par le contrat. Il n'est pas possible de le supprimer, ni de le restreindre contractuellement. Les parties peuvent toutefois l'étendre à des circonstances qui ne constituent pas des justes motifs au sens de la loi<sup>56</sup>.

La résiliation pour justes motifs déroge au principe de la fidélité contractuelle. Elle n'est dès lors admise que de manière restrictive. Dans l'appréciation des conditions de la résiliation, le juge tient compte généralement des principes de proportionnalité et de subsidiarité<sup>57</sup>.

Le droit de résiliation des contrats de durée pour justes motifs nécessite la réalisation de deux conditions : (i) être en présence d'un *contrat de durée*, et (ii) disposer d'un *juste motif* de résiliation.

Le contrat de durée est un contrat dont la prestation caractéristique est durable<sup>58</sup>, ce qui est le cas lorsque son étendue est fonction de la période durant laquelle

---

<sup>51</sup> Voir la caractéristique 2 (*Supra* II.D).

<sup>52</sup> MORSCHER, p. 86-87. Ce point est toutefois controversé, certains auteurs estimant qu'il s'agit d'un contrat *sui generis* (voir SCHMID, N 103 ss).

<sup>53</sup> Cf. *Supra* III.C.1.

<sup>54</sup> Arrêt précité 4A\_146/2016, c. 4.4.

<sup>55</sup> Arrêts précités 4A\_573/2020, 4A\_575/2020, c. 6.1 ; arrêt précité ACJC/1256/2020, c. 3.1.1 ; SCHMID, N 863 ; WERRO, p. 672.

<sup>56</sup> VENTURI-ZEN-RUFFINEN (SJ), p. 2-3.

<sup>57</sup> VENTURI-ZEN-RUFFINEN (SJ), p. 3.

<sup>58</sup> VENTURI-ZEN-RUFFINEN (SJ), p. 8.

elle doit être fournie (et non pas de sa nature)<sup>59</sup>. Conformément à la « caractéristique 5 » retenue ci-avant (*supra* II.D), les contrats *cloud* seront en principe qualifiables de contrats de durée<sup>60</sup>.

La résiliation ne peut intervenir qu'en raison de circonstances faisant que la continuation des rapports contractuels ne peut plus raisonnablement être exigée au regard du principe de la bonne foi<sup>61</sup>. Selon la conception actuelle, c'est la protection de la personnalité au sens de l'art. 27 CC (d'un individu ou d'une entreprise) qui joue un rôle de premier plan dans la question de la résiliation anticipée pour justes motifs des contrats de durée : la partie intéressée doit pouvoir se libérer de ses obligations parce que la continuation de la relation contractuelle constituerait une restriction excessive aux droits de sa personnalité.

Le juste motif doit relever d'un changement de circonstances depuis la conclusion du contrat et être qualifiable de *grave*, tant d'un point de vue objectif que subjectif<sup>62</sup> :

- La gravité objective est appréciée conformément aux règles de la bonne foi, de sorte que le motif sera objectivement grave si on peut attendre d'un tiers raisonnable, placé dans les mêmes circonstances, qu'il résilie le contrat<sup>63</sup>. Quelques critères permettent d'apprécier la gravité objective, notamment la durée déjà écoulée du contrat ou l'existence d'un rapport de confiance particulier<sup>64</sup>. Une faute du destinataire de la résiliation sera prise en compte, mais n'est pas en soi exigée. À titre d'exemple, la Cour de justice de Genève a récemment reconnu le défaut de sauvegarde de serveurs, impliquant un risque important de perte de données, comme un motif grave fondant la résiliation pour justes motifs<sup>65</sup>.
- La gravité subjective implique que le motif invoqué soit effectivement insupportable du point de vue de la partie qui s'en prévaut. Le fait de tarder à résilier un contrat ou le fait de manifester sa volonté de poursuivre la relation contractuelle moyennant une modification de ses termes, sont des indices permettant de conclure au défaut de gravité subjective<sup>66</sup>. En effet, dans ces situations, il est souvent considéré que la partie concernée ne peut plus se prévaloir du caractère insupportable de la continuation du contrat<sup>67</sup>.

---

<sup>59</sup> VENTURI-ZEN-RUFFINEN (thèse), p. 7.

<sup>60</sup> La doctrine qualifie en général le contrat d'*outsourcing*/infogérance de contrat de durée, pour des motifs qui sont assimilables au contrat *cloud* (SCHMID, p. 24-53, N 96).

<sup>61</sup> CHERPILLOD, p. 97.

<sup>62</sup> VENTURI-ZEN-RUFFINEN (SJ), p. 12.

<sup>63</sup> *Ibid.*, p. 13.

<sup>64</sup> *Ibid.*, p. 16.

<sup>65</sup> CJ/GE, arrêt ACJC/359/2018 du 20 mars 2018, c. 3.2.1.

<sup>66</sup> VENTURI-ZEN-RUFFINEN (SJ), p. 20.

<sup>67</sup> *Ibid.*, p. 21.

Dans une affaire récente, les tribunaux ont retenu qu'une résiliation pour juste motif d'un contrat portant sur des prestations de maintenance informatique n'était pas fondée, au motif notamment que le client avait toléré pendant une durée prolongée les défauts qu'il a par la suite invoqués pour justifier sa résiliation<sup>68</sup>. Cet exemple démontre la difficulté que rencontrent souvent les clients qui, après avoir cherché à « sauver les meubles » pendant une période prolongée en maintenant la relation, se retrouvent dans une position défavorable au moment de la résiliation. Il ne faut pas oublier que la sortie d'un contrat *cloud* est compliquée, et que le client peut se trouver en partie bloqué (*locked-in*) chez un prestataire<sup>69</sup>. Dans de telles circonstances, la résiliation du contrat est envisagée par le client comme *ultima ratio*, qu'il va chercher à éviter par tous les moyens. La gravité subjective peut alors à notre avis découler du fait que tous les moyens alternatifs ont été épuisés.

En résumé, une résiliation des contrats *cloud* pour juste motif est sur le principe ouverte, à condition de pouvoir démontrer l'existence d'un juste motif objectivement et subjectivement grave qui découle d'un changement de circonstances. Ces critères devront être appliqués à l'aune du cas d'espèce. La partie qui souhaite se réserver la possibilité de résilier le contrat sur ce motif devra prendre garde à ne pas donner l'impression qu'elle tolère la situation, faute de quoi elle risque d'être forclosée dans son droit.

## E. Résiliation pour imprévision (*clausula rebus sic stantibus*)

La théorie de l'imprévision, ou *clausula rebus sic stantibus*, permet à la partie qui s'en prévaut de se dégager partiellement ou totalement de ses obligations en cas de changement important et imprévisible des circonstances, ayant pour effet de créer une disproportion si grave entre sa prestation et la contre-prestation de l'autre partie que le maintien du contrat se révélerait abusif<sup>70</sup>.

Les deux conditions suivantes doivent être réalisées :

- Une modification inévitable et imprévisible des circonstances. Le principe *clausula rebus sic stantibus* est seulement applicable si des événements nouveaux et extraordinaires sont survenus, qui n'existaient pas au moment où les parties ont conclu leur accord et ce sans intervention de la partie qui s'en prévaut<sup>71</sup>. Afin d'apprécier la prévisibilité de ces événements, il

---

<sup>68</sup> Arrêt précité ACJC/1256/2020, c. 3.3.

<sup>69</sup> *Infra* IV.B.

<sup>70</sup> GABELLON, p. 215.

<sup>71</sup> *Ibid.*, p. 220.

convient de déterminer si un contractant averti et diligent aurait raisonnablement pu les anticiper, d'après l'expérience générale de la vie et le cours ordinaire des choses<sup>72</sup>.

- Un déséquilibre excessif entre les parties. Il doit résulter de la survenance de ces événements un déséquilibre excessif entre les prestations des parties (disproportion évidente entre l'exécution de la prestation par le débiteur et l'utilité de la contre-prestation reçue)<sup>73</sup>.

Enfin, l'équilibre doit être rompu au point que l'exécution de sa prestation par la partie qui l'invoque ne peut plus être exigée, en vertu du principe de la bonne foi dans les affaires<sup>74</sup>.

Pour autant que les conditions soient remplies, une résiliation d'un contrat *cloud* pour imprévision sera ainsi possible.

## F. Résiliation des contrats pour inexécution

Les contrats *cloud* peuvent enfin être résiliés pour inexécution en vertu des articles 107 al. 2 et 109 CO lorsque le débiteur de la prestation ne s'exécute pas ou s'exécute de manière insatisfaisante (demeure qualifiée)<sup>75</sup>.

La demeure qualifiée exige avant toute chose une inexécution du contrat. Cette inexécution n'a pas besoin d'être « grave », contrairement à ce qui vaut pour la résiliation pour justes motifs<sup>76</sup>. Il faut néanmoins que l'inexécution soit continue et que le cocontractant ait octroyé un délai d'exécution supplémentaire. Selon l'art. 108 CO, la fixation d'un délai supplémentaire n'est toutefois pas nécessaire lorsqu'il ressort de l'attitude du débiteur que cette mesure serait sans effet (ch. 1), lorsque, par suite de la demeure du débiteur, l'exécution de l'obligation est devenue sans utilité pour le créancier (ch. 2) ou lorsque le contrat prévoit que l'exécution doit avoir lieu exactement à un terme fixé ou dans un délai déterminé.

Il conviendra de prendre en compte dans ce cadre les règles que les parties auront éventuellement définies dans des accords de services (SLA), qui ont pour fonction de permettre aux parties de déterminer et mesurer la qualité des services fournis. Les SLA peuvent couvrir différentes prestations, comme la disponibilité du service, la fréquence des sauvegardes ou la résolution des problèmes affectant les services<sup>77</sup>. Ces SLA pourront notamment prévoir le

---

<sup>72</sup> *Ibid.*, p. 221.

<sup>73</sup> *Idem.*

<sup>74</sup> *Idem.*

<sup>75</sup> Pour un cas d'application, voir arrêt précité HC/2018/1159, c. 5.1.

<sup>76</sup> *Supra* III.C.

<sup>77</sup> GILLIÉRON.

niveau de défaillance (ou sa fréquence) à partir duquel une résiliation « pour justes motifs » est autorisée. À titre d'exemple, un contrat *SaaS* pourra stipuler que le client est en droit de se départir du contrat pour « *material breach* » (violation grave) si les niveaux de disponibilité du service sont en deçà des niveaux fixés pendant trois mois d'affilés, ou pendant quatre mois sur une période de 6 mois.

La demeure qualifiée n'exclut pas le droit de résilier un contrat de durée pour justes motifs. Les deux voies sont alternatives : lorsqu'une partie viole le contrat et que la violation est suffisamment grave pour constituer un juste motif de résiliation, le créancier peut soit résilier le contrat pour justes motifs, soit exercer les droits tirés de la demeure qualifiée<sup>78</sup>.

## **IV. Les enjeux pratiques et techniques liés à la sortie des contrats *cloud***

### **A. La continuité des opérations et la réversibilité**

Comme toutes les prestations d'*outsourcing*, le recours à des services dans le *cloud* fait porter un risque sur la continuité des opérations de l'organisation dans l'hypothèse d'une résiliation du contrat par le prestataire<sup>79</sup>. Ainsi, la possibilité ménagée contractuellement pour le prestataire de résilier le contrat ou de cesser de fournir ses services est susceptible d'entraîner de graves conséquences pour le client, selon la criticité du service fourni. Le client doit tenir compte de ce risque dans le cadre de sa stratégie *cloud* et prendre les mesures appropriées compte tenu de l'ensemble des circonstances.

La réputation et la confiance que l'on place dans le prestataire seront souvent déterminantes. En l'absence de ces éléments, le client devra s'assurer de pouvoir facilement transitionner vers les services d'un nouveau prestataire (ou les assumer à l'interne). Or, comme nous l'évoquerons ci-après, une telle transition peut en pratique être complexe pour de nombreuses raisons. Celles-ci touchent notamment à l'accès et au caractère portable des données<sup>80</sup>. Il faut également prendre en compte le temps nécessaire à la transition vers un nouveau prestataire, qui impliquera souvent un processus de négociation contractuelle plus ou moins complexe, voire une procédure d'appel d'offres obligatoires pour les organisations qui y sont soumises. Dans ces circonstances, il est le plus souvent illusoire de pouvoir transitionner du jour au lendemain

---

<sup>78</sup> VENTURI-ZEN-RUFFINEN (SJ), p. 8.

<sup>79</sup> Le même risque surgit en cas de cessation du service, ou si les services ne correspondent pas aux attentes minimales du client.

<sup>80</sup> *Infra* IV.C.

d'un service à un autre. La situation est toutefois quelque peu plus simple lorsque l'organisation utilise déjà (dans une moindre mesure) les services du second fournisseur vers lequel elle souhaite déplacer ses charges de travail<sup>81</sup>.

C'est dans ce contexte que les *clauses de réversibilité* prennent toute leur importance. Celles-ci sont relativement usuelles dans les contrats informatiques, notamment les contrats d'*outsourcing*<sup>82</sup> et visent à permettre une réinternalisation du service par l'organisation ou une reprise par un tiers. Suivant ce qui est stipulé dans le contrat, la réversibilité peut s'appliquer en cas de résiliation ordinaire du contrat, ou alors en cas de résiliation extraordinaire<sup>83</sup>. La portée de la clause dépendra des circonstances mais peut couvrir les éléments suivants :

- la continuation des services et la prolongation des droits d'utilisation (licence) pendant une période de transition ;
- la mise à disposition pendant cette période, de manière payante ou gratuite, de certaines informations ou accès ;
- la conservation des données afin de permettre leur récupération, et
- des services spécifiques d'assistance, p. ex. pour la transformation et/ou la migration des données.

Si les parties n'ont pas prévu de clause de réversibilité, ou si celle-ci est lacunaire, des questions complexes d'interprétation du contrat se poseront afin de déterminer si le prestataire est tenu à certaines prestations, et si oui, à quelles conditions.

## B. Le phénomène du « *Vendor Lock-In* »

On parle du phénomène de « *vendor lock-in* » pour décrire la dépendance technologique des clients face à leur prestataire de services *cloud* : confrontés à la complexité pratique (et au coût) que représenterait un changement de prestataire informatique, les clients se retrouvent verrouillés (*locked-in*) chez un prestataire<sup>84</sup>. Ceci est généralement causé par l'absence d'interopérabilité entre les différents prestataires *cloud*. À titre d'exemple, les applications développées pour une plateforme *IaaS* ou *PaaS* ne seront potentiellement pas

---

<sup>81</sup> C'est justement l'un des aspects des stratégies mutlicloud, cf. *Supra* II.C. La notion de « charge de travail », de l'anglais « *workload* » fait référence à la quantité de traitement que l'infrastructure informatique doit effectuer à un moment donné.

<sup>82</sup> ANCELLE/FERDJANI, p. 156 ; MÉTILLE, p. 620. Il s'agit d'une exigence réglementaire dans le domaine bancaire : cf. FINMA, Circulaire 2018/3, § 18.1 qui impose de garantir la « réintégration ordonnée de la fonction externalisée ».

<sup>83</sup> Pour les différents motifs de résiliation, cf. *Supra* III.

<sup>84</sup> ANCELLE/FERDJANI, p. 155 ; OPARA-MARTINS/SAHANDI/TIAN, p. 2.

compatibles avec la technologie d'un concurrent, impliquant d'importantes modifications en cas de transition.

Le phénomène du *vendor lock-in* peut également restreindre la capacité du client à récupérer ses données, respectivement à les « porter » d'un service à un autre : en effet, si les données ne sont disponibles que dans un format incompatible avec le nouveau service, elles seront *de facto* inexploitable. Il en va de même si les données sont incomplètes, car fournies sans celles nécessaires à leur exploitation (comme le paramétrage ou les métadonnées).

Concrètement, cela signifie que le droit de résilier le contrat (sur une base contractuelle ou légale) ne sera que d'une maigre utilité au client qui techniquement ne peut pas récupérer les données dont il a besoin dans un format exploitable pour lui<sup>85</sup>.

## C. L'accès aux données et leur portabilité

### 1. Notions

La notion de donnée (tout comme celle d'information) est complexe. Sans rentrer dans des considérations qui dépasseraient le cadre de cette contribution, l'on retiendra que le terme « donnée numérique » regroupe toute information enregistrée dans un format lisible par une machine et capable d'un traitement automatisé<sup>86</sup>. Conformément à cette définition, la donnée numérique est composée tout d'abord d'un niveau syntaxique, c'est-à-dire de l'expression de l'information en langage informatique (une suite de « 0 » et de « 1 »<sup>87</sup>). La donnée numérique aura également souvent (mais pas nécessairement) un niveau sémantique, qui se rapporte à la signification de l'information<sup>88</sup>. Une donnée numérique peut fournir des informations sur une donnée numérique (par exemple son format, son auteur, quand elle a été créée, par qui, *etc.*) : c'est ce que l'on nomme les métadonnées. Ces métadonnées seront souvent intégrées dans le niveau syntaxique de la donnée à laquelle elles se rapportent pour former un tout.

---

<sup>85</sup> ANCELLE/FERDJANI, p. 155.

<sup>86</sup> ALI-ELI Principles for a Data Economy, art. 3(1)(b) ; PICHONNAZ, p. 436. La définition n'est toutefois pas limitée à la donnée stockée (*data in rest*) et englobe également la donnée en cours de transmission (*data in transit*) ou en cours d'utilisation (*data in use*).

<sup>87</sup> Pour l'informatique actuelle. Cela évoluera avec le *quantum computing*.

<sup>88</sup> La définition de donnée comme représentation d'une information est malheureuse. La donnée n'a pas nécessairement de sens. Pour tirer une information d'une donnée, il faut que la donnée soit exprimée dans une syntaxe correctement assemblée et compréhensible, et qu'on l'interprète pour lui donner signification (FLORIDI, p. 16).

Les données sont souvent développées de manière dynamique sur la base d'autres données ou de facteurs externes. L'on peut distinguer, hormis les données primaires développées directement et seulement par leur détenteur :

- Les « **données fournies** » (*provided data*), qui sont fournies par un tiers, par exemple le client d'un service *cloud* ;
- Les « **données observées** » (*observed data*), qui sont produites par le prestataire de services en observant l'utilisation du service. En lien avec les services *cloud*, leurs prestataires ont tendance à collecter de nombreuses données sur l'utilisation qui est faite du service. Il peut s'agir de la fréquence et de l'intensité de l'utilisation, de l'accès à certaines informations, *etc.*, et
- Les « **données dérivées** » ou « **données inférées** » (*derived data/inferred data*), qui sont générées par le traitement d'autres données et comprennent des données agrégées et des données déduites d'autres données (données primaires, fournies ou observées) à l'aide de règles de décision externes<sup>89</sup>. Dans le cadre de services *cloud*, de nombreuses données sont générées lors de l'utilisation du service. Il peut s'agir de métadonnées, de paramètres de configuration, de paramètres de sécurité, de description des droits d'accès et de journaux d'accès au service, *etc.*<sup>90</sup>

La notion de données numériques est ainsi *multidimensionnelle*, tant dans la structure (syntaxique et sémantique) que dans le type d'informations (données primaires, données secondaires et métadonnées). Cet aspect doit être pris en considération dans l'analyse des prétentions légales à leur restitution.

Il faut encore distinguer la donnée en tant que telle (dans son sens syntaxique et éventuellement sémantique) de sa manifestation physique sur un support particulier. La donnée étant non exclusive, elle peut être copiée un nombre illimité de fois sans perte d'utilité. Pour être en présence d'une copie, il faut toutefois que la syntaxe de la donnée reste inchangée. En cas de modifications, mêmes mineures, il y aura création d'un ensemble de données différent (*données dérivées*).

---

<sup>89</sup> ALI-ELI Principles for a Data Economy, art. 3(1)(i). FLORIDI, p. 20 regroupe ces données sous la notion de « données secondaires ». À la suite des ALI-ELI Principles for a Data Economy (*cf.* p. 34), nous ne différencions pas entre données dérivées et données inférées.

<sup>90</sup> *Cf.* art. 24 al. 1 let. b de la Proposition de loi EU sur les données.



## 2. Le droit d'accès contractuel

Les parties sont (relativement) libres de ménager contractuellement le droit d'accès du client aux données<sup>91</sup>. Il est toutefois usuel que les contrats relatifs à des services *cloud* prévoient les droits suivants :

- Une clause imposant au prestataire de restituer à son client les données fournies par celui-ci dans le cadre de l'exécution des services. Il est d'usage de nommer ce type de données les « données client » (*Customer Data*). Ce droit à la restitution est souvent prévu dans la clause de confidentialité du contrat, raison pour laquelle ces données sont parfois désignées données confidentielles<sup>92</sup>. La portée exacte de la notion de données client ou données confidentielles dépendra de ce que le contrat prévoit, qu'il conviendra le cas échéant d'interpréter conformément aux règles usuelles. En principe, cette notion couvrira toutes les *données fournies* par le client, mais pas nécessairement les données générées par son utilisation des services (*données observées* ou *données dérivées*).
- En cas de rapport de sous-traitance, une obligation similaire est mise à la charge du prestataire en ce qui concerne les données personnelles fournies par le client. Les règles applicables aux données personnelles font souvent l'objet de volumineux *data processing agreements*, qui reprennent les exigences de l'art. 28 RGPD<sup>93</sup>, dont en particulier l'art. 28 al. 3 let. g RGPD qui concerne la restitution ou suppression des données au terme de la prestation de service.

Si ces clauses peuvent *a priori* donner l'impression de protéger le client de manière adéquate, tel ne sera pas nécessairement le cas. En particulier, les clauses ne traiteront en général pas du format dans lequel les données client doivent être remises, ni le prix que le client doit payer pour les obtenir. Au demeurant, afin de pouvoir porter les données vers un nouveau service, le client pourra avoir besoin, en sus des données (personnelles ou non) qu'il a fournies, également de certaines *données dérivées* qui sont nécessaires à leur exploitation, par exemple le paramétrage, les métadonnées, *etc.*

---

<sup>91</sup> Sous réserve de normes impératives, *cf. infra* IV.C.3. Il faut distinguer le droit d'accès contractuel du droit d'accès légal.

<sup>92</sup> Il convient d'être prudent avec cette construction. La notion de données confidentielles est en général définie de manière restrictive et exclut p. ex. les données publiquement connues. Ainsi, une clause qui autorise le client à réceptionner ses données confidentielles pourrait de la sorte exclure toute ou partie des informations communiquées par le client qui ne sont pas d'une nature confidentielle.

<sup>93</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

Les parties seront en conséquence bien inspirées de traiter *a minima* les points suivants dans leur contrat<sup>94</sup> :

- l'étendue du droit d'accès aux données (quelles données peuvent être demandées) ;
- le format des données ;
- les modalités de transfert ;
- la durée pendant laquelle les données seront accessibles, et
- les règles sur l'effacement des données.

### 3. *Le droit d'accès légal*

#### a) **Introduction**

Ce chapitre décrit les droits légaux qui peuvent être revendiqués pour accéder aux données détenues par un prestataire *cloud*, à défaut de prétentions plus étendues prévues dans le contrat.

Il convient de mentionner d'emblée qu'il n'existe pas à l'heure actuelle en Suisse de droit de propriété sur les données en tant que telles<sup>95</sup> que le client pourrait revendiquer<sup>96</sup>. Lorsque les données fournies, observées ou dérivées contiennent des informations se rapportant à des personnes identifiées ou identifiables, il s'agira de données personnelles (art. 3a LPD<sup>97</sup>/art. 5b nLPD<sup>98</sup>). Les personnes concernées disposeront de droits sur ces données (découlant de leur droit à l'autodétermination informationnelle)<sup>99</sup>. Les données peuvent également être créées de manière anonyme ou être anonymisées ultérieurement. Ces données non personnelles – qui sont parfois qualifiées de *données techniques*<sup>100</sup> – ne sont pas définies en droit suisse et ne sont pas soumises à un statut juridique particulier. Elles ne font ainsi l'objet d'aucun droit subjectif absolu, mais d'une maîtrise de fait. Le titulaire originaire de ces données sera ainsi celui qui a initialement la maîtrise de fait sur l'information (le détenteur de secret

---

<sup>94</sup> Il s'agit d'une exigence pour les prestataires *cloud* se conformant à la *Cloud Controls Matrix* (voir CCM, contrôle IPY-04). Ces éléments pourront être intégrés dans la clause de réversibilité (*Supra* IV.A).

<sup>95</sup> DE WERRA, *Entreprise*, p. 371.

<sup>96</sup> Dans son niveau sémantique, l'information qui se rapporte à la donnée peut faire l'objet d'une protection par une loi spéciale, comme par exemple le droit d'auteur, le brevet d'invention ou le secret d'affaires.

<sup>97</sup> Loi fédérale du 19 juin 1992 sur la protection des données (LPD), RS 235.1.

<sup>98</sup> Loi fédérale du 25 septembre 2020 sur la protection des données (FF 2020 7397).

<sup>99</sup> *Infra* IV.C.3.c).

<sup>100</sup> DE WERRA, *Entreprise*, p. 366. À noter que la notion de données techniques est parfois employée pour désigner les données générées dans le cadre de l'utilisation du service (p. ex. des logs informatiques), lesquelles peuvent contenir des données personnelles.

d'affaires, le producteur d'une base de données)<sup>101</sup>. En lien avec les services *cloud*, le titulaire originaire des données observées et des données dérivées sera en conséquence le prestataire du service. La personne qui a participé à la génération de ces données<sup>102</sup>, parce qu'elle a fourni les données primaires ou parce que les données se rapportent à elle, ne disposera ainsi pas d'une prétention *in rem* sur celles-ci.

Enfin, la portée du droit d'accès peut varier : il convient de différencier le droit à la restitution du droit à la portabilité des données (ou droit au portage des données). Fondamentalement, le droit à la portabilité est un droit plus étendu que le (simple) droit à la restitution, puisqu'il permet d'obtenir les données dans un format facilitant (en théorie en tout cas) la portabilité du service. Un droit à la restitution des données est notamment prévu dans le Code des obligations pour les contrats de service<sup>103</sup>. Il n'existe par contre pas de droit général à la portabilité des données numériques détenues par un prestataire *cloud*<sup>104</sup>.

## **b) L'obligation de restitution dans les contrats de service**

Le Code des obligations contient principalement des règles sur l'obligation de restitution dans le contrat d'entreprise (art. 365 al. 2 *in fine* CO) et le contrat de mandat (art. 400 al. 1 CO)<sup>105</sup>. Comme nous l'avons vu<sup>106</sup>, les contrats *cloud* seront le plus souvent qualifiés de contrats mixtes contenant, selon les circonstances concrètes du cas d'espèce, des éléments de différents contrats nommés ou *sui generis* (principalement : contrat de licence, d'entreprise de durée, de maintenance et du mandat). Pour déterminer si les règles de l'art. 365 al. 2 *in fine* CO ou de l'art. 400 al. 1 CO s'appliquent, il faut rechercher dans le cas concret le centre de gravité du contrat par rapport à la présente thématique<sup>107</sup>. L'obligation de restitution selon ces normes constitue en principe une

---

<sup>101</sup> BENHAMOU/TRAN, p. 583.

<sup>102</sup> Les ALI-ELI Principles for a Data Economy introduisent la notion intéressante de *co-generated data* pour décrire ce type de données et proposent d'octroyer certains droits aux co-générateurs.

<sup>103</sup> *Infra* IV.C.3.b).

<sup>104</sup> Contrairement à ce qui sera prévu en droit européen, *cf. infra* IV.C.4. Le seul droit dont l'introduction est prévue est le droit à la portabilité des données personnelles (*cf. infra* IV.C.3.c)bb).

<sup>105</sup> L'art. 475 CO applicable au contrat de dépôt autorise également le déposant à réclamer en tout temps la chose déposée, avec ses accroissements, même si un terme a été fixé pour la durée du dépôt. Il est également admis que la fin du contrat de licence entraîne l'obligation de restituer ce qui a été reçu (TERCIER/BIERI/CARRON, N 7373).

<sup>106</sup> *Supra* III.B.

<sup>107</sup> ATF 131 III 528, c. 7.1.1.

obligation impérative à laquelle on ne peut renoncer valablement<sup>108</sup>. Cela dépendra toutefois de la qualification du contrat retenue, les tribunaux disposant d'une marge de manœuvre importante en présence de contrats mixtes<sup>109</sup>.

Les prétentions en restitution selon les deux dispositions précitées ne se recourent pas intégralement, l'obligation de restitution de l'art. 365 al. 2 *in fine* CO ayant une portée plus restreinte que celle fondée sur l'art. 400 al. 1 CO<sup>110</sup>. Cela étant, toutes deux concéderont à notre avis, dans les situations qui nous concernent, le droit pour le client de récupérer les données numériques qu'il a transmises au prestataire *cloud* (données fournies)<sup>111</sup>, droit qui sera en principe déjà stipulé dans le contrat<sup>112</sup>.

Les questions plus complexes à trancher concernent (i) la portée exacte du droit à la restitution et (ii) ses modalités spécifiques, notamment quant au format des données et au prix de transfert.

Le texte de l'art. 400 al. 1 CO mentionne que le mandataire est tenu à restituer « *tout ce qu'il a reçu [du chef de sa gestion], à quelque titre que ce soit* ». Cette obligation couvre non seulement ce que le mandataire a reçu du mandant ou de tiers, mais également ce qu'il a *créé lui-même par l'exécution du mandat dans l'intérêt du client*, par exemple les rapports, les plans ou les données informatiques<sup>113</sup>. L'obligation de restitution a été limitée par la jurisprudence aux documents relatifs aux affaires traitées dans l'intérêt du client, ce qui exclut les documents purement internes, les notes, *etc.*<sup>114</sup>.

Pour cette raison, l'art. 400 al. 1 CO<sup>115</sup> n'inclura à notre avis pas de droit d'obtenir les *données dérivées* qui auront été créées par le prestataire dans le cadre de la fourniture du service *cloud*, sauf dans des cas limités si celles-ci ont été créées « *par l'exécution du mandat dans l'intérêt du client* »<sup>116</sup>. Il en va de même des *données observées*, qui seront exclues du champ de l'art. 400 al. 1 CO sauf si elles ont été générées dans l'intérêt du client (p. ex. sous la forme de rapports d'activités destinés au client pour maîtriser son utilisation du

---

<sup>108</sup> TERCIER/BIERI/CARRON, N 4480.

<sup>109</sup> Arrêt précité 4A\_141/2011 du 6 juillet 2011, c. 2.2.

<sup>110</sup> Pour une analyse détaillée, voir BENHAMOU/BRAIDI/NUSSBAUMER, p. 1306-1307.

<sup>111</sup> La portée de l'art. 365 al. 2 *in fine* CO en lien avec les contrats d'entreprise atypiques est discutée. Cette controverse ne concerne toutefois pas les contrats d'entreprise de durée, qui constitue la construction juridique pertinente dans notre cas (BENHAMOU/BRAIDI/NUSSBAUMER, p. 1306-1307 et *supra* III.C).

<sup>112</sup> *Supra* IV.C.2.

<sup>113</sup> TERCIER/BIERI/CARRON, N 4493.

<sup>114</sup> ATF 122 IV 322, c. 3 aa.

<sup>115</sup> Ce qui vaut à notre avis également pour l'art. 365 al. 2 *in fine* CO.

<sup>116</sup> L'on peut songer par exemple à des métadonnées ou d'autres structurations des données effectuées à la demande du client.

service), ce qui ne sera en principe pas le cas des données collectées par le prestataire pour gérer et améliorer la fourniture du service.

La loi n'impose pas le format dans lequel les données devront être restituées. Celui-ci dépendra donc de l'accord des parties, ou à défaut du principe de bonne foi. Selon BENHAMOU/TRAN, les données remises devront être utilisables et pouvoir être lues par l'utilisateur sans utiliser de services additionnels du prestataire, ceci afin de ne pas vider de sa substance le droit du client à la restitution. Cette affirmation doit à notre avis être nuancée. Comme exposé<sup>117</sup>, chaque prestataire informatique a développé sa propre technologie propriétaire qui ne sera pas nécessairement compatible avec celle des autres prestataires. L'obligation de rendre les données utilisables pourrait nécessiter selon les circonstances des activités additionnelles du prestataire pour transformer les données. Or, l'on ne saurait transformer l'obligation de restitution prévue à l'art. 400 al. 1 CO en véritable droit au portage des données, qui n'existe en l'état pas en droit suisse<sup>118</sup>. Les parties demeurent toutefois libres de convenir de telles prestations notamment dans une clause de réversibilité<sup>119</sup>.

S'agissant du prix, le droit à la restitution doit en principe pouvoir s'exercer sans frais supplémentaires, le prix du service devant inclure toutes les obligations, y compris l'obligation légale de restitution<sup>120</sup>. Les parties demeurent toutefois libres à notre avis de définir contractuellement de quelle manière les services sont facturés, notamment en définissant des prix pour l'activité de transfert des données. Il est d'ailleurs courant que les prestataires de services *cloud* ne facturent pas le transfert des données vers le *cloud* (« *ingress* »), mais facturent la « sortie » des données (« *egress* »). À noter que cette sortie des données ne concerne pas uniquement la fin du contrat, mais s'applique chaque fois que des données quittent le réseau du prestataire vers un emplacement externe, par exemple lorsque des applications écrivent des données sur le réseau local du client<sup>121</sup>.

Le prestataire ne pourra en principe pas s'opposer à la restitution en vertu d'un droit de rétention réel (art. 895 CC), dans la mesure où ce droit ne peut porter que sur des choses réalisables par nature (art. 896 al. 1 CO)<sup>122</sup>, ce qui n'inclura pas les données numériques du client. Le prestataire pourra uniquement s'opposer à la transmission des données sur la base de l'art. 82 CO si

---

<sup>117</sup> *Supra* IV.B.

<sup>118</sup> Concernant le droit à la portabilité des données personnelles qui sera instauré par la nLPD, cf. *infra* IV.C.3.c)bb).

<sup>119</sup> *Supra* IV.A.

<sup>120</sup> BENHAMOU/TRAN, p. 585.

<sup>121</sup> Pour AWS, voir <<https://aws.amazon.com/fr/blogs/architecture/overview-of-data-transfer-costs-for-common-architectures/>> (consulté le 20 avril 2022).

<sup>122</sup> ATF 122 IV 322, c. 3c, JdT 1998 IV 129 ; cf. ég. BENHAMOU/TRAN (n. 69), p. 585.

l'obligation de paiement s'inscrit dans un rapport d'échange au sens de l'art. 82 CO avec les services fournis pour la restitution des données<sup>123</sup>.

### c) Législation sur la protection des données

#### aa) Droit d'accès

La LPD confère à la personne concernée un droit d'accès à ses données personnelles (art. 8 LPD). La nouvelle LPD maintient ce droit de manière légèrement modifiée (art. 25 à 27 nLPD). Le droit d'accès de l'art. 8 LPD/25 nLPD est large puisqu'il concerne potentiellement toutes les données détenues par le prestataire *cloud*, qu'il s'agisse de *données fournies, observées* ou *dérivées*. Ce droit connaît toutefois des limitations importantes :

- Le droit ne peut porter que sur des données personnelles, soit « *toutes les informations qui se rapportent à une personne identifiée ou identifiable* » (art. 3a LPD<sup>124</sup>). Ceci exclut ainsi les données techniques, ainsi que les données personnelles anonymisées<sup>125</sup>. À noter que les logs informatiques, métadonnées et autres données générées dans le cadre de l'utilisation du service pourront contenir des données personnelles, sans que cela soit nécessairement le cas. Il n'en demeure pas moins que le droit d'accès de la LPD est fondamentalement incomplet.
- Le titulaire du droit d'accès est la personne concernée, ce qui exclura à compter de l'entrée en vigueur de la LPD révisée l'ensemble des personnes morales (art. 5 let. a nLPD). Les personnes morales devront toutefois s'assurer contractuellement un accès suffisant aux données personnelles des tiers (par exemple leurs clients ou employés) qu'elles transmettent au prestataire *cloud*, afin de pouvoir se conformer à leurs propres obligations découlant de la LPD.
- Le but fondamental du droit d'accès est de permettre à la personne concernée de faire valoir ses droits en matière de protection des données notamment en lui permettant de vérifier si le traitement respecte les principes fixés par la loi<sup>126</sup>. La demande d'accès peut être refusée si elle

---

<sup>123</sup> *Contra* : BENHAMOU/BRAIDI/NUSSBAUMER, p. 1310, qui estiment qu'une opposition sur la base de l'art. 82 CO ne sera jamais possible.

<sup>124</sup> Loi fédérale sur la protection des données du 19 juin 1992 (LPD), RS 235.1.

<sup>125</sup> Il existe une controverse en droit suisse concernant la nature des données pseudonymisées transmises à un tiers ne disposant pas de la clé de déchiffrement. Selon certains, ces données ne constituent pas des données personnelles pour le tiers. Sur ce sujet, cf. JOTTERAND, chapitre 4, (N 49 ss).

<sup>126</sup> ATF 138 III 425, SJ 2013 I 81, c. 5.3.

visé d'autres fins, en application du principe de l'interdiction de l'abus de droit<sup>127</sup>.

Si le débiteur du droit d'accès doit communiquer les renseignements par écrit sous une forme compréhensible et prendre les mesures de sécurité nécessaires (trier les données et caviarder les autres données), il reste libre de choisir le format et n'a aucune obligation de restituer telles quelles les données ni de garantir la portabilité et l'interopérabilité des données<sup>128</sup>.

## bb) Droit à la portabilité des données

La nLPD prévoit à son article 28 un droit à la portabilité des données (appelé « *Droit à la remise ou à la transmission des données personnelles* »). À la différence du droit d'accès, ce droit ne vise pas à vérifier le respect des exigences de la LPD, mais à permettre à la personne concernée de transmettre ses données d'un système de traitement automatisé à un autre.

L'art. 28 nLPD reprend *grosso modo* le contenu de l'art. 20 RGPD. Le titulaire du droit sera la personne concernée, ce qui exclut les entreprises utilisant le *cloud* qui ne bénéficient pas directement de ce droit. Son exercice est soumis à deux conditions : (i) que le responsable du traitement traite les données personnelles de manière automatisée et (ii) que les données personnelles soient traitées avec le consentement de la personne concernée ou en relation directe avec la conclusion, ou l'exécution d'un contrat entre elle et le responsable du traitement. Ces conditions seront en principe réalisées dans le cadre de contrats *cloud* conclus avec des consommateurs (B2C)<sup>129</sup>. Le droit à la portabilité peut être limité pour les mêmes motifs que le droit d'accès (art. 29 al. 1 *cum* 26 nLPD).

De manière similaire à ce qui vaut pour le droit d'accès, le droit à la portabilité est fortement limité dans son champ d'application puisqu'il ne porte que sur des données personnelles, ce qui exclut toutes les données non personnelles qui pourraient être nécessaires au portage du service. Au demeurant, le titulaire pourra requérir uniquement la portabilité des données personnelles *qu'il a communiquées* au prestataire *cloud*, ce qui inclut celles simplement « rendues accessibles » (art. 5 let. e nLPD) par la personne concernée, mais exclut notamment les *données dérivées* générées par le prestataire. À noter que dans le cadre de l'application du RGPD, le Groupe de travail Article 29 (prédécesseur du Comité européen de la protection des données) a élargi la notion de « *données*

---

<sup>127</sup> TF, arrêt 4A\_277/2020 du 18 novembre 2020, c. 5.

<sup>128</sup> BENHAMOU/BRAIDI/NUSSBAUMER, p. 1312.

<sup>129</sup> Ce qui ne sera pas le cas des données collectées dans le cadre de relations B2B. Une personne morale ne pourrait de toute manière pas faire valoir ce droit.

*fournies* » pour couvrir non seulement les données activement et sciemment fournies par la personne concernée, mais également les *données observées* qui ont été collectées dans le cadre de l'utilisation du service ou du dispositif (par exemple l'historique de recherche, les données relatives au trafic et les données de localisation d'une personne ou des données brutes comme le rythme cardiaque enregistré par une montre connectée)<sup>130</sup>. Bien que cette position soit controversée en droit européen<sup>131</sup>, le Conseil fédéral a expressément repris cette solution à l'art. 20 de l'Ordonnance sur la protection des données du 31 août 2022, qui prévoit que le droit à la portabilité porte sur « *les données que le responsable du traitement a collectées au sujet de la personne concernée et qui concernent son comportement dans le cadre de l'utilisation d'un service ou d'un appareil* » mais pas sur les « *données personnelles que celui-ci a générées en évaluant les données personnelles mises à disposition ou observées* ». Ainsi, les données *indirectement* communiquées ou rendues accessibles par l'utilisateur du service seront couvertes par le droit à la portabilité, même si elles constituent fondamentalement des *données observées* plutôt que des *données fournies*. Il en va par exemple des données brutes sur la santé observées au moyen d'une montre connectée portée par l'utilisateur.

Le droit à la portabilité confère à la personne concernée le droit d'obtenir du responsable du traitement les données « *sous un format électronique couramment utilisé* », par quoi il faut à notre avis entendre (à la suite du droit européen), un format ouvert permettant leur réutilisation, ce qui inclut notamment les formats XML, JSON ou CSV (mais en principe pas le format PDF)<sup>132</sup>. Ce droit n'a ainsi pas pour effet d'éliminer les différences de formats utilisés entre les prestataires actifs sur le marché du *cloud*<sup>133</sup>. Le responsable du traitement peut valablement offrir de fournir les données dans l'un de ces formats, sans que la personne concernée puisse exiger de les recevoir dans un format spécifique ou au moyen d'une interface de programmation (API)<sup>134</sup>.

---

<sup>130</sup> Lignes directrices relatives au droit à la portabilité des données, p. 12.

<sup>131</sup> Pour un résumé de la controverse : Tribunal de district d'Amsterdam, décision C/13/687315/HA RK 20-207 du 11 mars 2021, § 4.75 (qui concerne une demande de portabilité émise contre la société *Uber* par des chauffeurs).

<sup>132</sup> Le rapport explicatif du Conseil fédéral du 31 août 2022 concernant l'OPDo, p. 46, mentionne les formats ouverts ou permettant l'interopérabilité tels que XML et JSON pour les grandes quantités de données ou CSV, ODT, ODS, *etc.*, mais pas les formats difficiles à traiter (p. ex. images ou PDF). Pour le droit européen, *cf.* les lignes directrices relatives au droit à la portabilité des données, p. 21. Une communication de fichiers PDF n'est toutefois pas fondamentalement exclue, *cf.* décision précitée, C/13/687315/HA RK 20-207, § 4.81.

<sup>133</sup> ANCELLE/FERDJANI, p. 155-156.

<sup>134</sup> Décision précitée C/13/687315/HA RK 20-207, § 4.80.



En définitive, malgré les bonnes intentions, l'utilité du droit à la portabilité fondé sur l'art. 28n LPD sera en principe limitée, en particulier pour les entreprises utilisatrices de services *cloud*<sup>135</sup>.

#### 4. *Excursus : le projet de règlement européen sur les données (« Data Act »)*

##### a) **Introduction**

La Commission européenne a publié le 23 février 2022 sa Proposition de règlement sur les données (*Data Act*)<sup>136</sup>. Le texte est ambitieux et vise à instaurer :

- des règles permettant aux utilisateurs d'appareils connectés d'accéder aux données générées par ces derniers et de partager ces données avec des tiers pour fournir d'autres services ;
- des règles protégeant les PME en limitant la portée des clauses contractuelles excessives imposées par une partie ayant un pouvoir de négociation nettement plus fort ;
- des moyens pour les organismes du secteur public d'accéder et d'utiliser les données détenues par le secteur privé qui sont nécessaires dans des circonstances exceptionnelles, notamment en cas d'urgence publique.
- des règles visant à permettre aux entreprises et aux individus de plus facilement changer de prestataire de services *cloud* (« *switching right* »), et
- des limitations pour le transfert hors de l'Union européenne de données non personnelles, fortement inspirées de celles prévues par le RGPD.

Nous nous focaliserons ci-après sur les règles concernant le changement de prestataire de services *cloud* (« *switching right* »), qui font l'objet du chapitre VI (art. 23 à 26) de la Proposition de règlement sur les données. Ces règles s'imposeront à tout service de traitement de données, soit : tout « *service numérique [...] fourni à un client, qui permet une administration à la demande et un large accès à distance à un ensemble modulable et élastique de ressources informatiques partagées de nature centralisée, distribuée ou fortement distribuée* » (Art. 2 al. 12 de la Proposition de règlement sur les données). On

---

<sup>135</sup> Du même avis : ANCELLE/FERDJANI, p. 155-156.

<sup>136</sup> Proposition de Règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), SEC (2022) 81 final du 23 février 2022, accessible sous <<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=COM%3A2022%3A68%3AFIN>> (consulté le 20 avril 2022) (cité : « Proposition de règlement sur les données »).

retrouve ici les caractéristiques principales du *cloud* (accès à la demande à un ensemble paramétrable de ressources informatiques partagées)<sup>137</sup>.

## b) Droit de sortie (« *switching right* »)

Les articles 23 à 25 de la Proposition de règlement sur les données instaurent un véritable droit de sortie du *cloud* (ou de changement de prestataire), en :

- interdisant notamment les clauses contractuelles prévoyant un délai de résiliation de plus de 30 jours ;
- imposant durant cette période une obligation d'assistance à charge du prestataire<sup>138</sup>, et en
- conférant au client – qui peut être un individu ou une personne morale – le droit d'obtenir (en principe sous 30 jours) non seulement « *toutes les données importées par le client* » (donc les données fournies), mais également toutes « *les données et métadonnées créées par le client et par l'utilisation du service pendant la période où le service a été fourni, y compris, mais sans s'y limiter, les paramètres de configuration, les paramètres de sécurité, les droits d'accès et les journaux d'accès au service* »<sup>139</sup>.

Cette disposition instaure ainsi un droit d'accès et de portage non seulement des *données fournies*, mais également des *données générées* qui sont nécessaires à leur exploitation.

Après une période de transition de trois ans suivant l'entrée en vigueur de la loi, les prestataires de services ne pourront plus imposer de paiement au client pour la procédure de changement de prestataire<sup>140</sup>. Ce droit devra donc être accordé gratuitement, ce qui constitue un changement de paradigme important.

Enfin, les prestataires de service *cloud* devront prendre des mesures assurant une meilleure interopérabilité de leurs services, respectivement d'assurer une équivalence fonctionnelle dans l'utilisation du nouveau service (art. 26 de la Proposition de règlement sur les données). Ces règles dépendront du modèle de service offert (*SaaS, IaaS, PaaS*)<sup>141</sup>. En l'absence de spécifications d'interopérabilité existantes, les prestataires de services *SaaS* devront exporter les « *les formats de données et structures de données pertinents, dans un format structuré, couramment utilisé et lisible par machine* ».

---

<sup>137</sup> *Supra* II.

<sup>138</sup> Art. 24 al. 1 let. a de la Proposition de règlement sur les données.

<sup>139</sup> Art. 24 al. 1 let. b de la Proposition de règlement sur les données.

<sup>140</sup> Art. 25 de la Proposition de règlement sur les données.

<sup>141</sup> Sur la notion : *Supra* II.B.

## V. Conclusion

Nous vivons dans une période d'*intensité technologique*, pour reprendre le terme employé par Satya NADELLA, le CEO de *Microsoft*, lors d'une conférence à Londres en 2018<sup>142</sup>. Aujourd'hui, le succès d'une entreprise ou d'une organisation ne dépend plus uniquement de ces propres capacités internes, mais de son aptitude à tirer le meilleur des technologies existantes. L'adoption du *cloud* s'inscrit dans cette dynamique : le basculement vers le *cloud* n'est le plus souvent plus seulement considéré comme un simple avantage, mais comme une nécessité.

Cela ne signifie toutefois pas qu'il faille se lancer tête baissée dans le *cloud*. Loin de là. S'il est aujourd'hui nécessaire d'entrer dans le *cloud*, il faudra un jour nécessairement sortir de la relation. Cette « sortie » pourra prendre diverses formes (simple changement de prestataire, réintégration *sur site*, ou plus probablement basculement sur un *cloud* privé<sup>143</sup>). Or, la sortie du *cloud* pourra se révéler complexe et coûteuse si elle n'a pas été correctement planifiée. En sus des aspects propres à la résiliation du contrat *cloud*<sup>144</sup>, la sortie du *cloud* posera de nombreux problèmes pratiques, en particulier celui de l'accès aux données qui sont nécessaires au portage du service<sup>145</sup>.

Certes, des développements sont en cours au niveau européen pour faciliter cette transition<sup>146</sup>, mais rien n'est prévu actuellement en Suisse. Le client – s'il n'a pas stipulé dans le contrat les clauses nécessaires à la réintégration ordonnée du service, notamment par le biais d'une clause de réversibilité<sup>147</sup> – devra se contenter de dispositions légales souvent lacunaires<sup>148</sup>.

---

<sup>142</sup> <<https://news.microsoft.com/en-gb/2018/11/07/microsoft-ceo-satya-nadella-on-fuelling-tech-intensity-in-the-uk/>> (consulté le 20 avril 2022).

<sup>143</sup> *Supra* II.C.

<sup>144</sup> *Supra* III.

<sup>145</sup> *Supra* IV.C.

<sup>146</sup> *Supra* IV.C.4.

<sup>147</sup> *Supra* IV.A.

<sup>148</sup> *Supra* IV.C.3.

## VI. Bibliographie

### A. Ouvrages et articles

**Juliette ANCELLE/Karim FERDJANI**, Les contrats informatiques : état des lieux et questions choisies, *in* : Alexandre RICHARD/Damiano CANAPA (éd.) CEDIDAC, Droit et économie numérique, Lausanne 2021, p. 131-158 ; **Yaniv BENHAMOU/Laurent TRAN**, Circulation des biens numériques : de la commercialisation à la portabilité, *sic !* 2016, p. 571 ; **Yaniv BENHAMOU/Guillaume BRAIDI/Arnaud NUSSBAUMER**, La restitution d'informations : quelques outils à la disposition du praticien, *PJA* 11/2017, p. 1302 ; **Maxence CARRON**, Le mandat de durée : état de la jurisprudence sur l'art. 404 CO et perspectives, *DC* 2018, p. 225 ; **Ivan CHERPILLOD**, La fin des contrats de durée, CEDIDAC, Lausanne 1988 ; **Jacques DE WERRA**, Entreprises et Big Data : peut-on forcer les entreprises à partager leurs données non personnelles (par des licences obligatoires ou des licences « FRAND ») ?, *RSDA* 2020, vol. 92, no. 4, p. 365-392 (cité : DE WERRA, Entreprise) ; **Jacques DE WERRA**, Les contrats de niveau de service, *in* : Internet 2005 : travaux des journées d'étude, CEDIDAC, Lausanne 2005, p. 110-148 (cité : DE WERRA, Contrats) ; **Luciano FLORIDI**, Philosophical Conceptions of Information, *in* : Giovanni SOMMARUGA (éd.), Formal Theories of Information, LNCS 5363, p. 13-53, 2009 ; **Adrien GABELLON**, La théorie de l'imprévision ou l'adaptation du contrat par le juge, *in* : Lukas HECKENDORF/URSCHER/Karen TOPAZ DRUCKMAN (éd.), Les difficultés économiques en droit, Genève/Zürich/Bâle 2015, p. 216 ss ; **Philippe GILLIÉRON**, Service Level Agreements (SLA) *in* : Cloud-based agreements, Best practices from a practitioner's standpoint, *Jusletter IT* 23 mai 2019 ; **Bernhard HEUSLER/Roland MATHYS**, IT-Vertragsrecht, Zürich 2004 ; **Michel JACCARD/Vincent ROBERT**, Les contrats informatiques, *in* : Pascal PICHONNAZ/Franz WERRO (éds), La pratique contractuelle : actualités et perspectives, Genève 2009, p. 95-125 ; **Alexandre JOTTERAND**, Personal Data or Anonymous Data: where to draw the lines (and why)?, *Jusletter* 15 août 2022 ; **Sylvain MÉTILLE**, L'utilisation de l'informatique en nuage par l'administration publique, *PJA* 2019, p. 609 ss ; **Lukas MORSCHER**, Leistungsbescrieb, Gewährleistung und Haftung in IT Verträgen, *in* : Florian S. JÖRG/Oliver ARTER (éds), IT-Verträge, Berne 2007 ; **Alexander SCHMID**, Der IT-Outsourcingvertrag im schweizerischen Recht Hauptleistungspflichten, Leistungsstörungen und Vertragsgestaltung, *ITSL* n° 6 2019 ; **Justice OPARA-MARTINS/Reza SAHANDI/Feng TIAN**, Critical analysis of vendor lock-in and its impact on *cloud computing* migration : a business perspective, *Journal of cloud computing*, 5 (2016) ; **Pascal PICHONNAZ**, Le concept de maîtrise exclusive des données numériques : Quelques réflexions discursives, *RDS/ZSR* 140 (2021), p. 427 ; **Pierre TERCIER/Laurent BIERI/Blaise CARRON**, Les contrats spéciaux, 5<sup>e</sup> éd., Schulthess, Zürich 2016 ; **Marie-Noëlle VENTURI-ZEN-RUFFINEN**, La résiliation pour justes motifs des contrats de durée, thèse Fribourg, 2007 (cité : VENTURI-ZEN-RUFFINEN (thèse)) ; **Marie-Noëlle VENTURI-ZEN-RUFFINEN**, La résiliation pour justes motifs des contrats de durée, *SJ* 2008 II, p. 1 (cité : VENTURI-ZEN-RUFFINEN (SJ)) ; **Sarah WANG/Martin CASADO**, The Cost of Cloud, a Trillion Dollar Paradox, 27 mai 2021 (<<https://a16z.com/2021/05/27/cost-of-cloud-paradox-market-cap-cloud-lifecycle-scale-growth-repatriation-optimization/>>, consulté le 20 avril 2022) ; **Franz WERRO**, Le droit des contrats, 2<sup>e</sup> éd., Stämpfli, Berne 2019.

## B. Documents

**ALI-ELI**, Principles for a Data Economy – Data Transactions and Data Rights – ELI Final Council Draft, septembre 2021 (cité : « ALI-ELI Principles for a Data Economy ») (accessible sous : <[https://europeanlawinstitute.eu/fileadmin/user\\_upload/p\\_eli/Publications/ALI-ELI\\_Principles\\_for\\_a\\_Data\\_Economy\\_Final\\_Council\\_Draft.pdf](https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf)>, consulté le 20 avril 2022) ; **Association suisse des banquiers (ASB)**, Guide « Cloud », Recommandations pour sécuriser le *cloud* banking, 2<sup>e</sup> éd., Juin 2020 (<[https://www.swissbanking.ch/\\_Resources/Persistent/7/b/7/e/7b7eab588cc461aa494d7b38b4c7281255ad71a8/ASB\\_Guide\\_Cloud\\_2020\\_FR.pdf](https://www.swissbanking.ch/_Resources/Persistent/7/b/7/e/7b7eab588cc461aa494d7b38b4c7281255ad71a8/ASB_Guide_Cloud_2020_FR.pdf)>, consulté le 20 avril 2022) (cité : ASB, Guide cloud) ; **Cloud Security Alliance (CSA)**, *Cloud Controls Matrix*, v.4.0.5 2022 (accessible sous <<https://cloudsecurityalliance.org/research/cloud-controls-matrix/>>, consulté le 20 avril 2022) (cité : CCM) ; **FINMA**, Circulaire 2018/3 Outsourcing, version du 4 novembre 2020 (cité : FINMA, Circulaire 2018/3) ; **Groupe de travail « Article 29 » sur la protection des données**, Lignes directrices relatives au droit à la portabilité des données, adoptées le 13 décembre 2016 (version révisée et adoptée le 5 avril 2017) ; **Conseil fédéral**, Message du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois, FF 2017 6565 ss.



---

# L'utilisation de services *cloud* par des responsables du traitement privés

PHILIPP FISCHER  
Avocat associé, OBERSON ABELS SA  
LL.M. Harvard Law School

SÉBASTIEN PITTET  
Avocat-stagiaire, OBERSON ABELS SA

## Table des matières

<b>I. Introduction .....</b>	<b>37</b>
<b>II. Champ d'application de la LPD .....</b>	<b>38</b>
A. Introduction .....	38
B. Notion de données personnelles .....	39
1. Données anonymisées .....	39
2. Données pseudonymisées .....	39
C. Notion de traitement .....	42
D. Impact de la nouvelle loi sur la protection des données .....	42
<b>III. Sous-traitance .....</b>	<b>42</b>
A. Introduction .....	42
B. Relation contractuelle avec le prestataire de services <i>cloud</i> .....	43
C. Limites du traitement .....	43
D. Absence d'obligation légale ou contractuelle de garder le secret ..	44
E. Impact de la nouvelle loi sur la protection des données .....	45
<b>IV. Recours à un <i>cloud</i> à l'étranger .....</b>	<b>45</b>
A. Introduction .....	45
B. Communications dans un État assurant un niveau de protection adéquat .....	46
C. Communications dans un État n'assurant pas un niveau de protection adéquat .....	47
1. Principes .....	47
2. Clauses-modèles de l'Union européenne .....	50
3. Mise en œuvre par les prestataires de services <i>cloud</i> .....	52
D. Impact de la nouvelle loi sur la protection des données .....	53
<b>V. Particularité des États-Unis .....</b>	<b>54</b>
A. Introduction .....	54

B.	Première épisode – <i>Safe Harbor</i> .....	54
	1. Au niveau européen .....	54
	2. En Suisse.....	55
C.	Deuxième épisode – Schrems I.....	55
	1. Au niveau européen .....	55
	2. En Suisse.....	56
D.	Troisième épisode – <i>Privacy Shield</i> .....	56
	1. Au niveau européen .....	56
	2. En Suisse.....	57
E.	Quatrième épisode – Schrems II .....	57
	1. Au niveau européen .....	57
	2. En Suisse.....	58
F.	Et maintenant ?.....	59
	1. Au niveau européen .....	59
	a) En général.....	59
	b) Recommandations du CEPD.....	60
	aa) Procédure d'évaluation du niveau de protection au sein de l'État destinataire .....	60
	bb) Mesures supplémentaires.....	61
	aaa) Les mesures techniques.....	61
	bbb) Mesures contractuelles.....	62
	ccc) Mesures organisationnelles .....	62
	cc) Résumé.....	63
	c) Nouvel accord de principe EU-US.....	63
	2. En Suisse.....	64
	a) Guide du PFPDT .....	64
	b) Communication fondée sur une analyse de risque.....	66
G.	<i>Excursus</i> : le <i>US CLOUD Act</i> .....	67
	1. <i>US CLOUD Act</i> – Partie 1 .....	68
	2. <i>US CLOUD Act</i> – Partie 2 .....	69
	3. Vers une impossibilité complète de recourir à des prestataires de services informatiques qui disposent d'un lien avec les États-Unis ? .....	70
	a) Cas <i>Health Data Hub</i> en droit européen .....	70
	b) Décision du Conseil d'État du canton de Zurich.....	72
	c) Prise de position du PFPDT s'agissant de l'utilisation de services cloud .....	73
	4. Conclusion .....	75
<b>VI.</b>	<b>Règlementation applicable dans le secteur bancaire et financier .....</b>	<b>77</b>
A.	Exigences réglementaires.....	77
B.	Exigences découlant du secret bancaire.....	78



<b>VII. Conclusion.....</b>	<b>79</b>
<b>VIII. Bibliographie .....</b>	<b>80</b>
A. Doctrine.....	80
B. Communications du Préposé fédéral à la protection des données et à la transparence .....	82
C. Autres .....	82

## I. Introduction

Au cours de ces dernières années, l'utilisation des technologies numériques n'a cessé d'augmenter. Ce recours à la technologie s'est accompagné d'une explosion quantitative de la masse de données informatiques générées et traitées par les entreprises, mais également par les personnes physiques. Cette masse de données en perpétuelle augmentation a généré de nouvelles opportunités et de nouveaux défis, notamment au niveau du stockage et de l'accès à ces informations.

Avec la mondialisation, il devient nécessaire pour une entreprise, ou pour une personne, de pouvoir accéder aux données nécessaires à son activité, non seulement depuis son bureau, mais également depuis des lieux différents. En sus, il devient indispensable de pouvoir partager les données avec d'autres personnes.

Ces défis ont conduit à l'émergence de plateformes de partage de données à travers lesquelles des utilisateurs peuvent accéder à des données informatiques stockées sur des serveurs ne se situant plus forcément au même endroit que l'utilisateur : il s'agit là de la naissance du *cloud* informatique.

L'élément caractéristique du recours à des prestations de type *cloud* est l'accès à distance à une infrastructure ou à des fonctionnalités informatiques. Le lieu de stockage des données ne se situe plus dans le réseau interne de l'entreprise, mais dans un « nuage » informatique (*cloud*). L'accès aux données est possible à tout moment et en tout lieu<sup>1</sup>. À titre d'exemples, l'utilisation de *Dropbox*, d'*Instagram* ou la sauvegarde de photos sur *iCloud* sont des fonctionnalités qui relèvent du l'utilisation de services *cloud*.

Pour diverses raisons, l'utilisation de services *cloud* s'avère avantageuse pour les entreprises et les personnes physiques<sup>2</sup>. Par exemple, le recours à un auxiliaire

---

<sup>1</sup> Le présent article fait état des développements en la matière au 3 juillet 2022. Pour plus d'informations, voir par exemple : PFPDT, Explications concernant l'informatique en nuage.

<sup>2</sup> CHAPPUIS/ALBERINI, p. 338.

indépendant qui fournit une prestation de *cloud* permet souvent à l'entreprise de réduire les coûts de son infrastructure informatique. De plus, ce type de prestation de services offre, entre autres, une plus grande capacité de calcul (et donc un meilleur accès à des produits innovants), un espace de stockage de données dynamique et une augmentation de la rapidité de l'accès aux données. Enfin, le recours à des prestataires spécialisés dans le *cloud* permet également, dans certains cas, une amélioration de la sécurité des données (notamment compte tenu du fait que les coûts des mesures de sécurité peuvent être mutualisés).

Néanmoins, l'utilisation du *cloud* n'est pas sans risques. Comme nous aurons l'occasion d'y revenir, l'utilisation de services *cloud* implique que le contrôle des données, et donc dans une certaine mesure la maîtrise sur celles-ci, est confiée à un tiers. Cette situation peut conduire à une perte de contrôle sur les données. De plus, si le fournisseur du service *cloud* est situé à l'étranger, les données peuvent être traitées dans des États qui n'assurent pas nécessairement un niveau de protection des données identique au droit suisse. Par exemple, les prestataires de services *cloud* pourraient se voir ordonner, par des autorités ou des tribunaux étrangers (typiquement ceux de l'État d'incorporation du prestataire), de fournir un accès aux données, sans obtenir le consentement préalable de leur client (le responsable du traitement).

Cet article a pour objectif de mettre en lumière certains des enjeux juridiques liés au recours à des services de type *cloud* dans la perspective du droit de la protection des données. Après avoir rappelé les contours du champ d'application de la loi sur la protection des données (RS 235.1 ; LPD) (*infra* II.), nous traiterons de deux problématiques caractéristiques de l'utilisation de services *cloud*, soit le recours à des sous-traitants (*infra* III.) et le transfert de données personnelles à l'étranger (*infra* IV.). Nous aborderons aussi le recours à un prestataire de services *cloud* basé aux États-Unis ou présentant certains liens avec les États-Unis (*infra* V.). Avant de conclure, nous évoquerons brièvement d'autres normes dont il convient de tenir compte, dans certains secteurs de l'économie, dans le cadre du lancement de projets d'utilisation de *cloud* (*infra* VI.).

## II. Champ d'application de la LPD

### A. Introduction

La LPD s'applique aux traitements de données personnelles (art. 2 al. 1 LPD). La question de savoir si le recours à un service *cloud* tombe dans le champ d'application de la LPD présuppose une qualification juridique (i) des informations mises à disposition du prestataire de services (*infra* II.B.) et (ii) des services fournis par ce dernier (*infra* II.C.).

## B. Notion de données personnelles

L'art. 3 let. a LPD définit les données personnelles comme « *toutes les informations qui se rapportent à une personne identifiée ou identifiable* ». La notion de données personnelles comporte ainsi deux composantes.

- En premier lieu, les données qui ne se rapportent pas à une « personne » (physique ou morale, physique uniquement dans le cadre de la version révisée de la LPD) sont exclues du champ d'application de la LPD. À titre d'exemples, des photos de paysage ou des informations sur un produit qui sont des données matérielles ne se rapportent pas à une « personne »<sup>3</sup>.
- En second lieu, si les données se rapportent à une personne, il convient de déterminer si cette personne est directement identifiée, auquel cas l'analyse est aisée car la donnée est directement qualifiée de « donnée personnelle », ou si cette personne est seulement « identifiable ». Une personne est *identifiable* au sens de la LPD lorsqu'elle peut être identifiée sur la base d'informations supplémentaires et avec des efforts proportionnés<sup>4</sup>. Une analyse doit être effectuée au cas par cas (et le cas échéant répétée à intervalles réguliers) en tenant notamment compte des possibilités techniques de réidentification dont dispose la personne qui traite les données.

Ce deuxième niveau d'analyse donne lieu à des questions juridiques, notamment lorsque les données sont (i) anonymisées ou (ii) pseudonymisées.

### 1. Données anonymisées

Une donnée est *anonymisée* lorsque la référence à une personne est supprimée de manière irréversible. Autrement dit, il n'existe plus de possibilité de « relier » la donnée à la personne concernée. Dans cette situation, l'information ne se rapporte plus à une personne identifiable et la donnée sort par conséquent du champ d'application de la LPD<sup>5</sup>.

### 2. Données pseudonymisées

Une donnée est *pseudonymisée* lorsque la référence à la personne est supprimée de manière réversible. Autrement dit, une clé de conversion permet au détenteur de celle-ci d'identifier la personne concernée. Dans cette situation, quand bien même la personne concernée n'est pas directement identifiée à

---

<sup>3</sup> MEIER, N 422.

<sup>4</sup> ATF 138 II 346 (*Google Street View*), c. 6.1 ; MEIER/TSCHUMY, p. 4 s. ; MEIER, N 431 ss.

<sup>5</sup> Voir par exemple : MEIER, N 437 ; FF 2017 6640 ; HIRSCH/JACOT-GUILLARMOUD, p. 159.

travers la donnée pseudonymisée, elle reste identifiable pour le détenteur de la clé de conversion.

Le Message relatif à la révision de la LPD apporte des éclaircissements sur la question de l'application de la LPD aux données pseudonymisées. Selon le Message, la LPD « *ne s'applique pas aux données qui ont été anonymisées si une réidentification par un tiers est impossible (les données ont été anonymisées complètement et définitivement) ou ne paraît possible qu'au prix d'efforts tels qu'aucun intéressé ne s'y attellera. Cette dernière règle vaut aussi pour les données pseudonymisées* »<sup>6</sup>. Il semblerait donc, à la lecture du Message, que si une réidentification par le tiers n'est raisonnablement pas possible, les données pseudonymisées sortent du champ d'application de la LPD. Cette approche correspond à l'interprétation effectuée par la doctrine selon laquelle les données pseudonymisées ne constituent pas des données personnelles pour toute personne qui ne dispose pas de la clé de conversion<sup>7</sup>.

Dans un arrêt du 4 mai 2021<sup>8</sup>, le *Handelsgericht* du canton de Zurich a également considéré qu'en cas de pseudonymisation des données, si le tiers n'a pas accès à la clé et qu'il ne peut donc pas établir un lien entre la donnée et la personne concernée, l'information n'est pas une donnée personnelle et sort ainsi du champ d'application de la LPD (en ce qui concerne les traitements effectués par le tiers)<sup>9</sup>. Par conséquent, selon le *Handelsgericht*, si des données personnelles sont pseudonymisées (ou anonymisées) avant d'être transférées à l'étranger, les règles relatives à la communication transfrontalière de données au sens de l'art. 6 LPD ne s'appliquent pas.

Le *Handelsgericht* nuance toutefois cette conclusion en précisant que si le tiers qui reçoit les données peut se procurer la clé de conversion avec des efforts

---

<sup>6</sup> FF 2017 6640, mise en évidence ajoutée.

<sup>7</sup> Pour une analyse complète de la question : HIRSCH/JACOT-GUILLARMOD, p. 160 ss. Il convient tout de même de rappeler une position contraire du PFPDT d'il y a plusieurs années (cf. 22<sup>e</sup> rapport d'activités du PFPDT (2014/2015) – Externalisation à l'étranger de données bancaires pseudonymisées), qui se fondait sur une interprétation large de l'ATF 136 II 508 (*Logistep*), interprétation qui ne devrait toutefois probablement plus être suivie aujourd'hui au vu des explications qui figurent dans le Message à l'appui de la nLPD. En outre, les autorités européennes semblent privilégier une approche plus large s'agissant de la définition de « données personnelles » (cf. décisions *Google Analytics* – décision de l'autorité autrichienne de protection des données du 22 décembre 2021 (D155.027 2021-0.586.257) ainsi que la décision de mise en demeure de la CNIL du 10 février 2022 (disponible à l'adresse : <<https://www.cnil.fr/fr/utilisation-de-google-analytics-et-transferts-de-donnees-vers-les-etats-unis-la-cnil-met-en-demeure>>, consulté le 3 juillet 2022).

<sup>8</sup> Arrêt du *Handelsgericht* du canton de Zurich n° HG190107-O du 4 mai 2021.

<sup>9</sup> Arrêt du *Handelsgericht* du canton de Zurich n° HG190107-O du 4 mai 2021, c. 3.2.3 ; voir également auparavant : Arrêt du *Handelsgericht* du canton de Zurich n° HG150170-O du 30 mai 2017.

proportionnés, les personnes concernées restent identifiables et les données entrent dans le champ d'application de la LPD. Dans cette décision, une banque envisageait de transmettre des informations pseudonymisées (dont elle était la seule à posséder la clé de conversion) au *Department of Justice* américain. Le *Handelsgericht* a considéré que le transfert des données pseudonymisées pourrait facilement conduire l'autorité américaine à introduire une requête d'entraide pour obtenir les données non pseudonymisées et qu'ainsi l'autorité pourrait, avec des efforts raisonnables, identifier les personnes concernées. Le transfert était dès lors soumis à la LPD<sup>10</sup>.

En pratique, dans l'utilisation du *cloud* par des privés, si le responsable du traitement dispose à lui seul de la clé de conversion (système généralement désigné par l'appellation « *Hold Your Own Key* » (HYOK)), le tiers ne dispose en principe pas de la possibilité de forcer le responsable du traitement à lui fournir la clé qui donnerait accès aux données personnelles non pseudonymisées. Il conviendra néanmoins de déterminer si le tiers pourrait réussir à obtenir un accès à la clé de conversion par un autre biais. Dans cette analyse, de nombreux facteurs doivent être analysés afin de déterminer (i) si le tiers peut objectivement avec les moyens dont il dispose obtenir les données personnelles et (ii) si le tiers a un intérêt suffisant pour déployer de tels efforts en vue de l'identification<sup>11</sup>.

En résumé, si les données sont anonymisées préalablement au transfert au prestataire de services, ces données sortent du champ d'application de la LPD. S'agissant des données pseudonymisées, une analyse au cas par cas s'avérera nécessaire pour déterminer si le tiers peut (ou non) procéder à une réidentification (*reverse engineering*) avec des efforts raisonnables.

---

<sup>10</sup> Voir également : TF, 4A\_365/2017 du 5 octobre 2018, c. 5.2.2, résumé par JACOT-GUILLARMOD, US Programm : le transfert de données clients pseudonymisées, in <[www.lawinside.ch/660/](http://www.lawinside.ch/660/)> (consulté le 3 juillet 2022).

<sup>11</sup> MEIER/TSCHUMY, p. 5. Dans la décision ATF 136 II 508 (*Logistep*), le Tribunal fédéral a notamment estimé qu'une adresse IP pouvait être considérée comme une donnée personnelle. L'activité d'une société consistait en la poursuite de violation du droit d'auteur sur internet. La société déposait une plainte contre inconnu et pouvait ensuite accéder au dossier pénal et retrouver l'utilisateur derrière l'adresse IP (une information communiquée par le prestataire de services en matière d'accès à Internet aux autorités pénales). Le Tribunal fédéral a considéré ici que les adresses IP conservées par la société étaient des données personnelles et que la société devait se prévaloir d'un motif justificatif pour justifier son traitement (ce qu'elle n'a pas réussi à démontrer). Cette décision démontre la difficulté à circonscrire de manière définitive la notion de « donnée personnelle ». Voir également, s'agissant de la qualification juridique des adresses IP en tant que « donnée personnelle » : CJUE, affaire C-582/14, du 19 octobre 2016, *Patrick Beyer contre Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.

## C. Notion de traitement

Selon l'art. 3 let. e LPD, « 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 » doit être considérée comme un traitement.

Par définition, un service *cloud* est une plateforme de stockage de données, étant précisé que les services fournis ne se limitent généralement pas au pur stockage (mais comprennent également d'autres traitements de données). Partant, les services fournis entrent dans la définition de « traitement », pour autant naturellement que les informations mises à disposition du prestataire puissent être qualifiées de « données personnelles » (*supra* II.A.).

## D. Impact de la nouvelle loi sur la protection des données

La nouvelle loi sur la protection des données n'apporte pas de modification majeure aux définitions de « données personnelles » et de « traitement ». Une modification mérite tout de même d'être mentionnée.

Selon le droit actuel, la notion de donnée personnelle couvre les données relatives à des personnes physiques et des personnes morales. Le traitement de données d'une personne morale est ainsi soumis à la LPD. Cette particularité, que l'on ne retrouve pas en droit européen, sera supprimée. Le champ d'application de la nouvelle LPD sera ainsi limité aux données personnelles de personnes physiques.

## III. Sous-traitance

### A. Introduction

Dans une perspective de protection des données, l'utilisation de services *cloud* implique le recours à un sous-traitant au sens de l'art. 10a LPD<sup>12</sup>. Dès lors, le responsable du traitement doit respecter les différentes conditions fixées à l'art. 10a LPD. Plus précisément, le traitement par le prestataire de services *cloud* doit (i) être régi par un contrat garantissant la protection des données (*infra* III.B.), (ii) ne pas dépasser les traitements que le responsable du traitement

---

<sup>12</sup> Dans la nLPD, cette disposition a été reprise à l'art. 9 LPD. Cf. *infra* III.E. s'agissant des modifications apportées par la nouvelle LPD.

pourrait lui-même effectuer (*infra* III.C.) et (iii) ne pas être interdit par une obligation contractuelle ou légale de garder le secret (*infra* III.D.).

## **B. Relation contractuelle avec le prestataire de services *cloud***

La prestation du service *cloud* doit faire l'objet d'un contrat entre le responsable du traitement et le prestataire de services *cloud*. Ce contrat doit notamment prévoir des mesures techniques et organisationnelles garantissant la sécurité des données. Il doit également contenir des clauses qui assurent la confidentialité, la disponibilité et l'intégrité des données (art. 10a al. 2 et 7 LPD ainsi que les art. 8 ss et 20 ss OLPD<sup>13</sup>).

Par ailleurs, quand le responsable du traitement recourt à un tiers, il lui incombe de garantir le respect des normes de la LPD par le sous-traitant<sup>14</sup>. Le responsable du traitement est ainsi tenu de choisir avec soin, d'instruire et de surveiller le prestataire de services *cloud*<sup>15</sup>.

En outre, le recours à un prestataire de services *cloud* implique souvent un recours indirect à des « sous-sous-traitants », à savoir les sous-traitants du prestataire de services. Cette situation, traitée plus particulièrement dans la nLPD (art. 9 al. 3 nLPD qui impose un consentement préalable du responsable du traitement en cas de recours à un « sous-sous-traitant »), doit également être réglée dans les rapports contractuels entre le responsable du traitement et le prestataire de services *cloud*. Par exemple, le responsable du traitement doit avoir la possibilité de refuser le recours à certains « sous-sous-traitants ». De manière plus générale, le niveau de protection des données garanti dans la relation entre le responsable du traitement et le prestataire de service *cloud* doit également être respecté par le « sous-sous-traitant ».

## **C. Limites du traitement**

Au terme de l'art. 10a al. 1 let. a LPD, le prestataire de services *cloud* ne peut effectuer que « *les traitements que le mandant serait en droit d'effectuer lui-même* ». Il peut, en outre, faire valoir les mêmes motifs justificatifs que le mandant (art. 10a al. 3 LPD). Encore une fois, il appartient au responsable du traitement, dans sa relation contractuelle avec le prestataire de services *cloud*,

---

<sup>13</sup> Ordonnance du Conseil fédéral du 14 juin 1993 relative à la loi sur la protection des données (RS 235.11 ; OLPD).

<sup>14</sup> BSK DSG/BGÖ-BÜHLER/RAMPINI, art. 10a, N 11 ; SCHWARZENEGGER/THOUVENIN/STILLER/GOERGE, p. 30.

<sup>15</sup> SCHWARZENEGGER/THOUVENIN/STILLER/GOERGE, p. 31.

de limiter les traitements que le prestataire de services *cloud* est autorisé à effectuer et de mettre en place des outils (par exemple un droit d'audit) qui permettent de vérifier la bonne exécution de cette obligation.

#### **D. Absence d'obligation légale ou contractuelle de garder le secret**

Finalement, pour pouvoir confier le traitement de données à un tiers, le responsable du traitement doit s'assurer qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

S'agissant d'une obligation légale, la situation problématique la plus classique est l'existence d'un secret professionnel (par ex. l'art. 321 CP<sup>16</sup> dans le domaine de la santé ou des avocats ou l'art. 47 LB<sup>17</sup> dans le domaine bancaire). Dans ces situations, il convient de déterminer si le prestataire de services *cloud* doit être considéré comme un auxiliaire. Le cas échéant, le détenteur du secret n'aura pas nécessairement besoin du consentement du propriétaire du secret pour recourir à un prestataire de services *cloud* pour autant que les données ne soient pas transférées ou rendues accessibles en dehors de la Suisse. En revanche, si le prestataire de services *cloud* n'est pas considéré comme un auxiliaire, le détenteur du secret viole son obligation de confidentialité lorsqu'il communique des données au prestataire.

Dans la profession d'avocat, la doctrine majoritaire semble donner une réponse plutôt favorable à cette question en qualifiant généralement le prestataire de services *cloud* comme un auxiliaire, pour autant que ce dernier soit soumis à certaines obligations de confidentialité et qu'il ait été choisi avec soin par l'avocat<sup>18</sup>. Dans le domaine de la santé, la doctrine semble plus partagée sur cette question<sup>19</sup>.

S'agissant d'une obligation contractuelle, le responsable du traitement devra minutieusement vérifier qu'aucune délégation n'est exclue dans sa relation contractuelle avec la personne concernée.

---

<sup>16</sup> Code pénal suisse du 21 décembre 1937 (RS 311.0 ; CP).

<sup>17</sup> Loi fédérale du 8 novembre 1934 sur les banques et les caisses d'épargne (RS 952.0 ; LB).

<sup>18</sup> Par exemple : JOTTERAND, p. 180 ; BENHAMOU/ERARD/KRAUS, p. 120 ss ; CHAPPUIS/ALBERINI, p. 339 ss ; ROSENTHAL, Microsoft ; Voir également ATF 145 II 229 qui semble confirmer ceci ; *Contra* : WOHLERS, p. 22.

<sup>19</sup> GILLIÉRON est d'avis que le prestataire devrait être considéré comme un auxiliaire ; ERARD semble plus partagé, voir opposé à un recours à des prestataires *cloud* dans le domaine médical (ERARD, N 1364 ss).



## E. Impact de la nouvelle loi sur la protection des données

Sur le principe, la nouvelle loi sur la protection des données n'apporte pas de changement particulier s'agissant des obligations du responsable du traitement en cas de recours à un sous-traitant (art. 9 al. 3 nLPD). Comme mentionné ci-dessus, la nLPD a apporté quelques précisions en cas de « sous-sous-délégation ». Par ailleurs, la nouvelle disposition (art. 9 nLPD) impose au responsable du traitement un devoir d'information à la personne concernée en cas de recours à un sous-traitant (art. 19 al. 2 let. c nLPD).

Pour le surplus, l'on s'attend que la pratique qui s'est développée sous l'empire de l'art. 28 RGPD<sup>20</sup> s'agissant du contenu du contrat de délégation s'applique également en Suisse, en particulier après l'entrée en vigueur de la nouvelle LPD<sup>21</sup>.

## IV. Recours à un cloud à l'étranger

### A. Introduction

Lorsque le responsable du traitement recourt à un prestataire de services *cloud* à l'étranger ou plus généralement que les données personnelles seront accessibles depuis l'étranger, le responsable du traitement doit respecter les conditions de l'art. 6 LPD.

L'art. 6 LPD distingue deux situations en fonction du niveau de protection offert par l'État vers lequel les données sont communiquées. Après avoir examiné les particularités des communications dans un État assurant un niveau de protection adéquat (*infra* IV.B.), nous analyserons les particularités des communications dans un État n'assurant pas un tel niveau de protection (*infra* IV.C.).

Indépendamment de l'État vers lequel les données personnelles sont transmises ou rendues accessibles, une communication des données au prestataire de services *cloud* constitue un traitement de données personnelles qui doit respecter les principes généraux de la LPD (notamment : art. 6 et 8 LPD)<sup>22</sup>. En effet, même si l'État de destination dispose d'un niveau de protection adéquat, le responsable du traitement doit s'assurer que (i) la communication et (ii) le traitement à l'étranger (s'il s'agit d'un cas de délégation) respectent les principes

---

<sup>20</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (RGPD), Texte présentant de l'intérêt pour l'EEE, JO L 119, du 4 mai 2016, p. 1 ss.

<sup>21</sup> VASELLA, La nouvelle loi sur la protection des données, p. 280.

<sup>22</sup> BSK DSG/BGÖ-MAURER-LAMBROU/STEINER, art. 6, N 11 ; MEIER, N 1290.

de la LPD, une communication n'étant donc pas automatiquement autorisée par la LPD si elle est effectuée vers un État assurant un niveau de protection adéquat<sup>23</sup>.

À titre d'exemple, le responsable du traitement doit analyser si le transfert de l'ensemble des données à l'étranger est nécessaire ou si ce dernier contrevient au principe de proportionnalité. Ainsi, selon un exemple donné par MEIER, la communication du dossier complet d'un employé à l'étranger (même dans un État assurant un niveau de protection adéquat) à une autre entité du groupe pour la gestion des salaires et des analyses statistiques ne s'impose pas nécessairement et pourrait partant violer le principe de proportionnalité<sup>24</sup>.

## **B. Communications dans un État assurant un niveau de protection adéquat**

L'art. 6 LPD reflète le principe que des données personnelles peuvent être communiquées à l'étranger si l'État concerné dispose d'une législation garantissant un niveau de protection adéquat. Ainsi, en cas de transfert de données vers un tel État, le responsable du traitement peut en principe se fonder sur la présomption que la communication est autorisée au sens de la LPD (sous réserve du respect des autres obligations découlant de la LPD).

Le responsable du traitement doit toutefois toujours s'assurer que la personne qui reçoit les données ne recourt pas à des sous-traitants (disposant d'un accès aux données personnelles) situés dans des États n'assurant pas un niveau de protection adéquat, auquel cas le responsable du traitement devra prendre des mesures supplémentaires (*infra* IV.C.)<sup>25</sup>.

La liste des États garantissant un niveau de protection adéquat est tenue par le Préposé fédéral à la protection des données à la transparence (le « PFPDT ») et disponible en ligne<sup>26</sup>. L'entrée en vigueur de la nLPD et de son ordonnance opérera un changement d'ordre formel puisqu'il appartiendra directement au Conseil fédéral d'établir la liste des États assurant un niveau de protection adéquat. En effet, la OPDo proposera directement la liste des États, territoires, secteurs déterminés dans un État ou organismes internationaux au sein desquels

---

<sup>23</sup> TAF, A-6242/2010 du 11 juillet 2011, c. 10.3.

<sup>24</sup> MEIER, N 1291.

<sup>25</sup> Dans certaines situations, si le prestataire de services *cloud* fait partie d'un groupe dont la société mère se situe dans un État ne garantissant pas un niveau de protection adéquat, le responsable du traitement peut également être soumis à d'autres obligations (sur ce point, *infra* V.G.).

<sup>26</sup> <[https://www.edoeb.admin-ch/dam/edoeb/fr/dokumente/2021/20211115\\_Staatenliste\\_f.pdf](https://www.edoeb.admin-ch/dam/edoeb/fr/dokumente/2021/20211115_Staatenliste_f.pdf.download.pdf/20211115_Staatenliste_f.pdf)> (*consulté le 3 juillet 2022*).

un niveau de protection adéquat est garanti (art. 8 al. 1 OPDo *cum* Annexe 1 OPDo). L'on ne s'attend toutefois pas à ce que cette liste soit substantiellement différente de celle établie par le PFPDT.

## **C. Communications dans un État n'assurant pas un niveau de protection adéquat**

### *1. Principes*

Selon l'art. 6 al. 2 LPD, plusieurs situations peuvent conduire le responsable du traitement à être autorisé à communiquer des données personnelles dans un État ne garantissant pas un niveau de protection adéquat.

- Des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger (art. 6 al. 2 let. a LPD)

En pratique, le recours à des solutions contractuelles (art. 6 al. 2 let. a LPD), et plus particulièrement l'intégration de clauses modèles dans la relation contractuelle, sont les solutions les plus utilisées en cas de recours à des services *cloud*. Les responsables du traitement recourent le plus souvent aux clauses-modèles de l'Union européenne (les *Standard Contractual Clauses* de l'Union européenne ou SCC-UE). Nous analyserons par conséquent cette hypothèse plus en profondeur dans le chapitre suivant (*infra* IV.C.2.).

- La personne concernée a, en l'espèce, donné son consentement (art. 6 al. 2 let. b LPD)

Selon l'art. 4 al. 5 LPD, un consentement n'est valable que si la personne concernée (i) a librement exprimé sa volonté concernant un ou plusieurs traitements déterminés et (ii) après avoir été dûment informée. La disposition précise encore que lorsque le traitement concerne des données sensibles et des profils de la personnalité, le consentement doit au surplus être explicite.

La particularité de cette exception qui découle de l'art. 6 al. 2 let. b LPD réside dans le fait que la personne concernée peut révoquer en tout temps son consentement tant que la communication n'a pas eu lieu<sup>27</sup>. En cas de flux d'informations continu avec un État tiers, par exemple en cas de recours à des services de type *cloud*, l'échange d'informations doit s'arrêter dès le moment où la personne révoque son consentement.

Cette possibilité pour la personne concernée de retirer en tout temps son consentement génère une insécurité juridique pour le responsable du traitement qui perd en quelque sorte la maîtrise de la licéité du transfert des données. C'est

---

<sup>27</sup> MEIER, N 1343.

pourquoi, le recours à cette institution juridique pour fonder une communication peut s'avérer compliqué à mettre en œuvre en pratique, en particulier en cas d'utilisation de services *cloud*.

- Le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées concernent le cocontractant (art. 6 al. 2 let. c LPD)

Une première précision concerne l'exigence de la nécessité de la communication. Bien que cela ne figure pas explicitement dans la disposition, il ne suffit pas que la communication soit utile ou opportune pour pouvoir se prévaloir de cette exception<sup>28</sup>. Comme le relève le Message, la disposition ne s'applique « *que si la communication de données personnelles à l'étranger est indispensable pour la conclusion ou l'exécution d'un contrat* »<sup>29</sup>. Le champ d'application de l'art. 6 al. 2 let. c LPD doit donc être interprété de manière restrictive, la preuve du caractère indispensable de la communication devant être apportée par le responsable du traitement.

La doctrine et le PFPDT fournissent plusieurs exemples de situations dans lesquelles l'art. 6 al. 2 let. c LPD pourrait trouver application<sup>30</sup>. L'exemple le plus classique est celui de l'agence de voyage qui communique des données personnelles de ses clients à l'hôtel dans lequel ces derniers vont séjourner ou à une compagnie de transport qui doit les prendre en charge<sup>31</sup>.

Bien que l'utilisation d'un service *cloud* s'avère souvent économiquement avantageuse et bénéfique pour une entreprise, ce service ne pourra en principe pas être en relation directe avec l'exécution d'un contrat *conclu avec le client de l'entreprise (la personne concernée)*. En effet, l'absence du caractère nécessaire de la communication écartera dans la plupart des situations la possibilité, pour le responsable du traitement, de se prévaloir de cette disposition.

- La communication est, en l'espèce, indispensable soit à la sauvegarde d'un intérêt public prépondérant, soit à la constatation, l'exercice ou la défense d'un droit en justice (art. 6 al. 2 let. d LPD)

Dans l'activité typique d'une personne privée, le recours à cette exception est peu fréquent en raison du caractère indispensable que doit revêtir la communication. Plus particulièrement, dans le recours à des services *cloud*, cette exception ne trouvera probablement jamais application. En effet, la disposition

---

<sup>28</sup> MEIER, N 1348 ; PFPDT, Communication, p. 7.

<sup>29</sup> FF 2003 1941.

<sup>30</sup> MEIER, N 1358 ; BSK DSG/BGÖ-MAURER-LAMBROU/STEINER, art. 6, N 31.

<sup>31</sup> PFPDT, Communication, p. 8 ; MEIER, N 1355 ; BSK DSG/BGÖ-MAURER-LAMBROU/STEINER, art. 6, N 31.

visé à protéger des communications ponctuelles et exceptionnelles, ce qui ne coïncide pas avec la nature d'un service *cloud*.

- La communication est, en l'espèce, nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée (art. 6 al. 2 let. e LPD)

Pour les mêmes raisons qu'évoquées ci-dessus s'agissant de l'art. 6 al. 2 let. d LPD, cette exception ne s'appliquera pas dans le cadre du recours à des services *cloud*.

- La personne concernée a rendu les données accessibles à tout un chacun et elle ne s'est pas opposée formellement au traitement (art. 6 al. 2 let. f LPD)

Cette disposition reprend l'art. 12 al. 3 LPD, une disposition en vertu de laquelle il n'y a, en règle générale, pas d'atteinte à la personnalité en cas de traitement de données personnelles lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée expressément au traitement.

Cette exception vise notamment les données d'identité, les adresses, numéros de téléphone ou autres données personnelles rendues publiques dans les médias ou sur internet<sup>32</sup>. Des données publiées sur internet mais non publiques (par exemple sur un compte d'un réseau social avec des restrictions d'accès) ne tombent ainsi pas dans le champ d'application de la disposition.

Par ailleurs, il convient également d'analyser préalablement à la communication si les données personnelles ont été mises à disposition du public par la personne concernée (ou avec son accord) ou si, au contraire, les données ont été communiquées contre la volonté ou à l'insu de la personne concernée<sup>33</sup>.

S'agissant du recours à des services *cloud*, cette exception ne devrait probablement pas être pertinente car le responsable du traitement souhaite transférer à l'étranger des données personnelles qui ne sont en majorité pas disponibles au public.

- La communication a lieu au sein d'une même personne morale ou société ou entre des personnes morales ou sociétés réunies sous une direction unique, dans la mesure où les parties sont soumises à des règles de protection des données qui garantissent un niveau de protection adéquat (art. 6 al. 2 let. g LPD)

Comme mentionné précédemment, le recours à des services *cloud* s'effectue en principe à travers une société tierce. Cette dernière ne faisant par définition

---

<sup>32</sup> MEIER, N 1574.

<sup>33</sup> Voir notamment MEIER, N 1381.

pas partie du même groupe que le responsable du traitement, cette exception n'est pas pertinente dans le cadre des services *cloud*.

Finalement, comme mentionné ci-dessus, même si le responsable du traitement peut se prévaloir d'une des exceptions de l'art. 6 al. 2 LPD, il reste tenu de respecter les principes généraux de la LPD.

## 2. *Clauses-modèles de l'Union européenne*

Les SCC-UE constituent des clauses contractuelles qui visent à assurer un niveau de protection adéquat lors d'un traitement de données personnelles. Les SCC-UE reprennent ainsi les obligations qui découlent du RGPD et de manière générale de la LPD pour imposer, sur une base contractuelle, au récipiendaire à l'étranger de protéger adéquatement les données personnelles des personnes concernées (nonobstant l'absence d'une réglementation locale comparable au droit suisse).

Récemment modifiée<sup>34</sup>, la nouvelle version des SCC-UE apporte quelques modifications qu'il convient de relever. Tout d'abord, les nouvelles SCC-UE se présentent sous la forme de quatre modules qui reprennent les principales relations juridiques qui peuvent exister entre l'exportateur et l'importateur des données personnelles<sup>35</sup> :

- Module 1 : transfert de responsable du traitement à responsable du traitement ;
- Module 2 : transfert de responsable du traitement à sous-traitant ;
- Module 3 : transfert de sous-traitant à sous-traitant ; et
- Module 4 : transfert de sous-traitant à responsable du traitement.

Ensuite, les nouvelles SCC-UE augmentent les obligations des parties, s'agissant par exemple des obligations en matière de transparence, de sécurité et de documentation<sup>36</sup>.

Comme mentionné ci-dessus, les entreprises suisses ont fréquemment recours aux SCC-UE pour transférer des données vers des prestataires étrangers, notamment aux États-Unis. La dernière version des SCC-UE a ainsi été reconnue par le PFPDT (moyennant les ajustements ponctuels présentés ci-dessous) comme un mécanisme de protection valable peu après sa mise en œuvre au sein de l'Union européenne<sup>37</sup>.

---

<sup>34</sup> Sur l'évolution des SCC-UE, *infra* V.

<sup>35</sup> Pour une analyse détaillée : REICHLIN/KASPER.

<sup>36</sup> REICHLIN/KASPER.

<sup>37</sup> Prise de position du PFPDT du 27 août 2021.

Par conséquent, les responsables du traitement suisses peuvent se fonder sur les SCC-UE pour exporter des données personnelles vers des pays qui n'assurent pas un niveau de protection adéquat<sup>38</sup>. Comme indiqué, les responsables du traitement doivent néanmoins prendre en considération certains points additionnels afin de garantir la compatibilité des SCC-UE avec le droit suisse de la protection des données (*Swiss finish*)<sup>39</sup>.

Selon le PFPDT, le responsable du traitement (ou le sous-traitant) suisse qui exporte les données personnelles doit notamment intégrer les points suivants dans la relation contractuelle lorsqu'il recourt au SCC-UE.

- Les parties doivent prévoir que toutes les références au RGPD doivent être lues comme des références au droit suisse.
- Les SCC-UE doivent comporter une annexe ou être modifiées afin de préciser que le terme « État membre de l'UE » ne doit pas être interprété de manière à ce que les personnes concernées se trouvant en Suisse soient privées de la possibilité de faire valoir leurs droits<sup>40</sup>.
- Le PFPDT est l'autorité de surveillance (une surveillance parallèle avec les autorités européennes devant être prévue si le RGPD est également applicable au transfert régi par les SCC-UE)<sup>41</sup>.
- Les SCC-UE doivent s'appliquer aux données personnelles des personnes morales tant que la nouvelle LPD n'est pas entrée en vigueur.

Avec ces modifications qui, à l'exception de la dernière, ne pose généralement pas de difficulté en pratique, les SCC-UE peuvent ainsi être adaptées à une utilisation par un responsable du traitement suisse (SCC-UE/CH).

Finalement, le responsable du traitement doit prendre les mesures adéquates pour s'assurer que le destinataire est effectivement en mesure de respecter ses engagements contractuels. Ce dernier point peut soulever certaines interrogations dans son application pratique. En particulier, lorsque l'État destinataire ne dispose pas d'un niveau de protection adéquat et surtout qu'il prévoit des règles impératives qui font échec au respect des garanties contractuelles, le responsable du traitement doit se demander si une communication paraît appropriée et surtout licite. En effet, lorsque le responsable du traitement sait qu'il existe un risque que le cocontractant ne puisse pas respecter les garanties contractuelles, doit-il tout de même considérer que ces garanties suffisent à protéger adéquatement les personnes concernées ? Cette question fera l'objet d'une discussion spécifique ci-après, en prenant l'exemple des États-Unis (*infra* V.).

---

<sup>38</sup> Sous réserve de certaines exceptions. Sur ce point, voir *infra* V.

<sup>39</sup> Prise de position du PFPDT du 27 août 2021, p. 2 ss.

<sup>40</sup> Prise de position du PFPDT du 27 août 2021, p. 5.

<sup>41</sup> Prise de position du PFPDT du 27 août 2021, p. 5.

### 3. *Mise en œuvre par les prestataires de services cloud*

Alors même qu'en règle générale, la souscription de services auprès des principaux fournisseurs de services *cloud* (i) se fait par le biais d'un contrat avec une entité du groupe située dans l'Union européenne et (ii) implique un stockage des données sur des serveurs situés dans l'Union européenne, des transferts et/ou des accès depuis des États n'offrant pas un niveau de protection des données adéquat interviennent dans le cadre de la fourniture du service, en particulier en lien avec la fourniture de prestations de support technique ou en raison du recours à des sous-traitants.

Il convient donc, dans ce contexte, de s'assurer de la mise en œuvre des SCC-UE/CH pour les transferts et accès de données entre l'entité contractante du fournisseur de services (comme exportateur) et les autres entités de son groupe ou ses sous-traitants (comme importateurs) situés dans un État considéré comme étant non adéquat du point de vue de la protection des données.

Les principaux fournisseurs de services *cloud* ont introduit les SCC-UE pour les transferts (ou accès) de données à destination de la société mère du groupe (située aux États-Unis) par différents biais. Alors que *Google* et *Microsoft* prévoient le recours au Module 3 (de sous-traitant à sous-traitant) entre l'entité contractante du fournisseur et sa société mère, *Amazon* et *Salesforce* ont, à notre connaissance, choisi l'utilisation du Module 2 (de responsable du traitement à sous-traitant) entre l'entité qui souscrit les services *cloud* et le bénéficiaire<sup>42</sup>. Cette dernière option ne fait donc pas usage du Module 3 des SCC-UE qui prévoit le cas spécifique du transfert de données à un sous-traitant du fournisseur de service, alors considéré comme un sous-sous-traitant du point de vue du responsable du traitement. Au contraire, elle continue l'implémentation historique (soit préalable aux nouvelles SCC-UE) dans laquelle le responsable du traitement conclut les SCC-UE directement avec le sous-sous-traitant bénéficiaire des données.

Par ailleurs, dans notre expérience, les fournisseurs de services *cloud* intègrent en principe également (i) les références au droit suisse de la protection des données dans les clauses et définitions de leur *Data Processing Addendum* et (ii) le *Swiss finish* aux SCC-UE, par le biais d'avenants en matière de protection spécifiques pour la Suisse (appelé également : *Swiss Addendum*).

---

<sup>42</sup> S'agissant de *Microsoft*, voir par exemple le *Data Protection Addendum*, disponible à l'adresse <[microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?year=2021](https://microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?year=2021)> (consulté le 3 juillet 2022).



## D. Impact de la nouvelle loi sur la protection des données

Sans changer fondamentalement le contenu des dispositions relatives à la communication transfrontière de données personnelles, la dernière modification de la LPD apporte quelques précisions.

Sur la forme, la nouvelle modification de la LPD sépare les différentes exceptions à l'interdiction de communiquer des données qui sont actuellement regroupées au sein de l'art. 6 al. 2 LPD. Ces exceptions seront disposées aux art. 16-17 nLPD à travers un système en cascade. Si la protection de données personnelles communiquées à l'étranger ne peut pas être garantie par la législation interne de l'État concerné (art. 16 al. 1 nLPD), d'autres mesures doivent être prises pour garantir un niveau de protection adéquat (art. 16 al. 2 nLPD). Enfin, quand ces autres mesures de protection ne sont pas envisageables, la communication doit respecter une des exceptions de l'art. 17 al. 1 nLPD afin d'être conforme à la nLPD. Bien que cette séparation ne change pas la portée matérielle de l'art. 6 LPD, cette séparation apportera une clarté bienvenue.

Par ailleurs, lors de la modification de la LPD, l'art. 5 OLPD (publication sous forme électronique) sera introduit directement dans la nLPD, devenant l'art. 18 nLPD. Cette modification aura l'avantage de regrouper, au sein d'une même section de la nLPD, les trois dispositions topiques en matière de communication de données personnelles à l'étranger.

Finalement, l'établissement de la liste des États assurant un niveau de protection adéquat, actuellement établie par le PFPDT, figurera dorénavant dans une ordonnance du Conseil fédéral<sup>43</sup>.

Sur le fond, la modification de la LPD n'introduira que quelques changements et précisions mineurs. L'on peut mentionner par exemple l'extension bienvenue du champ d'application de l'art. 6 al. 2 let. d LPD (communication indispensable à l'exercice ou à la défense d'un droit en justice) aux « autorités » au sens large<sup>44</sup>. La nouvelle disposition (art. 17 al. 1 let. d ch. 2 nLPD) prévoira que la communication est nécessaire pour la constatation, l'exercice ou la défense d'un droit devant un tribunal *ou une autre autorité étrangère compétente*<sup>45</sup>.

---

<sup>43</sup> FF 2017 6658.

<sup>44</sup> ROSENTHAL, N 76.

<sup>45</sup> La version actuelle de la LPD avait empêché la communication de données personnelles par des banques suisses à des autorités américaines car les autorités américaines récipiendaires ne disposaient pas d'un pouvoir « juridictionnel » exigé par l'article 6 al. 2 let. d LPD (sur ce point, Recommandations du 15 octobre 2012 à l'attention de cinq banques, par. II.11, disponible sous : <<https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/datenschutz/empfehlungen.html>>, consulté le 3 juillet 2022).

## V. Particularité des États-Unis

### A. Introduction

Le transfert de données personnelles vers les États-Unis a été et demeure l'objet de controverses juridiques. Cette question est pourtant centrale en matière d'utilisation de services *cloud* dans la mesure où la plupart des prestataires de services *cloud* sont américains ou liés aux États-Unis. Pour comprendre la situation juridique actuelle en Suisse, il convient de reprendre les différents événements qui ont émaillé ces dix dernières années au niveau suisse et européen (*infra* V.B.-E.). Cette analyse nous permettra d'aborder la question épineuse du transfert de données dans des États qui disposent de règles impératives qui permettent notamment un droit d'accès étendu des autorités nationales aux données personnelles détenues par des entités privées (*infra* V.F.). Finalement, nous nous intéresserons aux implications du *US CLOUD Act* (*infra* V.G.).

### B. Première épisode – *Safe Harbor*

#### 1. *Au niveau européen*

Le premier épisode de cette saga débute en 2000 lorsque la Commission européenne estime qu'un transfert de données vers certaines entreprises américaines est possible, l'État assurant un niveau de protection adéquat en raison des garanties qui découlent du *EU-US Safe Harbor* (Décision 2000/520)<sup>46</sup>.

Ces garanties ont été développées par les États-Unis en collaboration avec la Commission européenne et énuméraient les critères qui devaient être respectés en vue d'un transfert de données personnelles vers les États-Unis. Cette décision de la Commission européenne était fondée sur l'art. 25 de la Directive UE 95/46.

Avec cette décision, le transfert de données vers les entreprises américaines ayant adhéré au *EU-US Safe Harbor* était autorisé, le pays garantissant, moyennant le respect des conditions figurant dans le *EU-US Safe Harbor*, un niveau de protection adéquat.

---

<sup>46</sup> Décision 2000/520 CE du 26 juillet 2000 conformément à la directive 95/46/CE.

## 2. En Suisse

En 2008, la Suisse a conclu avec les États-Unis un accord comparable et au contenu très similaire, le *Swiss-US Safe Harbour*<sup>47</sup>. Cet accord découlait d'un échange de lettres entre la Suisse et les États-Unis concernant l'établissement d'un cadre de protection des données pour la transmission de données personnelles aux États-Unis<sup>48</sup>.

### C. Deuxième épisode – Schrems I

#### 1. Au niveau européen

Le deuxième épisode de la saga intervient cinq ans plus tard, en 2015, lorsqu'un ressortissant autrichien, Maximilian Schrems, se plaint que les données personnelles qu'il fournit à *Facebook* étaient transférées depuis la filiale irlandaise du Groupe *Facebook* (*Facebook Ireland*) vers des serveurs appartenant à *Facebook Inc.* situés aux États-Unis.

M. Schrems considère que les règles en matière de protection des données en vigueur aux États-Unis n'offraient pas une protection suffisante, nonobstant les termes du *EU-US Safe Harbor* auquel le Groupe *Facebook* avait adhéré. M. Schrems se réfère notamment aux révélations faites par M. Edward Snowden au sujet des activités de la *National Security Agency*.

Le 25 juin 2013, M. Schrems saisit le commissaire d'une plainte. Le commissaire rejette la plainte au motif que la Commission européenne avait considéré que les États-Unis offraient un niveau de protection adéquat dans le cadre de transferts de données personnelles vers des entreprises américaines ayant adhéré au *EU-US Safe Harbor*.

M. Schrems introduit alors un recours devant la Haute Cour de justice contre cette décision. La Haute Cour de justice sursoit à statuer et pose des questions préjudicielles à la Cour de justice de l'Union européenne. Saisie des questions préjudicielles, la Cour de justice de l'Union européenne, par jugement du 6 octobre 2015, invalide la Décision 2000/520 au motif que les engagements souscrits dans le cadre du *EU-US Safe Harbor* étaient insuffisants pour garantir que les États-Unis assurent effectivement un niveau de protection adéquat en

---

<sup>47</sup> PFPDT, 24<sup>e</sup> rapport d'activités 2015/2016, p. 51.

<sup>48</sup> RS 0.235.233.6.

matière de protection des données<sup>49</sup>. En particulier, les droits d'accès larges des autorités américaines portent atteinte au droit du respect de la vie privée.

Cette décision de la Cour de justice de l'Union européenne a eu un impact considérable, dans la mesure où elle retirait le fondement juridique de nombreux transferts de données personnelles de l'Union européenne vers les États-Unis<sup>50</sup>.

## 2. *En Suisse*

La Suisse n'est pas restée immobile face à ces développements jurisprudentiels. Dans un communiqué de presse du 22 octobre 2015, le PFPDT a considéré que le *Swiss-US Safe Harbour* ne garantissait pas un niveau de protection adéquat. Suite à cela, le Conseil fédéral a constaté que, même s'il n'a pas d'effet contraignant direct en Suisse, l'arrêt *Schrems I* revêt une importance considérable. En effet, la décision met en exergue des problèmes qui concernent aussi le cadre de protection des données mis en place pour la transmission de données personnelles de la Suisse vers les États-Unis<sup>51</sup>. En particulier, le *Swiss-US Safe Harbour* ne garantit pas un niveau de protection adéquat car il n'engage que les entreprises certifiées, mais pas les autorités publiques<sup>52</sup>.

Tout comme l'Union européenne, la Suisse a ainsi considéré qu'il n'y avait plus de protection adéquate contre des accès disproportionnés des autorités américaines à des données personnelles transmises de la Suisse vers les États-Unis<sup>53</sup>.

## D. Troisième épisode – *Privacy Shield*

### 1. *Au niveau européen*

Troisième épisode de la saga, le 6 février 2016, quelques mois seulement après la publication du jugement « *Schrems I* », la Commission européenne annonce avoir conclu un nouvel accord avec les États-Unis. Le *EU-US Safe Harbor* est remplacé par le *EU-US Privacy Shield*, un nouveau dispositif

---

<sup>49</sup> CJUE, affaire C-362/14 du 6 octobre 2015, *Data Protection Commissioner contre Maximilian Schrems*, ECLI:EU:C:2015:650. La décision a été résumée sous : FRANCEY, L'invalidation du Safe Harbor (arrêt Facebook), in <[www.lawinside.ch/92/](http://www.lawinside.ch/92/)> (consulté le 3 juillet 2022). Voir également : SIDLER/VASELLA.

<sup>50</sup> FISCHER, De la « sphère de sécurité » au « bouclier de protection », p. 145.

<sup>51</sup> Avis du Conseil fédéral du 18 novembre 2015, disponible : <<https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaefit?AffairId=20154001>> (consulté le 3 juillet 2022).

<sup>52</sup> PFPDT, 21<sup>e</sup> rapport d'activités 2013/2014, p. 51.

<sup>53</sup> PFPDT, 21<sup>e</sup> rapport d'activités 2013/2014, p. 51.

visant à tenir compte des critiques formulées par la Cour de justice de l'Union européenne à l'égard du *EU-US Safe Harbor*. Le 12 juillet 2016, la Commission européenne publie la décision d'adéquation qui formalise la reconnaissance du *EU-US Privacy Shield* comme un dispositif de protection adéquat<sup>54</sup>.

Chaque entreprise américaine qui souhaite adhérer au *EU-US Privacy Shield* doit demander son inscription sur la liste d'adhésion (publiquement disponible) et s'auto-certifier comme répondant aux normes en matière de protection des données prévues dans le dispositif. Plus de 2'400 entreprises américaines ont adhéré au *EU-US Privacy Shield*<sup>55</sup>.

## 2. *En Suisse*

Une fois encore, la Suisse réagit de manière similaire à l'Union européenne. Le Conseil fédéral charge le Secrétariat d'État à l'économie (SECO) de constituer un groupe de travail interdépartemental ayant pour mission de négocier un nouvel accord pour remplacer le *Swiss-US Safe Harbour*. Sur la base du *EU-US Privacy Shield*, la Suisse négocie avec les États-Unis un accord qui offrirait des garanties équivalentes<sup>56</sup>.

Lors de sa séance du 11 janvier 2017, le Conseil fédéral prend connaissance de l'établissement d'un nouveau cadre pour le transfert des données personnelles depuis la Suisse à des entreprises sises aux États-Unis, le « Bouclier de protection des données Suisse-États-Unis » ou *Swiss-US Privacy Shield*, la Suisse disposant alors des mêmes conditions que l'Union européenne<sup>57</sup>.

## E. Quatrième épisode – Schrems II

### 1. *Au niveau européen*

Dans le quatrième épisode de la saga, le même ressortissant autrichien, Maximilian Schrems, se plaint à nouveau du transfert de ses données personnelles par la filiale européenne de *Facebook* à une entité du même groupe aux États-Unis. Dans un contexte similaire à celui qui a donné lieu à l'arrêt de 2015, la Cour de Justice de l'Union européenne est invitée à analyser, sur

---

<sup>54</sup> Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016.

<sup>55</sup> FISCHER, De la « sphère de sécurité » au « bouclier de protection », p. 146 et référence citée.

<sup>56</sup> PFPDT, 24<sup>e</sup> rapport d'activités 2016/2017, p. 29.

<sup>57</sup> Communiqué du Conseil fédéral du 11 janvier 2017 : « Bouclier de protection des données Suisse-États-Unis » : meilleure protection pour les données transférées aux États-Unis.

question préjudicielle, (i) la décision d'adéquation de la Commission européenne autorisant les transferts de données personnelles vers les États-Unis dans le cadre du *EU-US Privacy Shield*<sup>58</sup> et (ii) la décision de la Commission européenne en vertu de laquelle les SCC-UE offrent des garanties suffisantes pour un transfert de données vers un pays tiers<sup>59</sup>.

Dans une décision du 16 juillet 2020 (appelée « *Schrems II* »)<sup>60</sup>, la Cour de Justice de l'Union européenne invalide le *EU-US Privacy Shield*, au motif que cet instrument n'offrait pas un niveau suffisant de protection des données personnelles, notamment compte tenu des mesures de surveillance à disposition des autorités américaines.

Cette décision a eu pour conséquence immédiate que les transferts de données personnelles entre les entreprises européennes et les entreprises américaines participant au *EU-US Privacy Shield* ne bénéficiaient plus d'une présomption de conformité au RGPD.

## 2. *En Suisse*

Toujours dans la continuité des développements européens et même si l'arrêt *Schrems II* ne déploie pas d'effet direct en Suisse, le PFPDT a rapidement indiqué que le *Swiss-US Privacy Shield* n'offrait plus un niveau de protection suffisant et ne constituait donc plus un instrument autorisant le transfert des données vers les États-Unis<sup>61</sup>.

Même si aucune jurisprudence suisse publiée comparable à l'arrêt *Schrems II* n'existe actuellement, le PFPDT a estimé que les tribunaux suisses, en se fondant sur l'art. 6 LPD, devraient arriver aux mêmes conclusions concernant l'accès aux données par les autorités américaines que la Cour de Justice de l'Union européenne<sup>62</sup>.

---

<sup>58</sup> Sur ce point, *infra* V.D.

<sup>59</sup> Sur ce point, *infra* IV.C.2.

<sup>60</sup> CJUE, affaire C-311/18 du 16 juillet 2020, *Data Protection Commissioner contre Facebook Ireland Ltd et Maximilian Schrems*, ECLI:EU:C:2020:559. La décision est résumée dans : JACOT-GUILLARMOD, *Schrems II : Invalidation du Privacy Shield* (CJUE) (1/2), in <[www.lawinside.ch/945/](http://www.lawinside.ch/945/)> (consulté le 3 juillet 2022).

<sup>61</sup> Communiqué du PFPDT du 8 septembre 2020.

<sup>62</sup> Prise de position du PFPDT du 8 août 2020.

## F. Et maintenant ?

### 1. Au niveau européen

#### a) En général

Dans le deuxième volet de sa décision du 16 juillet 2020 (*Schrems II*)<sup>63</sup>, la Cour de Justice de l'Union européenne a indiqué que des clauses standards contractuelles pouvaient constituer une garantie suffisante pour permettre une communication vers un État n'assurant pas un niveau de protection adéquat (art. 46 par. 2 let. c RGPD), pour autant que l'exportateur des données (i) effectue une analyse de risques au préalable et (ii) s'assure que les SCC-UE permettent effectivement une protection adéquate des données transférées. Dès lors, si une telle analyse révèle que les SCC-UE ne sont pas suffisantes pour assurer un niveau de protection adéquat dans le pays de destination, l'exportateur devra (iii) mettre en œuvre des mesures de protection supplémentaires<sup>64</sup>.

Par conséquent, un niveau de protection équivalent à la réglementation européenne au sens de l'art. 46 par. 2 let. c RGPD n'est plus automatiquement garanti lorsque le transfert de données personnelles hors de l'Union européenne repose uniquement sur les SCC-UE. En effet, ces clauses ne sont que de nature contractuelle et ne peuvent, partant, faire obstacle à des mesures prises par les autorités de l'État destinataire. La nouvelle version des SCC-UE, qui a été publiée dans l'intervalle<sup>65</sup>, ne change rien à cette faiblesse inhérente à un système basé sur des engagements contractuels.

Ainsi, les exportateurs de données doivent au préalable de tout transfert procéder à une évaluation des risques au cas par cas (*transfer impact assessment*) et, au besoin, accompagner les SCC-UE de mesures de protection supplémentaires.

---

<sup>63</sup> CJUE, affaire C-311/18 du 16 juillet 2020, *Data Protection Commissioner contre Facebook Ireland Ltd et Maximilian Schrems*, ECLI:EU:C:2020:559. La décision est résumée dans : JACOT-GUILLARMOD, *Schrems II : Invalidation du Privacy Shield* (CJUE) (1/2), in <[www.lawinside.ch/945/](http://www.lawinside.ch/945/)> (consulté le 3 juillet 2022).

<sup>64</sup> Pour une analyse détaillée : FISCHER/LUBISHTANI.

<sup>65</sup> Sur ce point, cf. *supra* IV.B.2.

## b) Recommandations du CEPD

Suite à la décision *Schrems II*, le Comité européen de la protection des données (le « CEPD ») a publié des recommandations<sup>66</sup> destinées à faciliter, dans la mesure du possible, la mise en œuvre des exigences formulées par la Cour de Justice de l'Union européenne dans l'arrêt *Schrems II*. De deux ordres, ces recommandations portent, d'une part, sur l'évaluation du niveau de protection de l'État destinataire et des risques (*infra* V.F.1.b)aa) et, d'autre part, sur l'identification des mesures supplémentaires envisageables en vue de pallier l'insuffisance des SCC-UE (*infra* V.F.1.b)bb)).

### aa) Procédure d'évaluation du niveau de protection au sein de l'État destinataire

Pour procéder à l'évaluation du niveau de protection au sein de l'État destinataire, le CEPD propose une feuille de route (*roadmap*) composée de six étapes.

1. Premièrement, tout exportateur doit connaître et identifier quelles sont les données transférées (*know your transfers*) et, à cet égard, le registre des activités de traitement (art. 30 RGPD) constitue un outil essentiel ;
2. Ensuite, il est nécessaire d'identifier le fondement juridique sur lequel repose le transfert et de distinguer selon qu'il s'agit (i) d'une décision d'adéquation (art. 45 RGPD) ou (ii) de garanties appropriées au sens de l'art. 46 RGPD, parmi lesquelles figurent les SCC-UE, mais aussi les règles d'entreprise contraignantes, les clauses *ad hoc* ou encore les codes de conduite. Dans la première hypothèse, l'examen s'arrête tant et aussi longtemps que la décision d'adéquation est en force, alors qu'il se poursuit dans la seconde ;
3. Dans un troisième temps, le droit de l'État de destination doit être examiné, afin de déterminer si les garanties précitées sont *in concreto* appropriées et suffisantes, en ce qu'elles assurent bel et bien un niveau de protection adéquat. Pour ce faire, le CEPD renvoie aux Garanties essentielles européennes (EDPB – *European Essential Guarantees Recommendations*), en indiquant que l'examen doit être conduit avec soin (*carefully examined*) lorsque le droit en question permettant l'accès aux données par des autorités de poursuite ou de sécurité nationale est ambigu ou n'est pas public. Si la législation est lacunaire, l'examen doit reposer sur des critères

---

<sup>66</sup> *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, du 10 novembre 2020 ; pour une analyse détaillée : FISCHER/LUBISHTANI.



- objectifs et non subjectifs, à l'instar de la vraisemblance d'un accès aux données ne s'alignant pas sur les standards européens ;
4. Si l'évaluation qui précède révèle une insuffisance en termes de protection découlant soit du droit de l'État de destination, soit de sa pratique interne, qui empêcherait l'importateur de remplir ses obligations en vertu des SCC-UE, des mesures supplémentaires doivent être prises qui, par définition, vont au-delà des garanties envisagées par l'art. 46 RGPD ;
  5. Lorsque les mesures supplémentaires consistent en une modification (et non seulement un complément) des SCC-UE ou y contreviennent, alors le transfert est réputé ne plus reposer sur des SCC-UE au sens de l'art. 46 RGPD (*cf.* CEPD, Avis 17/20), si bien que l'autorisation de l'autorité de contrôle compétente (art. 46 par. 3 RGPD) est nécessaire ; et
  6. Enfin, il sied de réévaluer de manière régulière les développements législatifs, réglementaires et jurisprudentiels au sein de l'État de destination qui pourraient impacter la procédure d'évaluation.

bb) Mesures supplémentaires

Les mesures supplémentaires peuvent se diviser en trois catégories : (aaa) les mesures techniques, (bbb) les mesures contractuelles et (ccc) les mesures organisationnelles.

aaa) Les mesures techniques

Les mesures techniques évoquées par le CEPD sont (i) le cryptage et (ii) la pseudonymisation, pour autant que ces mesures puissent garantir que l'importateur des données, situé par hypothèse dans un État réputé non adéquat, ne dispose pas d'un accès aux données en clair<sup>67</sup>. Dans une perspective pratique, seules ces mesures techniques apparaissent, à l'heure actuelle, capables d'empêcher effectivement l'accès des autorités publiques du pays de l'importateur aux données personnelles transférées.

Toutefois, si l'importateur a besoin d'un accès aux données en « clair » pour rendre le service, les mesures techniques précitées ne pourront pas être mises en place et seules des mesures (ii) contractuelles et (iii) organisationnelles pourront être envisagées.

---

<sup>67</sup> *Cf. supra* II.B.2.

bbb) Mesures contractuelles

Le CEPD évoque également la possibilité de recourir à des mesures contractuelles, étant précisé toutefois que de telles mesures pourraient être mises en échec par le droit local applicable au récipiendaire, ce qui est précisément le point critiqué dans le cadre de la décision *Schrems II*. Ces mesures contractuelles peuvent notamment consister en :

- L’obligation, à charge de l’importateur, d’informer l’exportateur sur le cadre légal applicable à l’importateur, notamment s’agissant des mesures d’enquête des autorités, cette information permettant à l’exportateur de mener à bien l’analyse de risque exigée par la décision *Schrems II* (cf. *supra* V.E) ;
- Une garantie de l’importateur que la solution d’hébergement de données ne contient pas de *back doors* ;
- Des droits d’audit étendus en faveur de l’exportateur, de manière à permettre à ce dernier de s’assurer de l’absence de *back doors* et de cas de divulgation à des autorités ;
- Une obligation, à charge de l’importateur, de confirmer à intervalles réguliers l’absence de requête d’accès d’une autorité (la non-transmission d’une telle confirmation signalant ainsi à l’exportateur qu’une telle requête a été reçue<sup>68</sup>) ;
- Une obligation, à charge de l’importateur, de prendre toute mesure utile pour protéger les données, par exemple l’obligation de requérir des mesures provisionnelles pour suspendre un ordre de divulgation, de contester cet ordre en justice et de limiter toute divulgation au strict minimum requis (une telle clause est généralement appelée *defend your data clause*).

ccc) Mesures organisationnelles

Les mesures organisationnelles comprennent les politiques et processus de l’exportateur, dont l’importateur pourrait garantir le respect, de manière à assurer la protection des données durant tout le cycle de traitement des données.

Ces mesures organisationnelles peuvent notamment porter sur la mise en œuvre d’une structure de gouvernance relative aux transferts transfrontaliers de données, sur la documentation des requêtes d’accès émanant d’autorités étrangères et sur la fixation de principes en matière de minimisation de données.

---

<sup>68</sup> Un tel système est désigné par l’appellation *warrant canary* en référence aux mineurs qui apportaient des canaris dans les mines de charbon pour déceler des gaz toxiques.

cc) Résumé

En résumé, l'on retiendra que ces recommandations reflètent les attentes très élevées du CEPD s'agissant des mesures à prendre suite à l'arrêt *Schrems II*. Les mesures contractuelles proposées dans les recommandations constituent une palette intéressante de clauses qui pourraient, à l'avenir, faciliter les négociations avec les prestataires de services par l'émergence d'un certain « standard minimal » concernant les engagements contractuels étant toutefois précisé que des mesures de protection fondées exclusivement sur des engagements contractuels ne sont probablement pas suffisantes au regard des exigences formulées par la Cour de Justice de l'Union européenne dans l'arrêt *Schrems II*.

c) **Nouvel accord de principe EU-US**

Le 25 mars 2022, la Commission européenne et les États-Unis ont annoncé qu'ils avaient convenu d'un accord de principe sur un nouveau cadre transatlantique de protection des données personnelles, qui vise à favoriser les flux de données transatlantiques et à répondre aux préoccupations exprimées par la Cour de justice de l'Union européenne dans l'arrêt *Schrems II* de juillet 2020<sup>69</sup>.

Cet accord reste pour le moment une simple déclaration d'intention de vouloir mettre en œuvre des mesures visant à permettre une communication de données. Des mesures de sécurité concrètes devront encore être négociées et mises en œuvre dans le cadre réglementaire américain.

Le 6 avril 2022, le CEPD a d'ailleurs pris position sur cet accord en précisant qu'il examinera comment cet accord politique se traduit en propositions juridiques concrètes pour répondre aux préoccupations soulevées par la Cour de justice de l'Union européenne dans l'arrêt *Schrems II*<sup>70</sup>. Dans sa prise de position, le CEPD a précisé qu'à ce stade cette annonce ne constituait pas un cadre juridique sur lequel les exportateurs de données pouvaient se baser pour transférer leurs données vers les États-Unis. Les exportateurs de données

---

<sup>69</sup> Déclaration conjointe de la Commission européenne et des États-Unis sur le cadre transatlantique de protection des données personnelles du 25 mars 2022, disponible à l'adresse : [https://ec.europa.eu/commission/presscorner/detail/fr/ip\\_22\\_2087](https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_2087) (consulté le 3 juillet 2022).

<sup>70</sup> Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework du 6 avril 2022 de la CEPD, disponible à l'adresse : [https://edpb.europa.eu/system/files/2022-04/edpb\\_statement\\_202201\\_new\\_transatlantic\\_data\\_privacy\\_framework\\_en.pdf](https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_transatlantic_data_privacy_framework_en.pdf) (consulté le 3 juillet 2022).

doivent donc continuer à prendre les mesures évoquées par la Cour de justice de l'Union européenne dans l'arrêt *Schrems II*.

## 2. *En Suisse*

### a) **Guide du PFPDT**

Comme déjà évoqué précédemment, le PFPDT a également reconnu les nouvelles SCC-UE, tout en attirant l'attention sur les limites mises en évidence dans le cadre de l'arrêt *Schrems II*<sup>71</sup>.

Dans un guide publié en juin 2021, le PFPDT présente une marche à suivre que le responsable du traitement soumis à la LPD peut utiliser lorsqu'il communique des données personnelles à l'étranger<sup>72</sup>. Lorsqu'une communication est effectuée dans un État ne garantissant pas un niveau de protection adéquat, le responsable du traitement doit assurer la sécurité des données avec d'autres mesures de protection.

Le responsable du traitement doit en particulier vérifier si les autorités du pays tiers concerné peuvent avoir accès aux données communiquées et si ces accès sont compatibles avec le droit suisse de la protection des données. En particulier, les garanties suivantes doivent être ancrées dans la réglementation de l'État récipiendaire.

- Principe de légalité : il doit exister une base juridique suffisamment spécifique et claire concernant les buts, la procédure d'accès aux données par les autorités, les conditions juridiques matérielles de cet accès et les prérogatives des autorités en question.
- Proportionnalité : les prérogatives des autorités et les mesures qu'elles prennent doivent être appropriées et nécessaires pour atteindre les buts légaux de l'accès des autorités aux données.
- Voies de droits : les personnes concernées doivent disposer de voies de droit effectives, inscrites dans la loi, pour faire valoir leurs droits en matière de protection de la sphère privée et d'autodétermination informationnelle (par ex. droit d'accès, droit de rectification et droit de suppression).
- Garantie de l'accès au juge : les atteintes à la vie privée et l'autodétermination informationnelle doivent faire l'objet d'un contrôle efficace, indépendant et impartial (tribunal ou autre organe indépendant, par ex. une autorité administrative ou un organe parlementaire). Il faut pouvoir vérifier

---

<sup>71</sup> Guide du PFPDT, N 3.

<sup>72</sup> Guide du PFPDT, N 5 ss.

l'approbation (judiciaire) préalable de mesures de surveillance (protection contre l'arbitraire) et le fonctionnement effectif du système de surveillance.

Si les quatre garanties ci-dessus sont assurées, un niveau de protection adéquat peut être atteint au moyen de l'intégration des SCC-UE/CH dans le rapport contractuel avec le récipiendaire des données<sup>73</sup>.

Si les quatre garanties ne peuvent pas être assurées, le responsable du traitement doit prendre des mesures supplémentaires.

- Mesures contractuelles : le PFPDT rappelle que des mesures contractuelles supplémentaires (concernant à la fois l'exportateur de données et l'importateur de données) ne sont généralement pas suffisantes à elles-seules car elles ne peuvent pas lier les autorités de pays tiers et ne peuvent donc pas empêcher l'accès des autorités aux données personnelles communiquées.
- Mesures techniques et organisationnelles : des mesures techniques ou organisationnelles supplémentaires doivent être mises en œuvre. Ces mesures doivent être conçues de telle sorte que les autorités de l'État tiers ne puissent pas, dans les faits, accéder aux données personnelles transférées. Le PFPDT précise que dans le cas d'un stockage de données par un prestataire *cloud*, il serait envisageable d'effectuer par exemple un chiffrement des données personnelles qui serait mis en œuvre selon le principe BYOK (« *Bring Your Own Key* »), doublé du principe BYOE (« *Bring Your Own Encryption* »), de sorte qu'aucune donnée en clair ne soit disponible dans le *cloud* en question et qu'aucun chiffrement et qu'aucun déchiffrement n'y soient opérés.
- Enfin, s'il est impossible de compenser l'absence d'une ou plusieurs garanties à l'aide de mesures contractuelles, techniques ou organisationnelles, la communication des données devrait être suspendue.

Il ressort de ce guide que les mesures de protection doivent réduire à zéro le risque d'accès aux données personnelles par une autorité étrangère, faute de quoi le transfert est jugé incompatible avec la LPD. En cas de persistance d'un risque après l'analyse, aucune donnée personnelle ne peut ainsi être communiquée dans l'État ne garantissant pas un niveau de protection adéquat. Comme discuté ci-dessous, nous sommes d'avis que les autorités de protection des données devraient mettre en œuvre une approche plus nuancée fondée sur une réduction, mais non une suspension totale, du risque d'accès aux données personnelles par les autorités de l'État récipiendaire<sup>74</sup>.

---

<sup>73</sup> Dans une perspective pratique, l'on constate que les États qui remplissent ces quatre conditions figurent d'ores et déjà sur la liste du PFPDT des États réputés adéquat dans une perspective de protection des données, de sorte que le recours aux SCC-UE/CH est inutile, du moins s'agissant de données personnelles de personnes physiques.

<sup>74</sup> *Infra* V.F.2.b) et V.G.3.

Dans ce contexte, la « sensibilité » des données et les assurances données aux personnes concernées lors de la collecte devraient également être intégrées dans l'analyse.

## **b) Communication fondée sur une analyse de risque**

La légalité d'un transfert de données personnelles vers un État tiers réputé « non adéquat » dépend des circonstances factuelles de ce transfert et donc d'une analyse au cas par cas impliquant (i) l'examen approfondi du droit, et même de la pratique, du pays de destination (ex : ingérence des autorités de surveillance, droits des personnes concernées et possibilité de mise en œuvre effective de ceux-ci), (ii) l'identification précise du besoin d'accès du fournisseur aux données transférées pour rendre le service (accès aux données en clair nécessaire ou non) et sur cette base, (iii) la mise en place des mesures de sécurité appropriées (ex : anonymisation, pseudonymisation, chiffrement) et (iv) la conclusion des garanties contractuelles nécessaires avec le fournisseur de services (ex : engagement du fournisseur de s'opposer, dans les limites du droit applicable, à toute demande d'accès des autorités ; obligation d'information du responsable du traitement avant tout transfert de données à des autorités ; obligation préalable d'information par le fournisseur lorsque son droit national ne lui permet pas de remplir ses obligations en vertu du contrat ou des SCC-UE/CH).

Il n'y a donc pas de solution *one size fits all* et le recours aux SCC-UE/CH en matière de protection des données, qui étaient jusqu'à l'arrêt *Schrems II* largement utilisées en pratique sans analyse particulièrement approfondie du système juridique de l'État de destination, devra être complété par des garanties supplémentaires, techniques, contractuelles et/ou organisationnelles, en fonction du risque qu'il convient de couvrir. Le responsable du traitement pourra même être amené à conclure à l'impossibilité de contracter avec un fournisseur ou à la nécessité de mettre un terme au transfert de données personnelles vers certaines juridictions afin d'assurer la conformité avec les exigences de la LPD.

S'agissant plus particulièrement du recours à des prestataires de services *cloud*, il conviendra d'effectuer une analyse des risques de l'application du projet en considérant (i) les risques d'un accès illicite aux données et (ii) les risques d'un accès « licite » aux données.

Le risque d'un accès illicite aux données constitue le risque qu'un tiers accède de manière illicite aux données stockées dans le *cloud*. Plusieurs situations pourraient conduire à cette situation, la plus probable étant le piratage. Ce risque doit être qualifié selon nous de relativement faible. En effet, les principaux prestataires de services *cloud* sur le marché disposent de protections

très importantes contre les piratages<sup>75</sup>. Sur ce point, le recours à un prestataire de services *cloud* pourrait même réduire le risque de piratage par rapport à une internalisation du système informatique, surtout pour les petites structures. Par conséquent, le risque d'un accès illicite aux données est probablement plus faible en cas de recours à un prestataire de services *cloud* reconnu.

Le deuxième risque est celui d'un accès « licite » aux données. Il faut entendre par cela un accès « licite », par des autorités étrangères, sous l'angle du droit étranger (comme c'est le cas, par exemple, aux États-Unis). Bien que cet accès puisse être illicite d'un point de vue du droit suisse, il reste licite pour les autorités étrangères. Afin de calculer et de pouvoir appréhender ce risque, il convient de mener, selon nous, une analyse de risque qui doit en particulier prendre en compte les trois aspects suivants :

- la probabilité qu'une autorité étrangère dispose d'un droit d'accès légal sur les données et souhaite le faire valoir auprès du fournisseur ;
- la probabilité qu'une autorité étrangère réussisse effectivement à faire valoir son droit d'accès aux données par l'intermédiaire du fournisseur ;
- la probabilité qu'une autorité étrangère dispose d'un droit d'accès légal sur les données par le biais d'un système de surveillance de masse.

## **G. Excursus : le *US CLOUD Act***

Le droit d'accès étendu des autorités américaines à des données personnelles stockées aux États-Unis, mais surtout dans des entreprises dont la société mère est basée aux États-Unis trouve sa source dans le *Clarifying Lawful Overseas Use of Data Act* (le « *US CLOUD Act* »)<sup>76</sup>. Il convient ainsi à titre liminaire de distinguer (i) le transfert de données aux États-Unis et (ii) le transfert à des entités européennes (ou d'autres États assurant un niveau de protection adéquat) qui sont soumis au *US CLOUD Act*. En effet, le risque d'un accès aux données sera, à notre sens, nettement plus important dans la première hypothèse.

Le *US CLOUD Act* est une loi fédérale américaine adoptée suite à une procédure judiciaire qui opposait les autorités américaines au Groupe *Microsoft*<sup>77</sup>.

---

<sup>75</sup> Sans prendre en considération le risque que le piratage se fasse, non pas au niveau du prestataire de services *cloud* mais au niveau du responsable du traitement (par exemple car ce dernier dispose d'un mot de passe très simple).

<sup>76</sup> *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, H.R. 1625, 115<sup>th</sup> Cong. div. V (2018) (enacted) (to be codified in scattered sections of 18 U.S.C.), disponible à l'adresse : <https://www.congress.gov/bill/115th-congress/senate-bill/2383/text> (consulté le 3 juillet 2022).

<sup>77</sup> U.S. Supreme Court, *United States v. Microsoft Corp.*, 584 U.S., 138 S. Ct. 1186 (2018).

Les autorités américaines avaient exigé de *Microsoft Corp. (US)* la communication de courriels sauvegardés sur des serveurs hébergés par une société affiliée à *Microsoft* en Irlande. *Microsoft* avait refusé au motif que les informations demandées n'étaient pas conservées sur sol américain et échappaient donc à la compétence des autorités américaines. La juridiction d'appel a confirmé l'argumentation de *Microsoft*<sup>78</sup>. Avant que la Cour Suprême des États-Unis n'ait eu l'occasion de se prononcer sur cette question, le Congrès américain a adopté le *US CLOUD Act* qui confère expressément aux autorités américaines un droit d'accès sur des données hébergées à l'étranger. Le *US CLOUD Act* complète le *Stored Communications Act* (le « *SCA* ») en vigueur depuis 1986.

Sur le plan des concepts, le *US CLOUD Act* est subdivisé en deux parties, l'une ayant trait aux obligations des entreprises concernées et l'autre prévoyant la possibilité de conclure des *executive agreements* entre les États-Unis et des pays tiers<sup>79</sup>.

## 1. *US CLOUD Act* – Partie 1

La première partie du *US CLOUD Act* oblige certains prestataires de services informatiques qui disposent d'un lien avec les États-Unis à transmettre des données aux autorités américaines (indépendamment du lieu d'hébergement de ces données), pour autant que la procédure dans le cadre de laquelle ces données sont requises soit liée à des crimes graves (*serious crimes*). Dans ce contexte, plusieurs points méritent d'être précisés.

- Le *US CLOUD Act* s'adresse aux fournisseurs (i) de services électroniques de communication (*electronic communication service providers*) et (ii) de services informatiques à distance (*remote computing service providers*). D'une part, un fournisseur offre un *service électronique de communication* lorsqu'il donne la possibilité à ses utilisateurs d'envoyer ou de recevoir des communications électroniques. D'autre part, un fournisseur offre un *service informatique à distance* lorsqu'il propose des services de stockage ou de traitement informatique au moyen d'un système électronique de communication. Le champ d'application à raison de la matière du *US CLOUD Act* est donc large et inclut en particulier les prestataires de services *cloud*.
- Le *US CLOUD Act* concerne les prestataires *soumis à la juridiction américaine*, à savoir principalement les entreprises incorporées aux États-Unis (pour toutes les données que ces entreprises sont réputées « contrôler »),

---

<sup>78</sup> 2<sup>nd</sup> Circuit Court, *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016).

<sup>79</sup> Pour une analyse complète voir par exemple : SCHWARZ ; FISCHER/PITTET ; LUTZ/EGLI ; BRAUNECK.



mais potentiellement également des entreprises *non américaines* qui disposent d'une société affiliée ou d'un autre type de présence stable sur sol américain. Il appartient aux autorités américaines de déterminer au cas par cas si une entreprise étrangère située en dehors des États-Unis est soumise à la juridiction américaine en raison de ses activités<sup>80</sup>.

- Le *US CLOUD Act* concerne les données « *en possession, sous la garde ou sous le contrôle* » du prestataire soumis à la juridiction américaine, indépendamment de la localisation effective de ces données :

« *A provider of electronic communication service or **remote computing service shall** comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber **within such provider's possession, custody, or control**, regardless of whether such communication, record, or other information is located within or outside of the United States.* »<sup>81</sup>

## 2. *US CLOUD Act – Partie 2*

La deuxième partie du *US CLOUD Act* traite de la possibilité pour les États-Unis de conclure avec d'autres États un *executive agreement*, qui peut notamment régir les points suivants.

- Les États-Unis pourraient requérir directement (*i.e.*, hors entraide) des données auprès d'un prestataire ayant son siège dans l'État contractant (même si ce prestataire n'a pas de lien particulier avec les États-Unis).
- À l'inverse, l'État contractant pourrait requérir directement (*i.e.*, hors entraide) des données détenues par un prestataire de service *cloud* ayant son siège aux États-Unis, pour autant que ces informations ne concernent pas une *US Person* (en résumé : une personne résidente aux États-Unis ou de nationalité américaine).
- Le prestataire requis de fournir les données disposerait de la possibilité de contester, devant un tribunal américain, la demande des autorités américaines, pour autant que la personne concernée ne soit pas une *US Person*. Dans un tel cas, le tribunal américain procédera à une pesée des intérêts, en prenant en compte notamment (i) les intérêts des États-Unis, et particulièrement ceux de l'autorité qui souhaite obtenir les informations, (ii) les

---

<sup>80</sup> Sur ce point, voir notamment : le *White Paper* du *Department of Justice* d'avril 2019 : « Promoting Public Safety, Privacy, and the Rule of Law Around the World : The Purpose and Impact of the CLOUD Act », p. 6 ss ; voir également : Rapport de l'Office fédéral de la justice sur le *US CLOUD Act* (loi *Cloud*) justice du 17 septembre 2021, p. 7.

<sup>81</sup> Section 2713 (a) (1) du *US CLOUD Act*, mise en évidence ajoutée.

relations entre la personne visée et les États-Unis (iii) la probabilité d'une sanction (dans l'État du prestataire requis) ainsi que sa sévérité, (iv) la probabilité d'accéder aux données par d'autres canaux (e.g. l'entraide internationale) et (v) l'importance des données concernées pour l'enquête.

À l'heure actuelle, le seul *executive agreement* en vigueur a été conclu entre les États-Unis et le Royaume-Uni le 3 octobre 2021. En revanche, il n'existe, en l'état, pas d'*executive agreement* entre les États-Unis et la Suisse. Un récent rapport de l'Office fédéral de la justice (daté du 17 septembre 2021) ne plaide pas en faveur de la conclusion d'un tel accord<sup>82</sup>.

### 3. *Vers une impossibilité complète de recourir à des prestataires de services informatiques qui disposent d'un lien avec les États-Unis ?*

#### a) **Cas *Health Data Hub* en droit européen**

Une ordonnance<sup>83</sup> du 13 octobre 2020 du Conseil d'État français relative au *Health Data Hub* offre certaines pistes de réflexion préliminaires sur la question de la possibilité de recourir à des prestataires de services *cloud* ayant un lien avec les États-Unis et donc soumis au *US CLOUD Act*<sup>84</sup>.

Dans le prolongement de l'arrêt *Schrems II*, plusieurs associations et collectifs dans le domaine de la santé ont saisi le juge des référés du Conseil d'État français (la plus haute juridiction administrative française) en demandant la suspension du traitement de données personnelles liées à la santé dans le cadre de la lutte contre l'épidémie de COVID-19 sur une plateforme de données de santé (« *Health Data Hub* »). Le *Health Data Hub* est géré par un groupement d'intérêt public institué par le code français de la santé publique et est hébergé par la filiale irlandaise de *Microsoft Corporation* (« *Microsoft Ireland* »).

Les demandeurs invoquaient à l'appui de leur requête qu'un tel traitement constituerait une atteinte grave aux droits des personnes concernées eu égard au possible accès aux données par les autorités américaines dans le cadre de mesures de surveillance dont peuvent faire l'objet les sociétés européennes qui font partie d'un groupe américain, en vertu du champ d'application extraterritorial du *US CLOUD Act*.

---

<sup>82</sup> Rapport de l'Office fédéral de la justice sur le *US CLOUD Act* (loi *Cloud*) justice du 17 septembre 2021.

<sup>83</sup> Conseil d'État, ordonnance n° 444937 du 13 octobre 2020.

<sup>84</sup> Pour une analyse complète, voir LARGANT/FISCHER.

Ce *Health Data Hub* contient notamment des données déclaratives de symptômes issues de l'application mobile française *StopCovid* et des résultats d'examens effectués par des laboratoires, toutes les données hébergées et traitées dans le *Health Data Hub* étant pseudonymisées<sup>85</sup>.

La CNIL (Commission Nationale de l'Informatique et des Libertés), appelée à déposer des observations dans le cadre de la procédure de référé, estime qu'il n'est pas possible d'écarter complètement le risque (i) d'une telle demande d'accès des autorités américaines et (ii) d'un accès par *Microsoft Ireland* aux données sous-jacentes « en clair » (*clear text*) traitées dans le *Health Data Hub* en dépit du chiffrement et du stockage des clés de chiffrement.

Néanmoins, le Conseil d'État relève que (i) l'arrêt *Schrems II* analyse les conditions d'un transfert de données personnelles de l'Union européenne vers les États-Unis et non leur traitement par une société de droit américain ou sa filiale sur le territoire de l'Union européenne, (ii) les demandeurs ne font pas valoir une violation effective du RGPD, mais un risque éventuel de violation si *Microsoft Ireland* ne pouvait pas s'opposer à une demande d'accès des autorités américaines et (iii) il existe un intérêt public important au traitement de données relatives à la santé dans le cadre de la lutte contre la pandémie de COVID-19 et les moyens techniques proposés par *Microsoft Ireland* en lien avec le *Health Data Hub* sont sans équivalent à ce jour.

Sur la base de ce qui précède, le Conseil d'État retient que le traitement de données personnelles liées à la santé dans le *Health Data Hub* ne constitue pas une atteinte grave et manifestement illicite qui nécessiterait la mise en place (par l'autorité) de mesures d'urgence visant à éliminer tout risque, tout en étant proportionnées à l'intérêt public visé par le traitement.

Bien que la portée de cette ordonnance du Conseil d'État puisse être limitée au contexte dans lequel elle est rendue – soit (i) les données étaient pseudonymisées et chiffrées, (ii) un intérêt de santé publique important entrainait en jeu et (iii) l'affaire était soumise à une procédure de référé qui, en droit français, vise des requêtes urgentes justifiées par une violation particulièrement grave d'une liberté fondamentale – il est tout de même important de noter que la plus haute juridiction administrative française considère que le risque d'un accès par les autorités américaines à des données personnelles traitées dans l'Union européenne par une entité soumise à l'application extraterritoriale du *US CLOUD Act* constitue un risque hypothétique, ou à tout le moins ne constitue pas une atteinte grave et manifestement illégale aux droits des personnes concernées. Le Conseil d'État considère en particulier que l'arrêt *Schrems II* ne traite pas

---

<sup>85</sup> Dans l'Union européenne, des données pseudonymisées peuvent être considérées comme des données personnelles sous l'angle du RGPD, contrairement à ce qui semble prévaloir en Suisse sous l'angle de la LPD (*supra* II.B.2).

de l'impact de la législation américaine régissant l'accès à des données par les autorités de surveillance américaines sur les données traitées dans l'Union européenne par les entités européennes de groupes américains.

## b) Décision du Conseil d'État du canton de Zurich

Dans une décision du 30 mars 2022<sup>86</sup>, le Conseil d'État du canton de Zurich s'est positionné sur le recours par son administration aux services *M365 cloud* de *Microsoft* (en particulier les services *Exchange Online* et *Teams*). Quand bien même les serveurs qui stockent les données concernées se situent dans l'Union européenne, un accès indirect aux données pas les autorités américaines en raison du *US CLOUD Act* ne peut pas être écarté.

Selon le Conseil d'État zurichois, il n'est aujourd'hui plus envisageable de recourir exclusivement à des services *on-site* (donc non situés sur un *cloud*). En effet, pour ne pas se retrouver « hors-jeu » (selon les termes utilisés par l'autorité zurichoise) au niveau technologique, un recours à des services de type *cloud* est indispensable<sup>87</sup>.

Dans cette décision, le Conseil d'État zurichois a effectué une pondération des risques pour déterminer s'il était adéquat de recourir à des prestations de type *cloud*. Le Conseil d'État a estimé que, en l'espèce, le risque que des autorités étrangères accèdent aux données personnelles stockées sur des serveurs *cloud* de *Microsoft* situés dans l'Union européenne était très faible<sup>88</sup> et que l'administration cantonale pouvait dès lors recourir à des services *M365* de *Microsoft*, pour autant que certaines mesures additionnelles de protection soient prises afin de limiter ce risque<sup>89</sup>.

Cette prise de position (qui a été précédée de consultations avec le Préposé cantonal à la protection des données et les autorités de poursuite pénale) constitue un précédent intéressant. Cela étant dit, il convient d'analyser la situation au cas par cas ; notamment en fonction de la sensibilité des données concernées et de l'intérêt des autorités étrangères à vouloir accéder aux données concernées par le biais du mécanisme prévu par le *US CLOUD Act*.

---

<sup>86</sup> Décision du 30 mars 2022 du Conseil d'État du canton de Zurich. « 542. Einsatz von Cloud-Lösungen in der kantonalen Verwaltung (Microsoft 365), Zulassung ».

<sup>87</sup> Sans le recours au *cloud*, le canton serait hors-jeu technologique (« *ins technologische Abseits* »), car il se fermerait au progrès technologique (« *dem technologischen Fortschritt verschliessen [würde]* »).

<sup>88</sup> Selon les informations fournies par *Microsoft* au Conseil d'État zurichois, il n'y a encore jamais eu, dans le secteur public, de divulgation de données stockées dans l'Union européenne par *Microsoft* aux autorités américaines.

<sup>89</sup> Mesures de protection contractuelles, techniques et organisationnelles ; sur ce point, voir également : VASELLA, Regierungsrat Zürich.

À titre d'exemple, dans le domaine bancaire, les autorités étrangères pourraient avoir une volonté plus importante d'accéder à des données clients que dans d'autres domaines. Néanmoins, contrairement à la position stricte du PFPDT<sup>90</sup>, le Conseil d'État du canton de Zurich estime que le recours à l'utilisation de services *cloud* est possible malgré un risque faible (mais non nul) de communication aux États-Unis.

**c) Prise de position du PFPDT s'agissant de l'utilisation de services *cloud***

Le 13 juin 2022, le PFPDT a publié une prise de position relative à un projet de la Caisse nationale suisse d'assurance en cas d'accidents (la « SUVA ») impliquant le recours aux services *cloud* M365 de *Microsoft*, notamment les services *Outlook* (email et agenda) et *Teams* (vidéoconférence)<sup>91</sup>. Le projet implique un stockage des données personnelles sur une infrastructure *cloud* basée en Suisse. Le cocontractant (sous-traitant) de la SUVA est l'entité irlandaise du Groupe *Microsoft*.

La SUVA a identifié dans son analyse du projet le risque d'accès aux données hébergées sur le *cloud* par les autorités américaines en vertu du *US CLOUD Act*. Après avoir procédé à une analyse des risques, la SUVA estime que le risque d'un accès aux données par les autorités américaines dans ce contexte est très improbable (« *höchst unwahrscheinlich* ») et considère donc que le recours aux services M365 est licite au regard de la LPD (analyse similaire à celle effectuée par le Conseil d'État du canton de Zurich, discutée ci-dessus<sup>92</sup>).

Dans sa prise de position, le PFPDT estime tout d'abord que l'existence d'un risque de divulgation de données aux États-Unis eu égard au *US CLOUD Act* déclenche l'application des dispositions de la LPD en matière de communication transfrontalière de données (art. 6 LPD/art. 16 ss nLPD), nonobstant le stockage des données en Suisse<sup>93</sup>.

Ensuite, le PFPDT maintient sa position en vertu de laquelle, en cas d'existence d'un risque résiduel d'accès par les autorités d'un État ne garantissant pas un

---

<sup>90</sup> *Supra* V.F.2.a) et *infra* V.G.3.c).

<sup>91</sup> *Stellungnahme zur Datenschutz Risikobeurteilung der Suva zum Projekt Digital Workplace « M365 »* du 13 juin 2022 du PFPDT. Pour une analyse complète de cette prise de position, voir notamment : MÉTILLE, L'utilisation de *Microsoft*.

<sup>92</sup> *Supra* V.G.3.b).

<sup>93</sup> Même si la SUVA est qualifiée d'organe fédéral au sens de la LPD (art. 3 let. h LPD), les mêmes obligations en matière de communications transfrontalières s'appliquent aux responsables privés du traitement.

niveau de protection adéquat, aucune donnée personnelle ne peut être communiquée au prestataire<sup>94</sup>. En particulier, le PFPDT affiche un grand scepticisme quant à l'approche de la SUVA fondée sur les risques, l'autorité suisse prenant la position qu'une telle approche ne trouve pas d'ancrage dans le texte légal. De plus, face à l'argument de la SUVA suivant lequel les données concernées par le projet seraient de peu d'intérêt pour les autorités américaines, le PFPDT considère *a contrario* que le type de données personnelles ne devrait pas rentrer en compte dans l'analyse de risque en cas de communication transfrontalière.

À notre sens, contrairement à la position défendue par le PFPDT, le texte légal utilise une terminologie compatible avec une évaluation basée sur les risques (art. 6 LPD : « *contre les atteintes graves à la personnalité lors de transmissions à l'étranger* »/art. 16 nLPD « *un niveau de protection approprié est garanti* », mises en évidences ajoutées).

Les raisons suivantes pourraient, selon nous, expliquer la réticence du PFPDT à accepter l'existence d'un risque résiduel dans le cadre de sa prise de position relative au projet de la SUVA.

- La Commission européenne analyse actuellement si la décision d'adéquation de la Suisse pour le transfert de données basé sur le RGPD peut être maintenue. Le PFPDT cherche probablement à éviter toute prise de position qui pourrait avoir un impact négatif sur ce processus, en tenant compte également du net durcissement de la pratique des autorités européennes en matière de transfert de données personnelles aux États-Unis<sup>95</sup>.
- Pour rappel, le 25 mars 2022, la Commission européenne et les États-Unis ont annoncé avoir conclu un accord de principe sur un nouveau cadre réglementaire régissant les flux de données personnelles<sup>96</sup>. Cet accord reste pour le moment une simple déclaration d'intention. Dans sa prise de position, le PFPDT fait référence à cette annonce en précisant que, une fois un accord trouvé au niveau transatlantique, la Suisse devrait également négocier une telle réglementation.
- Le PFPDT a probablement également conscience de la nécessité concrète, pour l'économie suisse, de pouvoir recourir à des services de type *cloud* afin de maintenir sa compétitivité au niveau international.

---

<sup>94</sup> Guide PFPDT, analysé *in supra* V.F.2.a).

<sup>95</sup> À titre d'exemples, les décisions plus strictes prises dans les affaires de *Google Analytics* – décision de l'autorité autrichienne de protection des données du 22 décembre 2021 (D155.027 2021-0.586.257) ainsi que la décision de mise en demeure de la CNIL du 10 février 2022 (disponible à l'adresse : <<https://www.cnil.fr/fr/utilisation-de-google-analytics-et-transferts-de-donnees-vers-les-etats-unis-la-cnil-met-en-demeure>>, consulté le 3 juillet 2022) ; cf. *supra* V.G.3.b).

<sup>96</sup> Voir *supra* V.F.1.c).

Cette prise de position du PFPDT révèle la complexité de la question et les divergences d'opinions entre les différentes autorités de protection des données suisses. En effet, comme discuté ci-dessus<sup>97</sup>, le Conseil d'État du canton de Zurich avait estimé – après avoir consulté le Préposé cantonal zurichois à la protection des données – qu'une approche fondée sur le risque pouvait être appliquée pour analyser la licéité d'une communication transfrontalière en cas de recours à des services *cloud*.

#### 4. Conclusion

Le *US CLOUD Act*, lu en parallèle avec les dispositions de la nouvelle LPD (qui érige au rang d'infraction pénale le non-respect des règles suisses en matière de communication transfrontalière de données personnelles, art. 61 let. a nLPD) et avec la position stricte du PFPDT dans le contexte de la transmission de données personnelles vers des États réputés « non adéquats »<sup>98</sup>, doit clairement être un point d'attention pour toute entreprise suisse qui envisage de confier le traitement (y compris le stockage) de données à un prestataire soumis au *US CLOUD Act*. Tel sera typiquement le cas des principaux prestataires de services en matière de services *cloud*, tels que *Microsoft*, *Amazon* et *Google*.

L'analyse du risque découlant du *US CLOUD Act* doit également intervenir si la partie cocontractante est l'entité suisse ou européenne (par exemple irlandaise dans le cas de *Microsoft*) du groupe. De même, l'analyse de risque doit également être effectuée si un sous-traitant du prestataire de services présente un lien avec les États-Unis, pour autant naturellement que ce sous-traitant ait accès aux données en clair.

Cela étant dit, le *US CLOUD Act* ne doit, selon nous, pas non plus entraîner le blocage complet de tout projet impliquant un prestataire soumis à cette législation. À notre avis, une évaluation de l'impact de la communication (*Transfer Impact Assessment*) documentée devrait réduire de manière significative le risque d'une commission intentionnelle de l'infraction pénale prévue à l'art. 61 nLPD, étant précisé que le développement d'une pratique des autorités (cantonales) de protection des données sur cette question devra être suivi avec attention dès l'entrée en vigueur de la nouvelle LPD.

Pour rappel, l'accès aux autorités américaines de données à travers le *US CLOUD Act* garde un caractère exceptionnel. Il convient en effet de

---

<sup>97</sup> Voir *supra* V.G.3.b).

<sup>98</sup> Cf. les développements figurant dans le Guide du PFPDT (résumé au *supra* V.F.2.a) et la prise de position du PFPDT sur demande de la SUVA s'agissant d'un projet impliquant le recours aux services *cloud* M365 de *Microsoft* (analysée au *supra* V.G.3.c)).

rappeler que les modalités d'accès à l'information prévue par la Partie 1 du *US CLOUD Act* sont limitées aux situations de *serious crimes*. Par ailleurs, le risque juridique, en Suisse, lié au *US CLOUD Act* peut, à notre sens, être limité (sans être supprimé totalement) en travaillant sur les trois axes suivants :

- Préparation d'une analyse de risque documentée qui explique les raisons qui ont amené le responsable du traitement à initier un projet nonobstant les risques résiduels découlant du *US CLOUD Act* ;
- Introduction de clauses contractuelles spécifiques dans le rapport avec le prestataire de services *cloud* (par exemple une « *defend your data clause* »)<sup>99</sup> ;
- Information transparente des personnes concernées et, éventuellement, obtention du consentement (art. 6 al. 2 let. b LPD et art. 17 al. 1 let. a nLPD) de celles-ci (consentement qui peut être nécessaire dans tous les cas de transferts transfrontaliers de données personnelles qui ne peuvent pas être basés sur les SCC-UE/CH).

Comme mentionné, une juridiction française (le Conseil d'État) a estimé, certes dans le cadre d'une ordonnance statuant en référé, que le risque d'une divulgation fondée sur le *US CLOUD Act* ne constituait pas, en tant que tel, un transfert de données personnelles vers un État « non adéquat »<sup>100</sup>. Ainsi, selon cette ordonnance, ce risque ne déclenche pas les exigences découlant de l'arrêt *Schrems II* et, donc, des prises de position subséquentes des autorités<sup>101</sup>. Pour le surplus, dans un contexte suisse, il convient également de rappeler la décision du Conseil d'État zurichois qui a estimé que le risque découlant d'un accès fondé sur le *US CLOUD Act* était, dans la situation analysée, très faible et donc « acceptable »<sup>102</sup>.

---

<sup>99</sup> Sur les éléments à prendre en considération dans le contrat avec le prestataire, FISCHER/LARGANT, *On Cloud Number Nine : un bref survol des enjeux juridiques et réglementaires du cloud banking*, in <[www.swissprivacy.law/27](http://www.swissprivacy.law/27)> (consulté le 3 juillet 2022).

<sup>100</sup> LARGANT/FISCHER ; *Supra* V.G.3.a), dans sa prise de position sur une demande de la SUVA s'agissant d'un projet impliquant le recours aux services *cloud M365* de *Microsoft*, le PFPDT considère toutefois qu'un risque de transfert de données personnelles constituait déjà une communication transfrontalière (prise de position analysée au *supra* V.G.3.c).

<sup>101</sup> Recommandations du CEPD de juin 2021, *supra* V.F.1.b) ; en Suisse, le Guide du PFPDT est pertinent dans ce domaine, *supra* V.F.2.a).

<sup>102</sup> À noter toutefois les décisions plus strictes prises dans les affaires de *Google Analytics* – décision de l'autorité autrichienne de protection des données du 22 décembre 2021 (D155.027 2021-0.586.257) ainsi que la décision de mise en demeure de la CNIL du 10 février 2022 (disponible à l'adresse : <<https://www.cnil.fr/fr/utilisation-de-google-analytics-et-transferts-de-donnees-vers-les-etats-unis-la-cnil-met-en-demeure>>, consulté le 3 juillet 2022) ; cf. *supra* V.G.3.b).



## VI. Règlements applicables dans le secteur bancaire et financier

Un établissement bancaire qui souhaite recourir à des services *cloud* doit, en sus des obligations découlant du droit de la protection des données, tenir compte des exigences réglementaires (*infra* VI.A.) et examiner la compatibilité du projet avec le secret bancaire (*infra* VI.B.).

### A. Exigences réglementaires

La Circulaire FINMA 2018/03 – Outsourcing (la « Circulaire Outsourcing ») s'applique aux banques et maisons de titres suisses, ainsi qu'aux succursales suisses de banques et maisons de titres étrangères. À compter du 1<sup>er</sup> janvier 2021, le champ d'application de la Circulaire Outsourcing a été élargi aux directions de fonds (et aux SICAV autogérées qui sont traitées par analogie aux directions de fonds), ainsi qu'aux gestionnaires de fortune collective.

Dans une perspective matérielle, la Circulaire Outsourcing réglemente l'externalisation d'une fonction essentielle, à savoir une « *fonction dont dépend de manière significative le respect des objectifs et des prescriptions de la législation sur la surveillance des marchés financiers* » (Circulaire Outsourcing, N 4). Selon la pratique de la FINMA, toute externalisation impliquant la transmission à un prestataire de services d'une grande quantité de *client-identifying data* (CID) tombe *ipso facto* sous le coup de la Circulaire Outsourcing<sup>103</sup>.

L'application de la Circulaire Outsourcing déclenche une série d'obligations, dont les principales sont résumées ci-après :

- Choix, instruction et contrôle du prestataire de services (y compris *due diligence* documentée) ;
- Tenue d'un inventaire des externalisations de fonctions essentielles ;
- Extension du système de contrôle interne à la fonction externalisée ;
- Conclusion d'un contrat avec le prestataire de services qui contient notamment les dispositions suivantes :
  - Droit pour l'assujéti qui externalise de donner des instructions au prestataire de services et d'en contrôler l'exécution ;
  - Fixation contractuelle d'exigences en matière de sécurité de l'information, y compris un dispositif propre à assurer la continuité de la fonction externalisée en cas d'urgence ;

---

<sup>103</sup> Circulaire Outsourcing, Rapport sur l'audition concernant le projet de circulaire qui s'est déroulée du 6 décembre 2016 au 31 janvier 2017, 21 septembre 2017, p. 15.

- Droit d'accès et d'audit intégral, permanent et sans entraves au bénéficiaire (i) de l'assujetti, (ii) de son auditeur prudentiel et (iii) de la FINMA sur la fonction externalisée, à la fois auprès du prestataire de services et auprès de toute la chaîne de sous-traitance ; en cas de transfert à l'étranger (ce qui est souvent le cas lors du recours à un *cloud*), le prestataire de services doit garantir que ces droits puissent s'exercer dans le pays de destination ;
- Lorsque le prestataire de services fait appel à des sous-traitants pour exécuter tout ou partie d'une *fonction essentielle*, le contrat doit permettre à la banque (i) d'être informée suffisamment tôt du recours, respectivement du changement de sous-traitants et (ii) d'avoir la possibilité de mettre un terme au contrat d'externalisation si elle refuse le recours au sous-traitant. Ces sous-traitants doivent par ailleurs souscrire aux mêmes obligations que le prestataire de services *cloud*.

Les exigences de l'Annexe 3 de la Circulaire FINMA 2008/21 – Risques Opérationnels doivent également être prises en compte lorsque le recours au prestataire de services *cloud* implique la transmission de *client-identifying data* à ce dernier<sup>104</sup>.

## B. Exigences découlant du secret bancaire

La compatibilité avec le secret bancaire doit être analysée pour chaque projet qui implique la mise à disposition de *client-identifying data* au prestataire de services *cloud*, en particulier lorsque les spécificités de la prestation ne permettent pas la pseudonymisation ou le cryptage. Cette problématique sera exposée de manière très résumée ci-après.

Si la transmission est limitée à un prestataire de services *cloud* situé en Suisse (hypothèse peu réaliste compte tenu du *business model* des prestataires de services *cloud*), l'obtention d'une levée du secret bancaire par le client ne sera en principe pas nécessaire vu que le prestataire de services *cloud* est lui-même soumis au secret bancaire en vertu de l'art. 47 al. 1 let. a LB<sup>105</sup>. Ce constat vaut pour autant (i) que la banque exige contractuellement du prestataire de services le respect du secret bancaire et (ii) que la banque n'a pas donné des assurances différentes au client (par exemple en garantissant la non-transmission de *client-identifying data* en dehors de l'établissement).

---

<sup>104</sup> À noter que la FINMA a initié un processus de révision de cette circulaire.

<sup>105</sup> FF 1970 I 1197.

Le Guide « *Cloud* » publié par l'ASB<sup>106</sup> adopte le même raisonnement en cas de transmission de *client-identifying data* à un prestataire de services *cloud* localisé en dehors de Suisse, alors même que la protection pénale du secret bancaire est limitée par le principe de territorialité. En pratique, nombreuses sont les banques qui demandent une levée du secret bancaire dans cette dernière hypothèse, l'un des éléments clés, dans ce contexte, étant de s'assurer que cette renonciation au secret bancaire est octroyée sur une base dûment informée.

## VII. Conclusion

L'entreprise qui recourt à un prestataire de services *cloud* doit impérativement procéder à une analyse des risques, qui aborde notamment les risques juridiques, en amont du lancement du projet.

Premièrement, pour utiliser ce type de services, le responsable du traitement devra très probablement recourir à un prestataire externe. Cette première étape entraîne inmanquablement une certaine perte de contrôle sur les données personnelles et doit être encadrée de manière adéquate pour limiter de potentielles conséquences négatives pour les personnes concernées.

En second lieu, force est de constater que les principaux prestataires de services *cloud* sont aujourd'hui basés aux États-Unis<sup>107</sup>. Les mesures contractuelles de protection des données (nécessaires car les États-Unis sont un ordre juridique qui, dans une perspective suisse, ne bénéficie pas d'une réglementation adéquate en matière de protection des données) ne sont généralement pas, à elles seules, suffisantes pour assurer la conformité au droit suisse de la protection des données.

Il convient d'examiner si les données sont communiquées directement dans un État ne garantissant pas un niveau de protection adéquat ou si elles sont seulement potentiellement accessibles, de manière indirecte, notamment à travers le *US CLOUD Act*.

Ces deux conséquences inhérentes à tout projet impliquant des services *cloud* doivent être prises en considération dans l'analyse de risque effectuée par le responsable du traitement.

Le responsable du traitement devra toujours examiner en amont la nécessité et la possibilité de mettre en place des mesures techniques (anonymisation, pseudonymisation) destinées à limiter l'impact dans une perspective de protection des données. En effet, ces mesures permettent au responsable du

---

<sup>106</sup> Association suisse des banquiers, Guide « *Cloud* », 2<sup>e</sup> édition, juin 2022, p. 36 ss.

<sup>107</sup> Respectivement, ces prestataires présentent des liens avec les États-Unis et entrent par conséquent dans le champ d'application du *US CLOUD Act* (cf. *supra* V.G.).

traitement de limiter, voire de supprimer, le risque de porter atteinte à la personnalité des personnes concernées. Néanmoins, en fonction de la nature des services de type *cloud* envisagés par le responsable du traitement, ces mesures se révèlent parfois impossibles à mettre en œuvre, respectivement déclenchent des coûts qui menacent la viabilité économique du projet.

Pour conclure, n'oublions pas que les solutions *cloud* offrent des fonctionnalités attrayantes, utiles et innovantes pour les entreprises et renforcent même dans certaines situations le niveau de protection des données concernées (notamment au vu de la mutualisation des investissements en matière de sécurité). Dès lors, il conviendra plutôt d'appréhender et de limiter les enjeux relatifs à l'utilisation de ces services et des risques qui en découlent. Cette approche permettra de déterminer si, au vu des circonstances du cas d'espèce, la balance entre les risques inhérents aux services *cloud* (que des mesures de protection peuvent réduire, mais pas nécessairement supprimer entièrement) et les avantages qui en découlent penche plutôt du côté du recours à une infrastructure fondée sur le *cloud* ou pas.

À titre de remarque conclusive, il nous semble important de rappeler que le risque d'accès aux données personnelles par des autorités étrangères (notamment, mais pas uniquement, sur la base du *US CLOUD Act*) ne constitue pas l'unique prisme par lequel un projet d'externalisation de données doit être analysé. L'impératif de sécurité des données (à savoir la protection contre des intrusions de tiers qui ne sont pas acteurs gouvernementaux) et la nécessité de garantir la *business continuity* en cas de défaillance du prestataire représentent des enjeux tout aussi importants, voire plus cruciaux en termes de risques effectifs pour les données personnelles confiées à un tiers.

## VIII. Bibliographie

### A. Doctrine

**Yaniv BENHAMOU/Frédéric ERARD/Daniel KRAUS**, L'avocat a-t-il aussi le droit d'être dans les nuages ?, *Revue de l'avocat* 2019, p. 119-126 ; **Jens BRAUNECK**, Europa-Cloud : Zwang der US CLOUD Act EU-Unternehmen zur EU-rechtswidrigen Datenherausgabe ?, *EWS* 2019, p. 307 ss ; **Benoît CHAPPUIS/Adrien ALBERINI**, Secret professionnel de l'avocat et solutions cloud, *Revue de l'avocat* 2017, p. 337-343 ; **Frédéric ERARD**, Le secret médical – Étude des obligations de confidentialité des soignants en droit suisse, thèse de doctorat, Collection sui generis, Zurich 2021 ; **Reto FANGER**, Auswirkungen des revidierten Datenschutzgesetzes auf Cloudanbieter in der Schweiz, *Jusletter* du 22 avril 2021 ; **Philipp FISCHER**, De la « sphère de sécurité » au « bouclier de protection » : aspects choisis du EU-US privacy shield, *Revue de droit des affaires internationales*, Thomson Reuters, 2018, p. 143 (cité : FISCHER, De la « sphère de sécurité » au « bouclier de protection ») ; **Philipp FISCHER/Kastriot LUBISHTANI**, Mesures techniques, contractuelles et organisationnelles à observer suite à

l'arrêt Schrems II, 7 décembre 2020, in <[www.swissprivacy.law/40](http://www.swissprivacy.law/40)> (consulté le 3 juillet 2022) ; **Philipp FISCHER/Sébastien PITTET**, US CLOUD Act – un aperçu, 8 novembre 2021, in <[www.swissprivacy.law/101](http://www.swissprivacy.law/101)> (consulté le 3 juillet 2022) ; **Célian HIRSCH/Emilie JACOT-GUILLARMOD**, Les données bancaires pseudonymisée – Du secret bancaire à la protection des données, RSDA 2/2020, p. 151-167 ; **Emilie JACOT-GUILLARMOD**, Schrems II : Validation des clauses types (CJUE) (2/2), in <[www.lawinside.ch/950/](http://www.lawinside.ch/950/)> (consulté le 3 juillet 2022) ; **Alexandre JOTTERAND**, Les communications numériques de l'avocat avec son client : quels outils en 2022 ?, Revue de l'avocat 2022, p. 179 ss ; **Christian LAUX/Alexander HOFMANN/Mark SCHIEWECK/Jürg HESS**, Nutzung von Cloud-Angeboten durch Banken, Jusletter 27 mai 2019 ; **Marine LARGANT/Philipp FISCHER**, Health Data Hub, Jusletter du 7 juin 2021 ; **Urs MAURER-LAMBROU/Gabor-Paul BLECHTA (éds)**, Basler Kommentar Datenschutz/Öffentlichkeitgesetz, 3<sup>e</sup> éd., Bâle 2014 (cité : BSK DSG/BGÖ-AUTEUR) ; **Philippe MEIER**, Protection des données – Fondements, principes généraux et droit privé, Berne 2011 ; **Philippe MEIER/Nicolas TSCHUMY**, L'adresse IP : une donnée personnelle ? Ou quand la CJUE rejoint le TF !, Jusletter du 23 janvier 2017 ; **Sylvain MÉTILLE**, La (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020 : des principes, des droits et des obligations, in Astrid EPINEY/Sophie MOSER/Sophia ROVELLI (Hrsg.), Die Revision des Datenschutzgesetzes des Bundes/La révision de la Loi fédérale sur la protection des données, Zurich 2022 (cité : MÉTILLE, La (nouvelle) Loi fédérale sur la protection des données) ; **Sylvain MÉTILLE**, Le traitement de données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données du 25 septembre 2020, SJ 2021 II 1 ss ; **Sylvain MÉTILLE**, L'informatique en nuage au sein d'une étude d'avocats, Plaidoyer 3/13 2013, p. 39 ss (cité : MÉTILLE, L'informatique en nuage) ; **Sylvain MÉTILLE**, L'utilisation de l'informatique en nuage par l'administration publique, AJP/PJA 6/2019, p. 609 ss (cité : MÉTILLE, L'informatique en nuage par l'administration publique) ; **MÉTILLE Sylvain**, L'utilisation de Microsoft 365, illégale en Suisse ?, in : <<https://smetille.ch/2022/06/17/lutilisation-de-microsoft-365-illegale-en-suisse/>> (consulté le 3 juillet 2022) (cité : MÉTILLE, L'utilisation de Microsoft) ; **Philippe GILLIÉRON**, Télémonitoring et données médicales : le casse-tête des professionnels de la santé, 6 mai 2022, in <[www.swissprivacy.law/143](http://www.swissprivacy.law/143)> (consulté le 3 juillet 2022) ; **Tanja LUTZ/Luisa EGLI**, Braucht die Schweiz ein CLOUD Act Executive Agreement?, RSJ 117/2021, p. 119 ss ; **David ROSENTHAL**, Microsoft Cloud für Schweizer Anwälte, Revue de l'avocat 2021, p. 443-446 (cité : ROSENTHAL, Microsoft) ; **David ROSENTHAL**, Mit Berufsgeheimnissen in die Cloud : So geht es trotz US CLOUD Act, Jusletter du 10 août 2020 (cité : ROSENTHAL, US CLOUD Act) ; **David ROSENTHAL** (en collaboration avec Studer Samira/Lombard Alexandre pour la traduction), La nouvelle loi sur la protection des données, Jusletter du 16 novembre 2020 (cité : ROSENTHAL) ; **Martina SCHWARZ**, Der US-CLOUD ACT, EF 4/20, p. 193 ss ; **Christian SCHWARZENEGGER/Florent THOUVENIN/Burkhard STILLER/Damian GOERGE**, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Revue de l'avocat 2019, p. 25-32 ; **Iris SIDLER/David VASELLA**, Aus Safe Harbor wird Privacy Shield : Folgen des Urteils des EuGH i.S. Schrems, sic! 2016, p. 185 ss ; **David VASELLA**, EuGH i.S. Schrems II (Rs. C-311/18) : Der Privacy Shield ist wichtig, die Standardklauseln bleiben wirksam, der Exporteur hat hohe Pflichten, in Datenrecht.ch (cité : VASELLA) ; **David VASELLA**, La nouvelle loi sur la protection des données et sa mise en œuvre, TREX 2021 p. 278 ss (cité : VASELLA, La nouvelle loi sur la protection des données) ; **David VASELLA**, Regierungsrat Zürich: grünes Licht für M365 ; Risikobeurteilungsmodell Rosenthal kanonisiert; Risikogrenze bei 10% über 5 Jahre, in Datenrecht.ch (cité : VASELLA, Regierungsrat Zürich) ; **Rolf H. WEBER**, Datenexport in die USA – neue Welt nach Schrems II ?, EuZ 2021, S. 24 ss ; **Wolfgang WOHLERS**, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), Zurich 2016 ; **Remy**

ZGRAGGEN/Elena OLGATI, Cloud-Outsourcing im Versicherungsbereich, REAS 2021 p. 366 ss.

## B. Communications du Préposé fédéral à la protection des données et à la transparence

**Explications concernant l'informatique en nuage**, disponible à l'adresse : <[https://www.edoeb.admin.ch/edoeb/fr/home/protection-des\\_donnees/Internet\\_und\\_Computer/cloud-computing/explications-concernant-l-informatique-en-nuage--cloud-computing.html](https://www.edoeb.admin.ch/edoeb/fr/home/protection-des_donnees/Internet_und_Computer/cloud-computing/explications-concernant-l-informatique-en-nuage--cloud-computing.html)> (consulté le 3 juillet 2022) (cité : PFPDT, Explications concernant l'informatique en nuage); **Explications relatives à la communication de données personnelles à l'étranger suite à la révision de la loi fédérale sur la protection des données**, disponible à l'adresse : <[https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2017/01/erlaeuterungen\\_zurueberrmittlungvonpersonendateninsausland.pdf.download.pdf/explications\\_relativesalacommunicationdedonneespersonnellesaetr.pdf](https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2017/01/erlaeuterungen_zurueberrmittlungvonpersonendateninsausland.pdf.download.pdf/explications_relativesalacommunicationdedonneespersonnellesaetr.pdf)> (consulté le 3 juillet 2022) (cité : PFPDT, Communication); **Prise de position du PFPDT du 8 août 2020 sur la transmission de données personnelles vers les États-Unis et d'autres États n'offrant pas un niveau adéquat de protection des données au sens de l'art. 6 al. 1 LPD**, disponible à l'adresse : <[https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/Positionspapier\\_PS\\_%20ED%C3%96B\\_FR.pdf.download.pdf/Positionspapier\\_PS\\_%20ED%C3%96B\\_FR.pdf](https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/Positionspapier_PS_%20ED%C3%96B_FR.pdf.download.pdf/Positionspapier_PS_%20ED%C3%96B_FR.pdf)> (consulté le 3 juillet 2022) (cité : Prise de position du PFPDT du 8 août 2020); **Communiqué du PFPDT du 8 septembre 2020 : « Le PFPDT estime que le bouclier de protection des données Suisse – États-Unis n'offre pas un niveau de protection des données adéquat »**, disponible à l'adresse : <<https://www.edoeb.admin.ch/edoeb/fr/home/actualites/medias/medienmitteilungen.msg-id-80318.html>> (consulté le 3 juillet 2022) (cité : Communiqué du PFPDT du 8 septembre 2020); **Guide du PFPDT pour l'examen de la licéité de la communication transfrontière de données (art. 6, al. 2, let. a, LPD)**, publié en juin 2021 (cité : Guide du PFPDT); **Prise de position du PFPDT du 27 août 2021 : Transfert de données personnelles dans un pays ne présentant pas le niveau de protection des données requis, en application de clauses contractuelles types et de contrats types reconnus**, disponible à l'adresse : <<https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2021/Paper%20SCC%20def.%20FR%2008092021.pdf.download.pdf/Paper%20SCC%20def.%20FR%2008092021.pdf>> (consulté le 3 juillet 2022) (cité : Prise de position du PFPDT du 27 août 2021).

## C. Autres

**Conférence des préposé(e)s suisses à la protection des données (privatim)**, Aide-mémoire sur les risques et les mesures spécifiques à la technologie du Cloud du 17 décembre 2019.

---

# Überlegungen zu Recht und Risiko bei behördlicher Cloudnutzung

DANIEL DZAMKO-LOCHER<sup>1</sup>

Dr. iur. Rechtsanwalt, Leiter Direktionsbereich Datenschutz,  
Eidg. Datenschutz- und öffentlichkeitsbeauftragter (EDÖB)

## Inhaltsverzeichnis

<b>I. Problemstellung, Gegenstand und Eingrenzungen</b> .....	<b>84</b>
A. Problemstellung .....	84
B. Gegenstand.....	85
C. Eingrenzungen .....	86
<b>II. Datenschutz</b> .....	<b>86</b>
A. Einleitung .....	86
B. DSGVO, insbes. Art. 10a und 6.....	87
C. Bereichsspezifische Regelungen.....	92
D. Cloud-Risiken im Überblick .....	94
E. Risikomindernde Massnahmen .....	96
F. Fazit.....	101
<b>III. Amtsgeheimnis</b> .....	<b>102</b>
A. Einleitung .....	102
B. Art. 320 StGB .....	106
C. Fazit.....	112
<b>IV. Informationsschutz</b> .....	<b>112</b>
A. Einleitung .....	112
B. Geltendes Recht .....	113
C. Das Informationssicherheitsgesetz (ISG).....	113
D. Fazit.....	115
<b>V. Schluss</b> .....	<b>115</b>
<b>VI. Literatur</b> .....	<b>116</b>
<b>VII. Materialien</b> .....	<b>117</b>

---

<sup>1</sup> Ich äussere im vorliegenden Beitrag, der eine erweiterte Fassung eines Referats ist und stellenweise den Vortragsstil beibehält, meine persönliche Auffassung. Die Überlegungen reflektieren den Stand der Diskussion im Frühjahr 2022. Ich danke meinen Kolleginnen beim EDÖB für wertvolle Hinweise, insbes. Herrn Matthias Haussener, Informationssystem- und Sicherheitsspezialist, und Herrn Marc-Olivier Tricot, Spécialiste en Information et Sécurité. Ebenso danke ich Herrn Prof. Sylvain Métille für die kritische Durchsicht und wertvolle Hinweise.

## I. Problemstellung, Gegenstand und Eingrenzungen

### A. Problemstellung

Mit der digitalen Transformation der Bundesverwaltung strebt der Bundesrat auch die Nutzung von öffentlichen Cloud-Diensten an. Seine Cloud-Strategie verfolgt das Ziel, « *den Weg für die Nutzung von Cloud-Diensten zu ebnen* », durch die « *Nutzung von Public Clouds soll der schnelle Zugang zu neuesten Technologien für wirtschaftliche und innovative Verwaltungsleistungen* » ermöglicht werden<sup>2</sup>. Teilweise ergibt sich der wachsende Bedarf auch daraus, dass heute genutzte Standardapplikationen zunehmend als Cloud-Services angeboten und weiterentwickelt werden<sup>3</sup>. Zur Kehrseite dieser Entwicklung gehören eine gesteigerte Abhängigkeit von den meist global agierenden Anbietern und eine Reihe von neuen oder akzentuierten datenschutzrechtlichen Risiken<sup>4</sup>. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte fordert deshalb, dass der Datenschutz in den jeweiligen Cloud-Projekten frühzeitig mithilfe von Datenschutz-Folgenabschätzungen und auch schon bereits im Rahmen der Ausschreibungsverfahren berücksichtigt wird<sup>5</sup>. Seine Impulse wurden verschiedentlich aufgenommen und fanden auch Eingang in die Cloud-Strategie<sup>6</sup>.

Am 2. Februar 2022 legte der Bundesrat seine aktuellen Schwerpunkte für die Digitalisierung fest<sup>7</sup>, zwei der vier Schwerpunkte sind « Vertrauenswürdige Datenräume » sowie « Swiss Internet Jurisdiction und digitale Souveränität ». Damit lässt der Bundesrat erkennen, dass er nebst dem Ziel einer effizienteren und effektiveren digitalen Verwaltung auch der Wahrung informationeller Selbstbestimmung und Privatsphäre einen hohen Stellenwert einräumt. Auch die Sicherheitspolitische Kommission des Nationalrates setzte am 15. Februar 2022 ein Zeichen, indem sie der Parlamentarischen Initiative 21.495 Moret Isabelle Folge gab. Die Kommissionsmehrheit erachtet es « *als notwendig*,

---

<sup>2</sup> BUNDESRAT, Cloud-Strategie, Ziff. 1. Vgl. auch ISB, Bericht zur Bedarfsabklärung für eine « Swiss Cloud », Dezember 2020, Ziff. 6.4, S. 25.

<sup>3</sup> Ähnlich KANTON ZÜRICH, Cloud-Lösungen, Ziff. 1.

<sup>4</sup> Vgl. zu den seitens Verwaltung geäusserten Bedenken betreffend Datenschutz und Datensicherheit ISB, Ziff. 6.4, S. 25 f.

<sup>5</sup> Vgl. z.B. die Forderungen des EIDG. DATENSCHUTZ- UND ÖFFENTLICHKEITS-BEAUFTRAGTEN (EDÖB) in seinem 28. Tätigkeitsbericht 2020/21, S. 15 ff.

<sup>6</sup> BUNDESRAT, Cloud-Strategie, Fn. 2, Ziff. 4 : « Weiter ist zu beurteilen, ob [bei einer Datenverarbeitung in einer Public Cloud] Personendaten bearbeitet werden und mithin eine Datenschutz-Folgenabschätzung vorzunehmen ist... ».

<sup>7</sup> <<https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id87029.html>> (letztmals besucht am 2.2.2022).



dass die Schweiz eine eigenständige digitale Infrastruktur schafft, die insbesondere auch die Clouddienste umfasst »<sup>8</sup>.

Nachfolgend beleuchte ich einige der Anforderungen, die sich aus dem Datenschutzrecht und ausgewählten weiteren Rechtsquellen namentlich für die behördliche Nutzung von Public Clouds ergeben. Zu den augenfälligsten spezifischen Anforderungen für Behörden gehört das Amtsgeheimnis, insbesondere nach Art. 320 StGB, worauf ich in einem gesonderten Abschnitt näher eingehe.

## B. Gegenstand

Cloud-Services werden nach verschiedenen Kriterien charakterisiert und eingeteilt. Dies wurde bereits in zahlreichen Publikationen dargelegt<sup>9</sup>, weshalb ich mich hier auf einige wenige zusammenfassende Hinweise beschränke.

Merkmale, die Cloud-Services namentlich von typischen On-Premise- und Managed Service-Lösungen unterscheiden, sind :

- On-demand self service,
- Broad network access,
- Resource pooling,
- Rapid elasticity und
- Measured service<sup>10</sup>.

Regelmässig wird bei den Cloud-Services nach den Service Models unterschieden :

- Software as a Service (SaaS),
- Platform as a Service (PaaS) und
- Infrastructure as a Service (IaaS).

Ein weiteres Einteilungskriterium sind die Deployment Models bzw. Liefermodelle, folgend die geläufigsten :

- Private cloud,
- Community cloud,
- Public cloud und
- Hybrid cloud.

---

<sup>8</sup> Medienmitteilung SiK-N vom 15.2.2022, <[https://www.parlament.ch/press\\_releases/Pages/mm-sik-n-2022-02-15.aspx](https://www.parlament.ch/press_releases/Pages/mm-sik-n-2022-02-15.aspx)> (letztmals besucht am 17.2.2022).

<sup>9</sup> Vergleiche statt vieler BSK DSG-BÜHLER/RAMPINI, Art. 10a, N 22 ff.

<sup>10</sup> Vgl. hierzu und zum Folgenden die NIST Definition of Cloud Computing : <<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>> (letztmals besucht am 21.2.2022).

Der auffälligste Unterschied zwischen dem Bezug von Managed Services und Cloud Services ist, dass letztere stark standardisiert sind, während erstere weitgehend von den Kunden vorgegeben oder zumindest mitbestimmt werden<sup>11</sup>. Dies ist auch für datenschutzrechtliche Aspekte bedeutsam, im Extremfall kann es zu einer « *take it or leave it* »-Situation führen.

Wie bereits erwähnt, geht es nachfolgend insbesondere um die behördliche Nutzung von Public Cloud-Services.

## C. Eingrenzungen

Im Fokus stehen die Bundesbehörden und insbesondere die Bundesverwaltung, hauptsächlich mit Blick auf das Datenschutzrecht sowie das Amtsgeheimnis gem. Art. 320 StGB. Mit Blick auf im Wesentlichen analoge Anforderungen des kantonalen Datenschutzrechts dürften die nachfolgenden Ausführungen indes auch mit Blick auf kantonale Behörden relevant sein. Da Personendaten auch Informationen im Sinne der Regelungen zum Informationsschutz sind, schliesst der Beitrag mit einigen Ausführungen zu den einschlägigen bundesrechtlichen Regelungen<sup>12</sup>. Der Beitrag beschränkt sich auf das schweizerische Recht und klammert das Völkerrecht aus. Er setzt unter verschiedenen Aspekten Schwerpunkte und strebt weder eine vollständige noch eine vertiefte Behandlung der Fragen an.

## II. Datenschutz

### A. Einleitung

Nutzt eine Behörde Cloud-Services, liegt aus datenschutzrechtlicher Sicht eine Auftragsbearbeitung vor. Ihre Zulässigkeit richtet sich nach Art. 10a DSG bzw. Art. 9 nDSG, wobei die Behörde für den Datenschutz verantwortlich bleibt<sup>13</sup>. Da es sich in der Regel um internationale Anbieter

---

<sup>11</sup> Vgl. BUNDESRAT, Cloud-Strategie, Ziff. 7 Glossar.

<sup>12</sup> Vgl. zur Auswahl dieser Aspekte auch BUNDESRAT, Cloud-Strategie, welche nach Ziff 1 u.a. beantworten will, unter welchen Bedingungen Daten bezogen auf den Informations- und den Datenschutz sowie die Geheimhaltungspflichten in Public Clouds bearbeitet werden dürfen. Vgl. weiter ISB, Ziff. 7.3, Handlungsfeld 2, Zielsetzung : « (Völker-)rechtlicher Rahmen ist geklärt, insbesondere im Bereich Datenschutz, Informationsschutz, Geheimnisschutz ».

<sup>13</sup> Art. 16 Abs. 1 DSG i.V.m. Art. 22 VDSG. Auf gemeinsame Bearbeitungen i.S.v. Art. 16 Abs. 2 DSG gehe ich nicht näher ein. Ebensowenig auf Konstellationen, in denen ein Cloud-Anbieter zum Verantwortlichen wird.

handelt, kann es zu grenzüberschreitenden Bekanntgaben kommen, für die zusätzlich Art. 6 DSGVO bzw. Art. 16 ff. nDSG gilt<sup>14</sup>. Bei der Beurteilung einer Cloud-Lösung und für den Entscheid über die Umsetzung scheint sich in der behördlichen Praxis zunehmend ein *risikobasierter Ansatz* zu etablieren. Nachfolgend wird der Frage nachgegangen, in welchem Verhältnis ein risikobasierter Ansatz zu den anwendbaren Rechtsnormen steht und ob er sich im internationalen Verhältnis entfalten kann. Nicht näher behandelt, sondern nur anhand zweier Beispiele illustriert wird, dass stets auch weitere Normen, namentlich des bereichsspezifischen Datenschutzrechts, zu prüfen sind<sup>15</sup>.

## B. DSGVO, insbes. Art. 10a und 6

Bei der Auftragsbearbeitung nach Art. 10a DSGVO dürfen die Daten nur so bearbeitet werden, wie der Auftraggeber selbst dies tun darf<sup>16</sup>. Im behördlichen Kontext beinhaltet dies den grundrechtlichen Schutz der betroffenen Personen<sup>17</sup>. Deshalb kann die vertragliche Übertragung an den Auftragsbearbeiter durch eine Behörde nicht ohne Weiteres durch Akzept der allgemeinen Bedingungen des Cloud-Anbieters erfolgen, sondern erfordert für den konkreten Fall eine Prüfung und ggf. Anpassung der Vertragsregelungen<sup>18</sup>. Der Auftraggeber hat eine Überwachungspflicht und muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet<sup>19</sup>. Er hat den Dritten mithin sorgfältig auszuwählen, zu instruieren und zu überwachen<sup>20</sup>. Ausgeschlossen ist eine Datenbearbeitung durch Dritte allerdings, wenn eine gesetzliche (oder vertragliche) Geheimhaltungspflicht es verbietet<sup>21</sup>. Bei Behörden ist insbesondere das *Amtsgeheimnis* zu beachten, das unter Ziff. III unten näher beleuchtet wird.

Da die Bereitstellung von Cloud-Services oft durch Anbieter und Infrastruktur im Ausland erfolgt, steht zudem eine grenzüberschreitende Datenbekanntgabe in Frage, die nur nach den Voraussetzungen von Art. 6 DSGVO zulässig ist. Pro-

---

<sup>14</sup> Vgl. im Kontext des nDSG BBl 2017, 7032.

<sup>15</sup> Im DSGVO selbst sind ebenfalls weitere Normen zu beachten, wie namentlich die Grundsätze nach Art. 4 DSGVO oder Regeln aus dem 4. Abschnitt wie z.B. Verpflichtungen aus Art. 25 DSGVO. Zu den einschlägigen VDSG-Bestimmungen gehören namentlich Art. 8 ff. zu den TOM und Art. 22 zur Auftragsbearbeitung.

<sup>16</sup> Art. 10a Abs. 1 Bstb. a DSGVO, Art. 9 Abs. 1 Bstb. a nDSG.

<sup>17</sup> Vgl. auch BAERISWYL, Wenn die Rechtsauslegung «nebulös» wird, digma 2019, S. 118.

<sup>18</sup> In diesem Sinn auch MÉTILLE, S. 616.

<sup>19</sup> Art 10a Abs. 2 DSGVO, Art. 22 Abs. 2 VDSG ; Art. 9 Abs. 2 nDSG.

<sup>20</sup> Vgl. statt vieler EPINEY/FASNACHT, in BELSER/EPINEY/WALDMANN, § 10 N 43 ff.

<sup>21</sup> Art. 10a Abs. 1 Bstb. b DSGVO, Art. 9 Abs. 1 Bstb. b.

blematisch ist insbesondere, wenn im Zielland kein angemessenes Datenschutzniveau besteht oder Zugriff aus einem solchen Land droht. Bei der Übermittlung ins Ausland ergibt sich nach dem geltenden Art. 6 Abs. 1 DSGVO eine schwerwiegende Gefährdung der Persönlichkeit – und mithin ein ohne weitere Vorkehrungen inakzeptabel hohes und deshalb verbotenes Risiko – insbesondere dann, wenn die Gesetzgebung im Zielstaat keinen angemessenen Schutz gewährt<sup>22</sup>. Diesfalls müssen für eine rechtmässige Übermittlung nach Art. 6 Abs. 2 DSGVO Massnahmen ergriffen werden, in der Praxis namentlich mittels vertraglicher Regelungen<sup>23</sup>, die jedoch auch nicht immer ausreichenden Schutz gewähren können<sup>24</sup>.

Zu den umstrittenen Fragen in diesem Zusammenhang gehört, ob sich in diesen Fällen ein *risikobasierter Ansatz* entfalten kann<sup>25</sup>. Mangels gerichtlicher Beurteilung in der Schweiz fallen hierzu insbesondere die einschlägigen Verlautbarungen des EDÖB ins Gewicht<sup>26</sup>. Wenn wie im Fall der USA ein ungenügendes Datenschutzniveau vorliegt<sup>27</sup> und zusätzlich auch die seitens des EDÖB in Anlehnung an das EuGH-Urteil i.S. Schrems II<sup>28</sup> definierten grundlegenden Garantien<sup>29</sup> im Zielland nicht erfüllt sind, müssen nebst den vertraglichen Regelungen zusätzliche Massnahmen ergriffen werden. Eine Beurteilung der Massnahmen nach einem « risikobasierten Ansatz », der Risiken und Massnahmen identifiziert und im Hinblick auf ein Restrisiko bewertet, wird m.E. vom EDÖB in den publizierten Dokumenten nicht explizit verworfen, allerdings sind die Anforderungen hoch<sup>30</sup>.

---

<sup>22</sup> Art. 16 f. nDSG verlangen mit einem veränderten Ansatz inkl. neuer Feststellung der Angemessenheit durch den Bundesrat weiterhin einen angemessenen Schutz im Zielland oder kompensatorische Massnahmen oder Ausnahmen.

<sup>23</sup> Vgl. Art. 6 Abs. 2 Bstb. a DSGVO, Art. 19 i.V.m. 6 VDSG.

<sup>24</sup> EDÖB, Anleitung, N 08.

<sup>25</sup> Allerdings dominiere die bejahenden stimmen. Ablehnend gegenüber dem risikobasierten Ansatz im Kontext der Datenübermittlung in Staaten ohne angemessenes Datenschutzniveau MAURER-LAMBROU, US-Cloud Act, und DERSELBE, US Cloud Act, 13. Nach seiner Auffassung gibt es für den « *risikobasierten Ansatz, bei dem die analog einzuhaltenden Garantien beiseitegelassen werden, [...] keine rechtliche Basis* », « *no legal basis for the risk-based approach in which the four analogous guarantees to be complied with are set aside* ».

<sup>26</sup> Die einschlägigen Dokumente finden sich auf der Übersichtsseite « Übermittlung ins Ausland », <<https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html#-2053327153>> (letztmals besucht am 21.2.2022).

<sup>27</sup> Vgl. auch BJ, Ziff. 7 und Ziff. 5.5.

<sup>28</sup> Urteil des EuGH i.S. Schrems II (Rs. C-311/18).

<sup>29</sup> EDÖB, Anleitung, N 05.

<sup>30</sup> Auszüge EDÖB, Anleitung, N 08 : « *Zusätzliche vertragliche Massnahmen [...] sind kaum möglich [...] Die zusätzlichen technischen und organisatorischen Massnahmen müssen dergestalt sein, dass die Behördenzugriffe [...] faktisch verhindert werden* ». Die für die Datenhaltung genannten BYOK und zusätzlich BYOE dürften dafür nicht genügen. Vgl. weiter EDÖB, Übermittlung, Ziff. 4.1.

Der risikobasierte Ansatz wird in der Diskussion oft nicht näher erläutert. Als prägende Leitlinie der jüngsten DSGVO-Revision bedeutet er namentlich, dass das nDSG für unterschiedlich risikobehaftete Konstellationen unterschiedliche Regeln vorsieht, etwa durch strengere Pflichten bei hohen Risiken<sup>31</sup>. Teilweise schreiben Bestimmungen einen risikobasierten Ansatz direkt vor: Bereits bei einer grammatikalischen Auslegung ist dies offensichtlich z.B. in Art. 7 Abs. 2 oder 8 Abs. 1 nDSG, wonach technische und organisatorische Massnahmen u.a. *dem Risiko angemessen* sein müssen<sup>32</sup>.

Nach meinem Dafürhalten ist ein strukturiertes Vorgehen bei der Risikoanalyse betreffend Cloud-Vorhaben zu begrüßen, es schafft Transparenz bzw. Nachvollziehbarkeit. Eine solche Methode darf aber nicht dazu führen, dass das Gesetz weg- statt ausgelegt wird. Angesichts der rechtlichen und technischen Unsicherheiten und der damit verbundenen Projektrisiken sind praxistaugliche – also einfach handhabbare, effiziente – Instrumente für die digitalisierungswilligen Behörden verständlicherweise attraktiv. Inwieweit in Anwendung solcher Instrumente aufgrund einer Verkettung von risikomindernden Massnahmen ein Restrisiko quantifiziert und akzeptiert werden kann, muss sich indes durch Auslegung aus den anwendbaren Gesetzesnormen ableiten lassen<sup>33</sup>. Die Datenschutzbehörden in der Schweiz und Europa konkretisieren derzeit in ihrer Aufsichtspraxis die rechtlichen Anforderungen an behördliche Cloud-Lösungen, zwangsläufig inklusive der Frage des risikobasierten Ansatzes<sup>34</sup>, stets unter dem Vorbehalt einer gerichtlichen Beurteilung. Auch die Gerichte werden im Kontext der behördlichen Nutzung von Cloud-Lösungen

<sup>31</sup> Vgl. BUNDESRAT, Botschaft DSGVO, BBl 2017, 6970 f.

<sup>32</sup> Vgl. dazu auch BUNDESRAT, Botschaft DSGVO, BBl 2017 7030 oben und 7031; vgl. schon heute *angemessene Massnahmen* nach Art. 5 und 7 DSGVO.

<sup>33</sup> Zur schon länger dauernden Diskussion betreffend DSGVO vgl. z.B. SCHRÖDER MARKUS, passim, nach dem gemäss überwiegender Auffassung der risikobasierte Ansatz die gesetzlichen Anforderungen ergänzt und nicht ersetzt. Vgl. neuerdings Ablehnung des risikobasierten Ansatzes für Art. 44 DSGVO durch die österreichische Datenschutzbehörde, mit Teilbeschleidspruch vom 22.4.2022, <<https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt.pdf>> (*zuletzt besucht am 2.5.2022*), D.4. Spruchpunkt 2.c). Illustrativ dazu, wie sich Grenzen eines risikobasierten Ansatzes manifestieren können, Bger-Urteil 1C\_273/2020 v. 5.1.2021 (= BGE 147 I 346, enthält nicht alle hier erwähnten Erwägungen), wo in Anwendung des Grundsatzes der Datenminimierung bzw. der Verhältnismässigkeit die hohe Sicherheit der Verschlüsselung bzw. ein quantifiziertes Entschlüsselungsrisiko nicht entscheidend war (vgl. E. 5.5.3 und zur Sicherheit u.a. E. 5.1).

<sup>34</sup> Soweit für mich ersichtlich nimmt in der Schweiz der Kanton Zürich eine Vorreiterrolle ein und hat im Rahmen des kantonal massgeblichen Datenschutzrechts den risikobasierten Ansatz bereits anerkannt, indem er festhält, das « *Modell von David Rosenthal zur Ermittlung der Restrisiken eines Lawful Access* » sei « *breit abgestützt und anerkannt* » und werde « *deshalb für die Risikobeurteilung beim Einsatz von Cloud-Lösungen in der kantonalen Verwaltung als Standard festgelegt* » (KANTON ZÜRICH, Cloud-Lösungen, Ziff. 5).

die anerkannten Auslegungsmethoden anwenden, um den Normsinn zu eruieren und zu erkennen, welche konkreten Anforderungen aufgrund von Bestimmungen wie Art. 6 DSG (Art. 16 nDSG) oder Art. 10a DSG (Art. 9 nDSG) für behördliche Cloud-Lösungen gelten, unter Berücksichtigung des behördlichen bzw. grundrechtlichen Kontexts<sup>35</sup>.

Auch wenn das Datenschutzrecht den Behörden die Auftragsbearbeitung insbes. gemäss Art. 10a und 6 DSG erlaubt, muss m.E. bei staatlichen Personendatenbearbeitungen, die hoheitlich in grundrechtlich geschützte Positionen eingreifen, besonders darauf geachtet werden, dass mit der Nutzung von Cloud-Lösungen keine Schwächung der Betroffenenrechte bzw. der behördlichen Verpflichtungen einhergeht. Allerdings erzeugen behördliche Personendatenbearbeitungen, mit oder ohne Cloud, stets Risiken für die Betroffenen. Bei isolierter Betrachtung einer behördlichen Cloud-Lösung dürfte es somit regelmässig nicht möglich sein, zu beurteilen, ob namentlich dem Verhältnismässigkeitsgrundsatz entsprochen wird. Zudem sollte eine Schutzvorschrift im internationalen Verhältnis wie Art. 6 DSG ihrem Zweck entsprechend und systematisch so ausgelegt werden, dass sie einen optimalen Schutz der informationellen Selbstbestimmung und der Grundrechte der Betroffenen verwirklicht<sup>36</sup>. Deshalb dürften namentlich im Sinne der Prüfung der Verhältnismässigkeit Vergleiche zwischen verschiedenen Alternativen nötig sein (bisherige Lösung, andere Lösungen inkl. Teilumsetzungen von Cloud-Lösungen). Es lässt sich argumentieren, dass dem Verhältnismässigkeitsgrundsatz ein risikobasierter Ansatz

---

<sup>35</sup> So müssen auch die sich aus den einschlägigen Grundrechten, namentlich Art. 13 BV (und Art. 8 EMRK), ergebenden Anforderungen eingehalten werden. Abgesehen davon, dass das DSG verfassungsrechtliche Anforderungen aufnimmt und konkretisiert, entfalten sich diese auch im Rahmen der systematischen bzw. verfassungskonformen Auslegung, die von Art. 190 BV unberührt bleibt. Namentlich im Hinblick auf die Verhältnismässigkeit wohl ablehnend TRÜEB/ZOBL, S. 105, da Outsourcing-Lösungen zur Bedarfsverwaltung gehörten. Diese Überlegung gilt m.E. nicht, wenn bei der Cloud-Nutzung Personendaten bearbeitet werden, denn diesfalls liegt ein von der Behörde zu verantwortender Eingriff in die Grundrechte der Betroffenen vor. Es kann m.E. grundrechtlich keine « *Flucht in die Bedarfsverwaltung* » geben. Abgesehen davon gilt gerade der Verhältnismässigkeitsgrundsatz gestützt auf Art. 4 Abs. 2 DSG ohnehin.

<sup>36</sup> Vgl. aber neuerdings Ablehnung des risikobasierten Ansatzes für Art. 44 DSG durch die österreichische Datenschutzbehörde, Fn 33, D. 4. Spruchpunkt 2.c). Dort wird im Kern wie folgt argumentiert: Es gibt DSGVO-Bestimmungen, die ausdrücklich einen risikobasierten Ansatz normieren. Wo dies nicht geschieht, liegt ein bewusster Entsch. vor. Deshalb kann der risikobasierte Ansatz nicht analog auf Art. 44 DSGVO angewendet werden.

inhärent ist<sup>37</sup> und sich in diesem Sinne bei der datenschutzrechtlichen Beurteilung behördlicher Cloud-Nutzungen entfaltet<sup>38</sup>. Der Fokus liegt bei dieser Betrachtung verstärkt auf der Vermeidbarkeit von Risiken, einschliesslich des Verzichts auf gewisse Funktionalitäten bei Cloud-Services. Damit bleibt noch offen, wo allfällige absolute Grenzen des Risikos liegen, namentlich im Hinblick auf Rechte Betroffener. Auch ist mit der Bejahung eines risikobasierten Ansatzes noch nicht gesagt, welche Kriterien und welche Methode im konkreten Normkontext gesetzeskonform sind. So bleibt an dieser Stelle beispielsweise offen, inwieweit eine Verkettung von Massnahmen, die zu stets kleineren Wahrscheinlichkeiten führt, geeignet ist, um die Rechtskonformität im Rahmen von Art. 10a und 6 DSGVO sicherzustellen. Oder ob der behörden-spezifische Inhalt der ausgelagerten Personendaten und länderspezifische Behördeninteressen daran relevante Kriterien sind bzw. wie sie bewertet werden können. Schliesslich dürfte sich die Frage der Vermeidbarkeit von Risiken bei Cloud-Vorhaben als beschränkt justiziabel erweisen, beim an den gesetzlichen Aufgaben der Behörde zu messenden Bedarf wird auch die behördliche Autonomie zu achten sein.

Angesichts der bis zu einer gerichtlichen Klärung bestehenden Unsicherheiten ist zu hoffen, dass sich die im Rahmen der Cloud-Strategie durch die Bundesverwaltung vorgesehene rechtliche Klärung<sup>39</sup> sowie die in jedem Cloud-Projekt frühzeitig nötige rechtliche Beurteilung und Risikoanalyse hinreichend intensiv damit beschäftigen werden. Dazu gehört auch die Integration der genannten Aspekte in umfassende Datenschutz-Folgenabschätzungen<sup>40</sup>. Die Einhaltung der rechtlichen Vorgaben, hier insbesondere Art. 10a und 6 DSGVO bzw. Art. 9 und 16 nDSG, muss immer geprüft bzw. sichergestellt werden und ist von der Pflicht zu einer Datenschutz-Folgenabschätzung gem. Art. 22 nDSG zu unterscheiden. Die DSFA vermag auch nicht die gesetzlichen Anforderungen zu modifizieren, es handelt sich dabei um ein « *Instrument, um Risiken zu erkennen und zu bewerten, welche für die betroffene Person durch den Einsatz bestimmter Datenbearbeitungen entstehen können* »<sup>41</sup>.

---

<sup>37</sup> Vgl. in diese Richtung im EU-Kontext z.B. schon Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 30.5.2014, Ziff. 4. Zur *Erforderlichkeit* vgl. jüngst EDPS, Decision concerning the investigation into Frontex's move to the cloud (Case 2020-0584), 1.4.2022, Rz. 64 ff. und 36.

<sup>38</sup> Hier wird nicht näher auf die Frage der Horizontalwirkung eingegangen (vgl. Art. 35 Abs. 3 BV i.V.m. Art. 4 Abs. 2 DSGVO).

<sup>39</sup> Vgl. BUNDESRAT, Cloud-Strategie, Ziff. 5, MS5.

<sup>40</sup> Vgl. zum Instrument der DSFA insbes. Art. 22 nDSG. Zur Abgrenzung zwischen Risikoansatz und klassischem Risikomanagement vgl. Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt, White Paper Datenschutz-Folgenabschätzung, Eggenstein 2016, Ziff. 3.3.

<sup>41</sup> Vgl. BUNDESRAT, Botschaft DSGVO, BBl 2017, 7059.

## C. Bereichsspezifische Regelungen

Verschiedene bereichsspezifische Vorgaben für Bundesbehörden sind zwar nicht speziell auf Cloud-Services gemünzt, aber ebenfalls relevant.

Ein Beispiel dafür ist das Regierungs- und Verwaltungsorganisationsgesetz (RVOG, SR 172.010) und die ausführenden Verordnungen. So können die Bundesorgane ihre Geschäfte und den Schriftverkehr in einem Informations- und Dokumentationssystem führen, in welchem Zusammenhang Art. 57h Abs. 2 RVOG vorschreibt, dass zu Personendaten ausschliesslich Mitarbeitende des betreffenden Bundesorgans Zugang haben, und dies nur, soweit sie sie zur Erfüllung ihrer Aufgaben brauchen. Da es um die Verhinderung übermässiger Bearbeitungen innerhalb der Behörden geht, darf man aus dem Wortlaut nicht schliessen, die Bestimmung verbiete Outsourcing und mithin Cloud-Lösungen schlechthin. Die Regierungs- und Verwaltungsorganisationsverordnung (RVOV, SR 172.010.1) sowie die Verordnung über die elektronische Geschäftsverwaltung in der Bundesverwaltung (GEVER-Verordnung, SR 172.010.441) gehen darauf nicht näher ein, Art. 11 ff. GEVER-Verordnung enthalten aber einschlägige Informations- und Datenschutzvorgaben, wie z.B. die Verschlüsselungspflicht für « vertraulich » klassifizierte Informationen<sup>42</sup> sowie die Protokollierungspflicht. In die umgekehrte Richtung geht die ebenfalls das RVOG ausführende Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (VDTI, SR 172.010.58), die in Art. 11 ausdrücklich erlaubt, nicht allgemein zugängliche Daten externen Leistungserbringern zugänglich zu machen, wenn folgende Voraussetzungen erfüllt sind: Erforderlichkeit für die Leistungserbringung, Zustimmung der verantwortlichen Behörde oder der vorgesetzten Stelle, und *angemessene* vertragliche, organisatorische und technische Vorkehrungen, um eine weitere Verbreitung der Daten zu verhindern. Der vorgelagerte Entscheid für eine bundesinterne oder externe Leistungserbringung und die Auswahl erfolgt nach Art. 8 VDTI gestützt auf Marktanalysen und unter Berücksichtigung der Grundsätze der Opportunität, Interoperabilität, Wirtschaftlichkeit und Sicherheit. Es könnte missverstanden werden, dass im Hinblick auf bestehende Vorgaben des Datenschutz- und Informationsschutzrechts nur von einem *Grundsatz* der *Sicherheit* die Rede ist, der zu *berücksichtigen* ist. Da auf Stufe des RVOG keine Indizien für eine Relativierung datenschutzrechtlicher Anforderungen ersichtlich sind, hat diese ausführende Verordnungsregelung keine Auswirkung darauf. Die Wahl und Auswahl nach den genannten Kriterien hat im Rahmen der sonstigen rechtlichen Vorgaben namentlich des Daten- und Informationsschutzes zu erfolgen.

---

<sup>42</sup> Zu dieser informationsschutzrechtlichen Qualifikation siehe unten Ziff. IV.B.



Nach dem Gesagten kann aus Art. 11 Abs. 1 Bstb. c VDTI auch keine Begründung eines allgemein gültigen risikobasierten Ansatzes hergeleitet werden.

Ein weiteres Beispiel ist Art. 112a Abs. 1 Bundesgesetz über die direkte Bundessteuer (DBG, SR 642.11), welcher der Eidg. Steuerverwaltung vorschreibt, zur Erfüllung der gesetzlichen Aufgaben *ein Informationssystem zu betreiben*, welches besonders schützenswerte Personendaten über administrative und strafrechtliche Sanktionen enthalten kann, die steuerrechtlich wesentlich sind. Die Personendaten und zur Bearbeitung verwendeten Einrichtungen sind vor unbefugtem Verwenden, Verändern oder Zerstören zu schützen. Der Bundesrat hat soweit ersichtlich von seiner Kompetenz zum Erlass von Ausführungsbestimmungen, u.a. über die Organisation und den Betrieb des Informationssystems, bisher nicht Gebrauch gemacht. Dabei darf aus dem « Betreiben » nicht geschlossen werden, die ESTV selbst müsse den technischen Betrieb vollumfänglich selbst durchführen. Damit ist die Frage zumindest nach dieser Bestimmung nicht, ob ein Outsourcing möglich ist, sondern vielmehr, an wen und in welcher Ausprägung. Die einschlägigen Ausführungen in der Botschaft zur Bestimmung sind wenig konkret, die spürbare Sensibilität betreffend « Fremdzugriffe von unbefugten Dritten » mag bei der Gewichtung des Zugriffsrisikos eine Rolle spielen, hilft aber sonst auch nicht viel weiter<sup>43</sup>. Somit ergeben sich bei summarischer Betrachtung keine für Cloud-Lösungen relevanten konkreten Vorgaben.

Je nach Ergebnis können bereichsspezifische Vorschriften auch Auswirkungen auf den Einsatz von cloudbasierten Standardapplikationen bei der Bearbeitung der Inhalte haben, z.B. bei der Textverarbeitung. Die Standardapplikation darf m.E. nicht dazu führen, dass Vorgaben für die Fachapplikation unterlaufen werden. Das Zusammenspiel der rechtlichen Vorgaben für Fachapplikationen und Standardapplikationen sollte mithin bei der Evaluation von letzteren für die Bundesbehörden ebenfalls untersucht werden. Weiter ist bei den digitalen Cloud-Basisleistungen der Verwaltung zusätzlich das Risiko zu beurteilen, welches sich daraus ergibt, dass sämtliche zugehörigen Behörden Kunden des gleichen Cloud-Anbieters sind, sodass zu einer betroffenen Person möglicherweise Personendaten aus Datenbeständen verschiedener Behörden durch einen Cloud-Anbieter bearbeitet werden.

---

<sup>43</sup> Vgl. dazu auch Botschaft über die Schaffung und die Anpassung gesetzlicher Grundlagen für die Bearbeitung von Personendaten vom 25.8.1999, BBl 1999 9005 : « Die Datenschutz-Probleme stellen sich in allen Steuererlassen ähnlich. In jedem Fall gilt es zu verhindern, dass das Steuergeheimnis verletzt wird. Die Datensammlungen und elektronischen Datenverarbeitungssysteme der Steuerverwaltung müssen gegen jeglichen Fremdzugriff von unbefugten Dritten geschützt werden. »

## D. Cloud-Risiken im Überblick

Die Behörde bleibt als Auftraggeberin verantwortlich und muss die Rechtslage bzw. die Cloud-Lösung entsprechend gestalten, sich über die Umstände informieren, die Umsetzung kontrollieren, regelmässige Audits durchführen, falls nötig Pflichten durchsetzen oder gar vom Vertrag zurücktreten. Zu den zusätzlichen oder akzentuierten Datenschutzrisiken bei Cloud-Lösungen gehören insbesondere<sup>44</sup> :

*Standardisierung und Weiterentwicklung* : Ungünstige und unflexible Standard-Regelungen, die z.B. ausländisches Recht anwendbar erklären und ausländische Gerichtsstände vorsehen. Die massgeblichen vertraglichen Regelungen können auch auf verschiedene Dokumente verteilt sein, was die Komplexität erhöht und den Überblick erschwert, zumal sich die einzelnen Teile laufend verändern können, etwa aufgrund von Weiterentwicklung der Services. Ein Risiko in diesem Zusammenhang ist, dass die Risikobeurteilung selbst rasch überholt sein kann bzw. die aktuelle Situation und Entwicklung nicht mehr adäquat erfasst.

*Intransparenz* : Mangelhafte Gewissheit/Transparenz über den Ort der Datenbearbeitung (Serverstandorte), über weitere Beteiligte (Unterauftragsverhältnisse, Wartung der Infrastruktur) und über Informationssicherheitsmassnahmen (bei Datenverlust und -missbrauch). Innerhalb von Dienstanbieterketten können die Verantwortlichkeiten und geltenden Regeln für die unterschiedlichen Kategorien von Daten und Bearbeitungen verwässert werden. Auch kann der Überblick über den Standort oder die Standorte von Daten und damit die auf sie anwendbaren Rechtsordnungen inkl. Rechtsprechungen verloren gehen, was auch die Rechtsausübung durch Betroffene erschwert.

*Mangelhafte Vertraulichkeit und Integrität* : Dies betrifft nicht nur die von den Behörden bearbeiteten Inhaltsdaten, sondern auch die Mitarbeiterdaten, die namentlich im Rahmen der nötigen Nutzerkonten und Logging-Prozesse vom Cloud-Provider bearbeitet werden, sowie Randdaten, welche Informationen über die Nutzung der Infrastruktur enthalten. Vertraulichkeits- und Integritätsrisiken bestehen sowohl bei der Speicherung und Bearbeitung als auch aufgrund der Übertragung der Daten über das Internet, namentlich im Hinblick auf unbefugte Eingriffe während der Übermittlung, ausländische staatliche Internetüberwachung oder weitgehende ausländische Vorschriften zur Vorratsdatenspeicherung für die Strafverfolgung. Bei nicht ausreichend abgesicherter

---

<sup>44</sup> Die nachfolgende Aufzählung lehnt sich stark an PRIVATIM, Merkblatt Cloud-spezifische Risiken und Massnahmen vom 3.2.2022, <[http://www.privatim.ch/wp-content/uploads/2022/02/privatim\\_Cloud-Merkblatt\\_v3\\_0\\_20220203\\_def\\_DE-1.pdf](http://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def_DE-1.pdf)> (letztmals am 21.2.2022 besucht) sowie an EDPS, Leitlinien zur Nutzung von Cloud-Computing-Diensten durch die Organe und Einrichtungen der EU, 16.3.2018, Anhang 4 an und verwertet auch Erkenntnisse aus der Sichtung behördlicher Cloud-Projekte.

Mandantentrennung besteht die Gefahr, dass Dritte unautorisiert Daten einsehen oder manipulieren können. Spezifische IT-Sicherheitsrisiken betreffen u.a. die Authentizität des beauftragten Dienstes, Schwierigkeiten bei der Verwaltung der Schlüssel sowie bei der Verwaltung der Identitäten und Authentifizierungen.

*Interessenkonflikt* : Überschüssende Personendatenbearbeitungen wegen eigener kommerzieller Interessen des Anbieters. Dies betrifft auch die Nutzung von Daten der Mitarbeitenden der Behörde.

*Mangelhafte Kontrollmöglichkeiten* : Abgrenzung der Datenbearbeitungen auf der Cloud-Infrastruktur, Kontrolle rechtlicher Zusicherungen beschränkt möglich, ggf. nur nachgelagert mittels Revisionsberichten, mangelnde Einsicht in IKS des Anbieters.

*Geringeres Datenschutzniveau* : Bei Personendatenbearbeitungen in Gebieten, die aus schweizerischer Sicht kein gleichwertiges Datenschutzniveau aufweisen.

*Erschwerte Durchsetzbarkeit* : Erschwerte Durchsetzbarkeit der vertraglichen Verhaltens- und Sorgfaltspflichten sowie Gewährleistung von datenschutzrechtlichen Ansprüchen durch Betroffene (z.B. Auskunftsrecht, Sperrung, Löschung).

*Ausländischer Behördenzugriff* : Gefahr von Zugriffen ausländischer Behörden. Dabei ist zu differenzieren zwischen rechtlichen Zugriffen auf Cloud-Anbieter, die einer fremden Rechtsordnung aufgrund ihrer Sitzzugehörigkeit oder ihres Vollstreckungssubstrats unterstehen (wie beim CLOUD-Act) und faktischen Zugriffsmöglichkeiten, die sich allein auf politische Opportunität stützen (z.B. Geheimdienstprogramme).

*Verminderte Verfügbarkeit der Dienste* : Einschränkungen beim Internetzugang bei fehlerhafter Kapazitätsplanung, Ausfall des Dienstanbieters, Netzwerküberlastung, Cyberangriffe. Je weiter entfernt die Daten vom Verantwortlichen sind, desto mehr der dazwischenliegenden Elemente können versagen oder angegriffen werden. Sicherheitsmassnahmen müssen auf jedem Glied in der Kette stark sein. Risiken bei den Cloud-Anbietern selbst sind auch zu beachten, wobei Gegenmassnahmen etwa gegen die Gefahr des Datenverlusts, wie namentlich die verteilte Datenspeicherung, selbst datenschutzrechtliche Probleme erzeugen.

*Auflösungsprobleme, Lock-In* : Mangelhafte Regelung der Auflösung des Vertragsverhältnisses (Datenportabilität, Vernichtung der Daten), de facto Unmöglichkeit, Kündigungsmöglichkeiten rechtzeitig umzusetzen, um eine inakzeptable Änderung nicht hinnehmen zu müssen. Möglicher Untergang des Anbieters oder kommerzielle Übertragung auf andere Anbieter, die ggf. einer anderen Rechtsordnung unterstehen.

## E. Risikomindernde Massnahmen

Nachfolgend weise ich auf verschiedene rechtliche, technische und organisatorische Massnahmen hin, welche die spezifischen Cloud-Risiken reduzieren<sup>45</sup>. Inwieweit die genannten Massnahmen für eine zulässige Cloud-Nutzung ausreichend sind bzw. umgesetzt werden müssen, lässt sich nur gestützt auf sämtliche jeweils anwendbare Rechtsnormen beurteilen. Wenn es beispielsweise nicht gelingt, eine inländische Datenbearbeitung sicherzustellen, kann unter anderem eine wirksame Verschlüsselung der Personendaten als Lösungsansatz in Betracht kommen. Nicht aber, wenn es sich um Patientendaten im Rahmen des elektronischen Patientendossiers handelt, für die eine Datenhaltung in der Schweiz vorgeschrieben ist<sup>46</sup>.

*Anwendbares Recht und Gerichtsstand* : Wird schweizerisches Recht und ein schweizerischer Gerichtsstand vereinbart, erhöht dies die Wahrscheinlichkeit, dass vertragliche Pflichten des Cloud-Anbieters wirksam durchgesetzt werden können. Noch besser ist unter diesem Gesichtspunkt, wenn es sich um einen Anbieter mit Sitz in der Schweiz handelt<sup>47</sup>. Letzteres kann sich z.B. auch bei einem Konkurs des Anbieters günstig auswirken, weil sich damit die Chance des Zugriffs der verantwortlichen Behörde auf ihre Daten erhöht (Verfügbarkeit).

*Kontrollwahrung* : Die Behörden dürfen Personendaten nur im gesetzlichen Rahmen bearbeiten<sup>48</sup>. Dieser Rahmen wird durch eine zulässige Auftragsbearbeitung nicht erweitert<sup>49</sup>. Das Vertragswerk mit dem Cloud-Anbieter muss dies gewährleisten und darf dem Anbieter keine Freiräume gewähren, welche diesen partiell zu einem (ggf. Mit-)Verantwortlichen machen, denn dies würde den Rahmen eines Outsourcings im Rahmen der Auftragsbearbeitung verlassen. Das Risiko einer solchen, zu grossen Autonomie des Cloud-Anbieters kann z.B. entstehen, wenn er das Recht hat, Teile des Vertragswerks unilateral anzupassen, evtl. einschliesslich der Vorrangregelung zwischen Elementen des Vertragswerks. Unklare, komplexe, verschachtelte Vertragswerke mit dynamischen Verweisen tragen ebenfalls zu einer diffusen Rechtslage bei, welche es schwierig macht, den Cloud-Anbieter auf Pflichten bzw. Rechtspositionen zu behaften. Diesen Kontrollverlust steigern können zudem lückenhafte Regelungen, bei denen z.B. die Typen der erfolgenden Bearbeitungen und die Datenkategorien nicht umfassend geregelt sind. Gleiches gilt für eine ungenügende Beschreibung der zulässigen Bearbeitungszwecke, was dazu führen kann, dass dem Cloud-Anbieter Beurteilungsfreiräume zur Frage verbleiben, was noch zu

---

<sup>45</sup> In starker Anlehnung an die bereits in Fn. 44 hievore genannten Quellen.

<sup>46</sup> Art. 12 Abs. 5 EPDV (SR 816.11).

<sup>47</sup> Vgl. auch BAERISWYL, S. 120.

<sup>48</sup> Vgl. Art. 17 DSG ; Art. 34 nDSG.

<sup>49</sup> Art. 10a Abs. 1 Bstb. a DSG ; 9 Abs. 1 Bstb. a nDSG.

legitimen eigenen Zwecken zählt und was nicht, oder wo die Grenze zulässiger produktbezogener Datenanalysen verläuft. Eine möglichst detaillierte Regelung der Kategorien von Personendaten und Betroffenen ist im Übrigen auch eine Voraussetzung, um eine Beschränkung auf das Minimum der nötigen Datenbearbeitungen zu verwirklichen (Datenminimierung als Ausdruck der Verhältnismässigkeit). Um Regelungslücken zu vermeiden, sollte vertraglich unter Berücksichtigung der Art der Cloud-Services (IaaS, PaaS, SaaS) geregelt werden, welche Massnahmen durch den Cloud-Anbieter und welche durch die Behörde umzusetzen sind.

*Audits* : Die verantwortliche Behörde kann ihre Pflicht zur Überwachung der Cloud-Anbieter (und ihrer Unterauftragsbearbeiter) nur wirksam wahrnehmen, wenn sie vertraglich die Möglichkeit von genügenden eigenen oder durch Dritte durchgeführten Audits hat, was z.B. dann nicht der Fall ist, wenn der Cloud-Anbieter diese selber anordnen kann und Inhalt, Qualität sowie durchführende Prüfstelle bestimmt. Zur Wirksamkeit gehört auch eine Auditplanung. Soweit die Behörde über die nötigen Ressourcen verfügt, insbesondere allenfalls bei breit genutzten Standardprodukten, können in technischer Hinsicht nach Inbetriebnahme praktische Tests durchgeführt werden, welche den effektiven Datenfluss bei der Nutzung der Cloud-Lösung verfolgen. Mit Blick auf die ständige Weiterentwicklung der Produkte sollte zudem sichergestellt werden, dass alle Updates zur Kenntnis genommen und damit zusammenhängende allfällige Anpassungen vorgenommen werden.

*Auf Behörden zugeschnittene Vertragsanpassungen* : Bündeln Branchen oder Behörden ihre Kräfte, ist es u.U. einfacher möglich, Rahmenverträge mit Cloud-Providern auszuhandeln, die den gemeinsamen Anforderungen besser entsprechen. So hat die Schweizerische Informatikkonferenz (SIK) mit *Microsoft* ein Rahmenwerk für die öffentlichen Verwaltungen vereinbart, welches die Grundlage für Verträge des Kantons Zürich mit *Microsoft* bildete<sup>50</sup>. Weiter ist auch immer anzustreben, individualisierte ergänzende Regelungen zu vereinbaren, wie dies im genannten Beispiel des Kantons Zürich offenbar geschehen ist<sup>51</sup>. Die spezifischen Risiken von Cloud-Anbietern können rechtlich u.a. auch mit der Vereinbarung von hohen Konventionalstrafen gemildert werden.

*Ort der Datenbearbeitung* : Ausgangspunkt ist der Datenschutzstandard für eine Cloud-Infrastruktur in der Schweiz. Ist sie im Ausland, sind die Regeln für die Bekanntgabe von Personendaten ins Ausland zu beachten<sup>52</sup>. Zu bevorzugen sind hierbei Gebiete mit angemessenem Schutz. Aber auch dann ist namentlich das Risiko eines ausländischen behördlichen Zugriffs erhöht, beispielsweise, wenn eine ausländische Strafbehörde in einer Untersuchung nach

---

<sup>50</sup> KANTON ZÜRICH, Cloud-Lösungen, Ziff. 3.

<sup>51</sup> Vgl. Fn. 50 hievor.

<sup>52</sup> Vgl. hierzu und zum Folgenden auch die Hinweise oben Ziff. II.B.

dem anwendbaren nationalen Straf- und Strafprozessrecht auf Datenserver auf ihrem Territorium zugreift. Die *inter partes* geltende Vereinbarung mit dem Cloud-Anbieter wird man einer ausländischen Behörde zudem nicht entgegenhalten können<sup>53</sup>. Die vertraglichen Regelungen zum Ort der Datenbearbeitung sollten umfassend sein und sämtliche Kategorien von Daten und Bearbeitungen regeln, insbesondere auch Daten über die Nutzerinnen und Nutzer und solche, welche die Cloud-Anbieter aus der Nutzung der Dienstleistungen und Produkte gewinnen können. Die Regelungen haben sich auch auf den Beizug von Unterauftragsbearbeitern zu erstrecken.

*Verschlüsselung und andere technische Zugriffsschranken* : Personendaten sind sowohl bei der Übertragung (*in transit*), während der Speicherung (*at rest*) als auch bei der Bearbeitung i.e.S. (*in process*) einer Gefahr durch Datenverlust oder Datenmanipulation ausgesetzt. Während die Personendaten bei der Bearbeitung in aller Regel unverschlüsselt vorliegen, müssen sie zumindest bei der Übertragung und Speicherung verschlüsselt werden. Dabei ist ein nicht vertragskonformes Handeln des Cloud-Anbieters nie ganz auszuschliessen. Dies gilt aber auch für herkömmliches Outsourcing und ist keine Cloud-spezifische Problematik. Die Behörde muss sicherstellen, dass sie Kenntnis über die kryptographischen Mittel und deren Anwendung hat. Bedeutsam ist in diesem Zusammenhang eine auf anerkannten Normen, Verfahren und Methoden beruhende Schlüsselverwaltung. Je nach angewandeter Verschlüsselungstechnik ist der Schutz der Daten unterschiedlich hoch zu bewerten. Besonders wirksame Ansätze, wie namentlich *Hold Your Own Key (HYOK)*, auch Totalverschlüsselung bezeichnet, lassen sich oftmals nur mit viel Aufwand und hohen Kosten realisieren oder führen zu Funktionseinbussen. Von der Behörde geschaffene und verwaltete Schlüssel im Sinne des *Bring Your Own Key (BYOK)*-Ansatzes bieten hingegen einen deutlich geringeren Schutz, weil der Verschlüsselungsvorgang innerhalb der Cloud erfolgt. Der Datenschutz während der Bearbeitung hingegen soll durch *Confidential Computing*<sup>54</sup> gewährleistet werden. Dies wird dadurch erreicht, dass die Daten während der Verarbeitung in einer hardwarebasierten, vertrauenswürdigen Ausführungsumgebung (*Trusted Execution Environment, TEE*) isoliert werden. Eine TEE-Hardware stellt einen abgesicherten Container bereit und schützt so einen Teil des Prozessors und Speichers der Hardware. *Confidential Computing* ist bereits heute verfügbar und kann verwendet werden<sup>55</sup>. Welche Massnahmen jedoch für einen angemessenen technischen Schutz nötig sind, lässt sich wiederum nur im konkreten Anwendungsfall und unter Würdigung aller Faktoren beurteilen.

---

<sup>53</sup> Vorbehalten wird die Prüfung allfälliger völkerrechtlicher Schutznormen betreffend Personendaten im Verantwortungsbereich staatlicher Behörden und ihre praktische Wirksamkeit.

<sup>54</sup> Vgl. hierzu z.B. EIGENMANN, passim.

<sup>55</sup> Vgl. zu den aktuellen Entwicklungen RUSSINOVICH *et al.*, passim.

Wegen der raschen technologischen Entwicklung muss die Situation zudem periodisch neu evaluiert werden.

*Support-Regelungen* : Eine typische Konstellation, in der seitens Cloud-Anbieter ein Klartext-Zugriff droht, ist der Support bei technischen Problemen. Das Risiko kann auf verschiedenen Ebenen angegangen werden : Vertraglich, indem eine Zusicherung eingeholt wird, dass der Support ohne Klartext-Zugriff erfolgt. Prozedural, indem bei einem nötigen Klartext-Zugriff eine dafür zuständige Person der Behörde dies mitverfolgt. Und auch technisch, etwa indem ein nötiger Zugriff auf Klartext-Daten nur nach erfolgter Freigabe im Einzelfall durch die Behörde möglich ist<sup>56</sup>.

*Geheimhaltung und Zweckbindung* : Geheimhaltungs- und Zweckbindungsverpflichtungen tragen dazu bei, den Kreis der zugriffsberechtigten Personen auf das nötige Mass zu beschränken und zu verhindern, dass die Daten zu anderen Zwecken als den behördlichen bearbeitet werden<sup>57</sup>. Die Regelungen müssen sich auch auf die regelmässig ebenfalls vom Cloud-Anbieter bearbeiteten Personendaten der behördlichen Mitarbeitenden als Nutzerinnen und Nutzer erstrecken. Eine weitere Massnahme liegt darin, als Behörde die Zugangsrechte selbst zu verwalten.

*Subcontracting* : Nach Art. 9 Abs. 3 nDSG darf der Auftragsbearbeiter die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen. Damit die Genehmigung ihren Zweck erfüllen kann, muss sich der Verantwortliche ausreichend detaillierte Informationen zu den Unterauftragsbearbeitern ausbedingen. Die Informationen sollten die Subunternehmer nicht nur identifizieren, sondern auch beschreiben, für welche Dienstleistungen oder Produkte sie beigezogen werden und welche Datenkategorien wie und wo bearbeitet werden, mit welchen Massnahmen zur Gewährleistung der Datensicherheit und des Datenschutzes. Die Cloud-Anbieter sollten verpflichtet werden, den geplanten Beizug neuer Subunternehmen im Voraus anzuzeigen. Die speziellen oder generellen Genehmigungen sollten so erfolgen, dass keine Lücken für bestimmte Arten von Daten und ihre Bearbeitung entstehen. Optimal ist es, wenn die verantwortliche Behörde inakzeptable Unterauftragsbearbeiter ablehnen kann. Soweit dies nicht möglich ist, kann man sich allenfalls mit einem Kündigungsvorbehalt begnügen. Damit dies als risikomindernde Massnahme ins Gewicht fällt, braucht es aber realisierbare Ausstiegsszenarien.

*Information bei Datenschutzverletzungen* : Nach nDSG ist der Verantwortliche dazu verpflichtet, Verletzungen der Datensicherheit mit hohem Risiko dem EDÖB zu melden, der Auftragsbearbeiter muss dem Verantwortlichen gar jede

---

<sup>56</sup> Eine solche Lösung ist die sogenannte « *Microsoft Customer Lockbox* ».

<sup>57</sup> Vgl. auch BAERISWYL, S. 119.

Verletzung melden<sup>58</sup>. Unter Umständen sind auch die Betroffenen zu informieren<sup>59</sup>. Dabei handelt es sich nicht um Cloud-spezifische Verpflichtungen, aber insbesondere der regelmässige Einsatz von zahlreichen Unterauftragsbearbeitern bei Cloud-Lösungen macht eine wirksame Regelung über alle Stufen hinweg wichtig. Ungeachtet einer direkten gesetzlichen Verpflichtung des Cloud-Anbieters<sup>60</sup> sollten deshalb Informationspflichten vertraglich geregelt werden<sup>61</sup>.

*Prozess bei Beendigung des Vertrags* : Zu einer Beendigung kann es aus verschiedenen Gründen kommen, etwa, weil ein Anbieter künftig seine Leistung nicht mehr anbietet oder anbieten kann, z.B. wegen Konkurs. Oder weil die Behörde eine Veränderung weder hinnehmen noch verhindern kann und deshalb kündigt (z.B. inakzeptable Ausweitung der Unterauftragsbearbeiter). Soweit das öffentliche Organ die bislang im Rahmen der Cloud bearbeiteten Daten weiter braucht, muss schon im Voraus sichergestellt werden, dass die Daten verfügbar bleiben. Bereits vor dem Entscheid für die Cloud-Lösung muss ein Prozess geplant werden, um innert Kündigungsfrist eine alternative Lösung finden oder schaffen zu können. Dieser Prozess muss regelmässig neu evaluiert werden, damit er im Zeitpunkt einer allfälligen Kündigung noch umsetzbar ist. Werden die Daten nicht mehr benötigt und brauchen nicht migriert zu werden, ist ihre Löschung sicherzustellen.

*Regelmässige Risikoprüfung* : Zu den Charakteristika von Cloud-Services gehört, dass sie ständig weiterentwickelt werden. Die Risikobeurteilung als Instrument hat deshalb nur eine begrenzte zeitliche Wirksamkeit. Mit regelmässigen Neuevaluationen kann das Risiko gesenkt werden, von einer inzwischen veränderten Gefahrenlage überrascht zu werden.

*Zertifizierung betreffend Datenschutz* : Zertifizierungen können die Einhaltung bestimmter Standards beim Umgang mit Personendaten sowie betreffend die Informationssicherheit nachweisen. In der Schweiz können Auftragsbearbeiter nach dem nDSG ihre Systeme, Produkte und Dienstleistungen zertifizieren lassen<sup>62</sup>. Als Teil der nach DSG bzw. nDSG ergriffenen Massnahmen können auch die in der Praxis wichtigen ISO-Normen Gegenstand einer Zertifizierung sein<sup>63</sup>. Inzwischen gibt es auch eine ISO-Norm für Public Clouds<sup>64</sup>. Infolge der raschen technologischen Weiterentwicklung sind Zertifizierungen jeweils

---

<sup>58</sup> Art. 24 Abs. 1 und 3 nDSG.

<sup>59</sup> Art. 24 Abs. 4 und 5 nDSG.

<sup>60</sup> Vgl. Art. 3 Abs. 1 nDSG.

<sup>61</sup> Über das gesetzliche Minimum hinaus, vgl. Art. 24 Abs. 2 nDSG, z.B. mit detaillierterer Beschreibung des Vorfalles, und auch zeitlich klarer als Art. 24 Abs. 1 nDSG.

<sup>62</sup> Art. 13 Abs. 1 nDSG.

<sup>63</sup> Vgl. ROSENTHAL, Das neue Datenschutzgesetz, N 180.

<sup>64</sup> Vgl. ISO/IEC 27018:2019, Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.



rasch überholt und müssen periodisch erneuert werden. Dennoch sind sie in der Praxis bedeutsam und können eine Bedingung sein, um einen Zuschlag in einer Ausschreibung zu erhalten<sup>65</sup>.

*Service Level Agreement* : In einem *Service Level Agreement (SLA)* werden die vom Cloud-Anbieter zu erbringenden Leistungen und Abrechnungen vereinbart, wodurch die Dienstgüte zwischen dem Anbieter und der Behörde vertraglich festgelegt wird. Dabei wird der Vertrag aus der Sicht der Behörde beschrieben und der Cloudanbieter hält im Gegenzug die Eigenschaften, den Umfang und die Qualität seiner Leistungen in einem Katalog fest. Neben den Verfügbarkeiten der Leistungen sind in einem SLA ebenfalls die Ressourcenzuteilungen, die Verfügbarkeitsquote, die Reaktions- und Wartungszeiten, die Problemlösungszeiten sowie Vereinbarungen über Sicherheiten, Priorisierungen, Garantien und Abrechnungsmodelle enthalten. Die Vereinbarungen werden über einen *Key Performance Indikator (KPI)* festgehalten und gemessen. Zusätzlich werden in einem SLA Regeln festgehalten, die bei einem Verstoß des Anbieters gegen die zugesagten Leistungen Rechtsfolgen bzw. bei einer Nichteinhaltung der Verfügbarkeit Konventionalstrafen nach sich ziehen.

## F. Fazit

Bei behördlichen Cloud-Nutzungen handelt es sich um Auftragsbearbeitungen, die insbesondere die datenschutzrechtlichen Anforderungen von Art. 10a und 6 DSGVO erfüllen müssen. Daneben sind weitere DSGVO-Bestimmungen und bereichsspezifische Vorschriften zu berücksichtigen. Spezifische Anforderungen an Fachapplikationen müssen beim Einsatz von cloudbasierten Standardapplikationen zur Bearbeitung von deren Inhalten berücksichtigt werden.

In der Behördenpraxis scheint sich zunehmend ein risikobasierter Ansatz durchzusetzen, um die Rechtmässigkeit von Cloud-Lösungen zu beurteilen und über ihre Umsetzung zu entscheiden. Der risikobasierte Ansatz, der sich bereits im geltenden DSGVO findet, war die erste Leitlinie der Totalrevision hin zum nDSG vom 25. September 2020. Er prägte differenzierte Regelungen für Personendatenbearbeitungen, je nach Risiko für die Betroffenen, und manifestiert sich in Bestimmungen, die explizit risikobasierte Vorgaben machen. Darüber hinaus realisiert sich der risikobasierte Ansatz im Rahmen datenschutzrechtlicher Grundprinzipien, namentlich des Verhältnismässigkeitsgrundsatzes, und allgemein als Auslegungselement datenschutzrechtlicher

---

<sup>65</sup> Vgl. z.B. die Ausschreibung « 20007 608 Public Clouds Bund », die u.a. das Eignungskriterium EK04 enthielt, wonach der Anbieter über bestimmte Zertifizierungen verfügen musste.

Bestimmungen. Damit ist auch gesagt, dass durch Auslegung der jeweils anwendbaren Rechtsnormen nach anerkannter Auslegungsmethodik ermittelt werden muss, ob und inwiefern sich ein risikobasierter Ansatz entfalten kann. Bisher gibt es in der Schweiz keine einschlägige, für Cloud-Nutzungen relevante Gerichtspraxis. Die für Bundesbehörden relevanten Verlautbarungen des EDÖB zu Art. 6 DSG schliessen einen risikobasierten Ansatz nicht explizit aus, formulieren aber hohe Anforderungen.

Für behördliche Cloud-Nutzungen kommt m.E. dem grundrechtlichen Kontext eine besondere Bedeutung zu. Da eine isolierte Betrachtung einer Cloud-Lösung kaum eine Beurteilung zulässt, namentlich im Lichte der Verhältnismässigkeit, braucht es vergleichende Betrachtungen zwischen alternativen Lösungen mit einer Gesamtwürdigung der Umstände. Dem dürfte ein risikobasierter Ansatz inhärent sein, der sich über eine teleologische und systematische Auslegung auch im Rahmen von Art. 10a und 6 DSG entfalten kann. Damit bleibt noch offen, wo allfällige absolute Grenzen des Risikos grenzüberschreitender Übermittlungen liegen, namentlich im Hinblick auf Rechte Betroffener. Auch dürfte sich die Frage der Vermeidbarkeit von Risiken bei Cloud-Vorhaben als beschränkt justiziabel erweisen, beim an den gesetzlichen Aufgaben der Behörde zu messenden Bedarf wird auch die behördliche Autonomie zu achten sein.

Den bei Cloud-Risiken erkennbaren neuen oder akzentuierten Risiken kann mit einer Vielzahl von Massnahmen entgegengewirkt werden. Ob damit den datenschutzrechtlichen Anforderungen genügt werden kann und welche der Massnahmen zu ergreifen sind, kann nicht generell beurteilt werden, sondern nur bezogen auf ein konkretes Vorhaben. Die zahlreichen verfügbaren Massnahmen und das Entwicklungspotential im Bereich des *Confidential Computing* sollten m.E. bei der Würdigung der rechtlichen Anforderungen an behördliche Cloud-Nutzungen genügend berücksichtigt werden, nicht zuletzt im Rahmen einer geltungszeitlichen Auslegung.

### **III. Amtsgeheimnis**

#### **A. Einleitung**

Mit « Amtsgeheimnis » ist gemeinhin die Pflicht von Angestellten der Verwaltung oder von Behördenmitgliedern gemeint, die ihnen in dieser Stellung bekanntgewordenen, nicht öffentlich zugänglichen oder bekannten Tatsachen geheim zu halten. Werden vor allem die Strafbestimmungen zum

(Berufs- und) Amtsgeheimnis behandelt<sup>66</sup> und interessiert insbesondere, unter welchen Voraussetzungen die Strafbarkeit entfällt, namentlich der (Eventual-) Vorsatz<sup>67</sup>, dann droht ein unvollständiges Bild. Denn es gibt diverse Erlasse, welche amtliche Geheimhaltungspflichten regeln, wie das Bundespersonalgesetz oder etwa das Bundesgesetz über die direkte Bundessteuer, welches bereichsspezifisch das « Steuergeheimnis » als qualifiziertes Amtsgeheimnis vorsieht. Aus behördlicher Sicht sollte m.E. die Optik massgeblich sein, das Amtsgeheimnis zu wahren bzw. dessen objektive Verletzung zu vermeiden, und nicht die Vermeidung der Strafbarkeit. Bei dieser Betrachtung steht die strafrechtliche Sanktionierung der Amtsgeheimnisverletzung von Art. 320 StGB neben den verwaltungsrechtlichen Amtsgeheimnispflichten und verstärkt diese<sup>68</sup>. Geht es beispielsweise um Steuerdaten natürlicher Personen betreffend die direkte Bundessteuer, müssen insbesondere die einschlägigen personalrechtlichen Vorschriften über das allgemeine Amtsgeheimnis<sup>69</sup>, Art. 110 DBG zum Steuergeheimnis als auch Art. 320 StGB<sup>70</sup> zur Anwendung gebracht werden. Eine mögliche Verletzung des Amtsgeheimnisses ist im Übrigen in zweierlei Hinsicht zu prüfen : Einerseits durch planmässige Nutzung der Cloud-Services bzw. Übermittlung und weitere Bearbeitung von Daten an bzw. durch den Cloud-Anbieter und sein Personal sowie allfällige Subunternehmen, andererseits durch unplanmässige Bearbeitung durch Dritte<sup>71</sup>.

Nachfolgend steht das Thema des strafrechtlichen Schutzes des Amtsgeheimnisses durch Art. 320 StGB im Zentrum. Exemplarisch und summarisch wird vorab auf zwei weitere Geheimnisregelungen hingewiesen. So konkretisiert die Geheimhaltungspflicht des Art. 22 BPG die Treue- bzw. Sorgfalts- und

<sup>66</sup> Vgl. bspw. MÉTILLE, passim ; betreffend das Berufsgeheimnis vgl. bspw. SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 25 ff.

<sup>67</sup> Vgl. bspw. ROSENTHAL, Cloud, Rz 80.

<sup>68</sup> LOCHER, N 8 zu Art. 110 DBG, mit weiteren Hinw., auch auf a.M. : « das Amtsgeheimnis lässt sich nicht auf Art. 320 StGB abstützen, sondern diese Bestimmung sanktioniert nur Verletzungen einer – auf anderer Grundlage beruhenden – Geheimhaltungspflicht ». Diese Auffassung wurde allerdings inzwischen durch BGE 142 IV 65, E. 5.2 verworfen, wonach die Pflicht zur Geheimhaltung keine beamtenrechtliche oder sonstige Norm erfordert, die das ausdrücklich vorsieht. Im vorliegenden Zusammenhang ist dies irrelevant. Entscheidend ist, dass die verwaltungsrechtlichen Amtsgeheimnisregelungen ohnehin eine eigenständige Bedeutung haben und in ihrem Anwendungsbereich für Behörden massgeblich sind.

<sup>69</sup> In erster Linie kantonales Recht, da die kantonalen Steuerbehörden die direkte Bundessteuer veranlagern und beziehen. Soweit die ESTV betroffen ist, kommt das BPG zur Anwendung.

<sup>70</sup> Auf weitere anwendbare Bestimmungen, wie z.B. Art. 321 StGB oder Art. 35 DSG, wird hier nicht näher eingegangen. Letztere Bestimmung ist ebenfalls auf Behörden und im Rahmen von Abs. 2 auf Auftragsbearbeiter nach Art. 10a DSG anwendbar, vgl. BSK DSG-NIGGLI/MAEDER, Fn. 9, Art. 35, N 12 ff. Art. 62 nDSG erfasst zudem neu alle Geheimnisse, vgl. BBl 2017 7102.

<sup>71</sup> Zu denen auch unbefugte Mitarbeitende des Cloud-Anbieters zählen.

Interessenwahrungspflicht des Art. 20 BPG<sup>72</sup>. Die Angestellten des Bundes unterstehen dem Berufsgeheimnis, dem Geschäfts- sowie dem Amtsgeheimnis. Die geschützten Geheimnisse können inhaltlich weiter gehen als die vom StGB erfassten, so dass nicht jede Verletzung von Art. 22 BPG zwingend auch eine strafbare Geheimnisverletzung ist<sup>73</sup>. Das Gesetz definiert den Geheimnisbegriff nicht näher, gemäss der ausführenden Verordnungsbestimmung in der BPV<sup>74</sup> sind die Angestellten « zur Verschwiegenheit über berufliche und geschäftliche Angelegenheiten verpflichtet, die nach ihrer Natur oder auf Grund von Rechtsvorschriften oder Weisungen geheim zu halten sind »<sup>75</sup>, womit sowohl Personendaten als auch andere Informationen betroffen sein können. Was ein zu wahrendes Geheimnis ist, wird somit vor allem in bereichsspezifischen Gesetzen geregelt ; das Bundespersonalrecht regelt es nur, soweit es direkt mit dem Arbeitsverhältnis verknüpft ist<sup>76</sup>. Diesbezüglich sind insbesondere Art. 27 ff. BPG zur (Personen-) Datenbearbeitung und die BPDV<sup>77</sup> einschlägig, u.a. mit etlichen Regelungen zu den eingesetzten Informationssystemen. Unter Vorbehalt vertiefter Prüfung ist somit der allgemeinen Regelung des Amtsgeheimnisses in Art. 22 BPG i.V.m. Art. 94 Abs. 1 BPV wenig Konkretes zu den Anforderungen für technische Umsetzungen, dem Outsourcing und mithin Cloud-Nutzungen zu entnehmen. Jedenfalls kann eine behördliche Nutzung von Cloud-Lösungen nicht gestützt darauf generell ausgeschlossen werden. Eine grössere Chance auf greifbare und auch für Cloud-Lösungen relevante Vorgaben besteht bei den bereichsspezifischen Regelungen, namentlich auf Verordnungsstufe, wie insbes. das Beispiel der BPDV zeigt.

Ein weiteres Beispiel ist das Steuergeheimnis, welches Gegenstück bildet zur weitreichenden Offenbarungspflicht der steuerpflichtigen Person und oft als « qualifiziertes Amtsgeheimnis » charakterisiert wird<sup>78</sup>. Es schützt in erster Linie die Privatsphäre der steuerpflichtigen Person, fördert ein im öffentlichen Interesse liegendes Vertrauen zwischen steuerpflichtiger Person und Steuerbehörde und dient mittelbar der Sachverhaltsermittlung, indem es auskunftspflichtigen Dritten die pflichtgemässen Offenlegungen erleichtert<sup>79</sup>. Da sich Steuerdaten naturgemäss auf Steuersubjekte beziehen und nach dem DBG

---

<sup>72</sup> HELBLING, N 5 f. zu Art. 22.

<sup>73</sup> HELBLING, N 7 zu Art. 22.

<sup>74</sup> Bundespersonalverordnung (BPV ; SR 172.220.111.3).

<sup>75</sup> Art. 94 Abs. 1 BPV.

<sup>76</sup> HELBLING, N 9 f., 24 zu Art. 22.

<sup>77</sup> Verordnung über den Schutz von Personendaten des Bundespersonals (BPDV ; SR 172.220.111.4).

<sup>78</sup> LOCHER, N 35 zu Einführung zu Art. 109 ff. DBG.

<sup>79</sup> LOCHER, N 10 zu Art. 110 DBG ; Analoges gilt im StHG, vgl. ZWEIFEL/HUNZIKER, in : ZWEIFEL/BEUSCH (Hrsg.), Art. 39 StHG N 3.

darunter natürliche und juristische Personen zu verstehen sind<sup>80</sup>, handelt es sich dabei gleichzeitig um Personendaten i.S. von Art. 3 Bstb. a DSGVO<sup>81</sup>. Geheim sind alle vom Geheimnisträger der Steuerbehörde bekannt gegebenen oder vom Geheimnisträger bei der amtlichen Tätigkeit erfahrenen Tatsachen, es gilt der materielle Geheimnisbegriff<sup>82</sup>. Die Geheimhaltungspflicht erstreckt sich nicht nur auf alle mit dem Vollzug des DBG befassten Behörden der Steuererhebung, Rechtsmittel-, Steuerstraf- und Erlassbehörden, sondern auch auf die *beigezogenen* Personen<sup>83</sup>. Für alle diese Personen gilt dabei das « Käseglockenprinzip », d.h. zwischen ihnen ist das Steuergeheimnis grds. aufgehoben<sup>84</sup>. Dritten, die ausserhalb der « Käseglocke » stehen, dürfen die Geheimnisse nur unter bestimmten Voraussetzungen offenbart werden, namentlich bei einer gesetzlichen Grundlage im Bundesrecht im Sinne von Gesetzen oder Verordnungen der Bundesversammlung, sofern diese ausdrücklich oder sinngemäss zur Durchbrechung des Steuergeheimnisses ermächtigen<sup>85</sup>. Dem Wortlaut lässt sich nicht entnehmen, ob unter den beigezogenen Personen auch Cloud-Anbieter mit ihrem berechtigten Personal verstanden werden können. Es wird an der steuerrechtlichen Praxis und Lehre sein, dies vertieft zu prüfen. *Prima vista* lässt sich allein aus dem Umstand, dass geheime, mitunter besonders schützenswerte Personendaten<sup>86</sup> betroffen sind, nicht generell die Nutzung von bundesexternen Cloud-Services ausschliessen. Auch, dass der Gesetzgeber beim Bezug wohl eher an punktuelle Einsätze und nicht an die dauernde Bereitstellung von Cloud-Services gedacht hatte, schliesst m.E. nicht *a priori* eine solche Interpretation aus. Die Frage verlagert sich damit in die konkrete Ausgestaltung. Hier wie beim allgemeinen Amtsgeheimnis lässt sich aus den rudimentären gesetzlichen Regelungen kaum viel dafür gewinnen.

---

<sup>80</sup> Abgesehen von speziellen Konstellationen, vgl. Art. 1 i.V.m. 11 DBG.

<sup>81</sup> Nach dem i.K.-Treten des nDSG trifft dies nur noch betreffend natürliche Personen zu, vgl. Art. 5 Bstb. a nDSG.

<sup>82</sup> LOCHER, N 27 zu Art. 110 DBG.

<sup>83</sup> LOCHER, N 18 f. zu Art. 110 DBG, der bspw. Informatiker nennt.

<sup>84</sup> LOCHER, N 3 zu Art. 110 DBG.

<sup>85</sup> LOCHER, N 32 ff. zu Art. 110 DBG, der bei bloss allgemeinen Amts- und Rechtshilfeverpflichtungen eine Abwägung der öffentlichen und privaten Interessen i.S. einer Verhältnismässigkeitsprüfung zulässt.

<sup>86</sup> Steuererklärungen enthalten z.B. Angaben über die Konfession, Krankheitskosten oder Vergabungen (die Rückschlüsse auf weltanschauliche oder politische Ansichten zulassen).

## B. Art. 320 StGB

Das *Amtsgeheimnis* in Art. 320 StGB schützt neben dem öffentlichen Interesse an einer funktionierenden staatlichen Verwaltung auch Individualinteressen<sup>87</sup>. Wegleitender Gedanke dabei ist, dass wenn Privatpersonen den Behörden Informationen aus dem Geheim- oder Privatbereich geben müssen, dieser Eingriff nicht weiterreichen darf, als nötig<sup>88</sup>. Nach Art. 320 Ziff. 1 StGB strafbar macht sich, « [w]er ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung wahrgenommen hat ». Es handelt sich um ein echtes Sonderdelikt, Täter können nur Behördenmitglieder und Beamte sein.

Die notwendige *Tätereigenschaft* – Behördenmitglieder oder Beamte<sup>89</sup> – wird nicht eingehend behandelt, weil ich mich auf die Bundesorgane und insbesondere auf die Bundesverwaltung fokussiere. Deren Mitglieder und Angestellte kommen als Täter offensichtlich in Frage. Im Übrigen ist aber nicht das personalrechtliche Kriterium des Anstellungsverhältnisses entscheidend, sondern die Ausübung von Funktionen im Dienst der Öffentlichkeit, so dass sowohl institutionelle als auch funktionelle Beamte erfasst sind<sup>90</sup>. Externe Hilfspersonen im Bereich IKT, die Dienstleistungen für die Verwaltung erbringen, fallen indes nicht in den Täterkreis von Art. 320 Ziffer 1 StGB<sup>91</sup>. Dies wird sich mit dem Inkrafttreten der jüngsten Revision der Bestimmung ändern, welche den Täterkreis um die Hilfspersonen erweitert<sup>92</sup>.

Es gilt der sog. *materielle Geheimnisbegriff*, bei dem es nicht darauf ankommt, ob die Tatsache von der Behörde geheim erklärt wurde: « Als Geheimnis gilt jede Tatsache, die nur einem beschränkten Personenkreis bekannt ist und an deren Geheimhaltung der Geheimnisherr ein berechtigtes Interesse hat »<sup>93</sup>. Dies trifft beispielsweise zu für die in einem polizeilichen Informationssystem erfasste persönliche Wohnadresse, wenn sie für Private gesperrt ist und die Bekanntgabe einen Interessennachweis erfordert<sup>94</sup>. Zurückgedrängt wird der Geheimnisbegriff durch das Öffentlichkeitsprinzip, auf Bundesebene namentlich

---

<sup>87</sup> Über Art. 320 StGB hinaus gibt es weitere Bestimmungen im StGB, die Einzelaspekte von Geheimhaltungspflichten regeln, vgl. hierzu BSK StGB-OBERHOLZER, Art. 320 N 2.

<sup>88</sup> BSK StGB-OBERHOLZER, Art. 320 N 4 ; PK StGB-TRECHSEL/VEST, Art. 320 N 1.

<sup>89</sup> Vgl. die Legaldefinition für « Beamte » in Art. 110 Abs. 3 StGB.

<sup>90</sup> Vgl. hierzu BSK StGB-OBERHOLZER, Art. 320 N 6 f.

<sup>91</sup> BUNDESRAT, Botschaft ISG, BBl 2017 3077.

<sup>92</sup> BBl 2020 10010 ; AS 2022 232.

<sup>93</sup> BSK StGB-OBERHOLZER, N 8 zu Art. 320.

<sup>94</sup> BSK StGB-OBERHOLZER, N 8 zu Art. 320, m.Hw. auf die Rechtsprechung des BGer.

mit dem BGÖ<sup>95</sup>. Was in Anwendung des BGÖ öffentlich zugänglich ist, ist kein Geheimnis<sup>96</sup>. Personendaten müssen allerdings vor der Einsichtnahme anonymisiert werden, und wo dies nicht möglich ist, sind Zugangsgesuche nach dem DSG zu beurteilen<sup>97</sup>. Wenn anonymisierte oder pseudonymisierte bzw. verschlüsselte – für den Cloud-Anbieter und andere Dritte nicht reidentifizierbare – Personendaten in einer Cloud bearbeitet werden, liegen aus Sicht des Empfängers keine Personendaten vor und ist das DSG nicht mehr anwendbar<sup>98</sup>. Wohl aber kann es sich bei verbleibendem, unpersönlichem Informationsgehalt um Geheimnisse im Sinne von Art. 320 StGB handeln, der sich nicht auf Personendaten beschränkt. Auf diese Konstellation wird aus einem datenschutzrechtlichen Blickwinkel nicht näher eingegangen. Nach dem Gesagten müssen behördlich bearbeitete Personendaten unter Vorbehalt des BGÖ als Geheimnisse im Sinne von Art. 320 StGB qualifiziert werden. Wenn Behördenmitglieder und Verwaltungsangestellte im Rahmen ihrer gesetzlichen Aufgaben Personendaten bearbeiten, liegt ferner der *Kausalzusammenhang* zwischen der Kenntnis<sup>99</sup> von der Tatsache und der amtlichen Funktion typischerweise vor.

*Offenbart* wird eine geheime Tatsache, indem sie einer nicht ermächtigten Drittperson zur Kenntnis gebracht wird oder deren Kenntnisnahme ermöglicht wird<sup>100</sup>. Damit ist zweierlei näher zu untersuchen, der Kreis der ermächtigten Personen und die Bekanntgabe. Zunächst ist festzuhalten, dass der Kreis der ermächtigten Personen nicht mit « Bundesorgan » oder « Bundesverwaltung » übersetzt werden darf, das Amtsgeheimnis gilt auch innerhalb der einzelnen Verwaltungsweige<sup>101</sup>. Es reicht also nicht, dem Amtsgeheimnis zu unterstehen, um in den Kreis der Berechtigten zu gelangen<sup>102</sup>. Mit MÉTILLE kann für das

<sup>95</sup> Die Öffentlichkeit kann sich auch aus anderen Regelungen ergeben, z.B. wenn ein Steuerregister nach kantonalem Recht öffentlich ist und voraussetzungslos eingesehen werden kann. Die darin enthaltenen Personendaten sind keine Geheimnisse i.S.v. Art. 320 StGB.

<sup>96</sup> Das führt zu einer gewissen Rechtszersplitterung, indem der Geheimnisbegriff des bundesrechtlichen StGB im Anwendungsbereich der kantonalen Öffentlichkeitsgesetze von der kantonalen Gesetzgebung mitdefiniert wird. Wieweit das de facto zu spürbaren Unterschieden führt, kann hier nicht näher geprüft werden.

<sup>97</sup> Art. 9 BGÖ i.V.m. Art. 19 DSG. Der Verweis des BGÖ ins DSG bezieht sich praxisgemäss spezifisch auf Art. 19 Abs. 1<sup>bis</sup> DSG.

<sup>98</sup> Das DSG ist aber immer auf die Anonymisierung selbst sowie bei Pseudonymisierung bzw. Verschlüsselung auf diejenigen anwendbar, für die eine Reidentifikation weiterhin möglich ist.

<sup>99</sup> Einer näheren Klärung vorbehalten bleibt u.a. die Frage, was im Kontext von IT-Systemen und eGov-Lösungen der Verwaltung als Kenntnis zu gelten hat.

<sup>100</sup> BSK StGB-OBERHOLZER, Art. 320 N 10.

<sup>101</sup> BSK StGB-OBERHOLZER, Art. 320 N 10.

<sup>102</sup> LOCHER, N 3 zu Art. 110 DBG, betont im Vergleich zum Steuergeheimnis beim Amtsgeheimnis den eingeschränkten Kreis der Berechtigten und spricht deshalb nur beim Steuergeheimnis vom « Käseglocke-Prinzip ». Auch unter der « Käseglocke »

zulässige Teilen von Informationen auf die « *bonne marche du service* » und daraus abgeleitet auf zwei funktionelle Kriterien abgestellt werden: Die von der Offenbarung betroffene Information weist einen Bezug zur Funktion und Tätigkeit des Empfängers auf und ist nötig oder zumindest nützlich für die Erfüllung seiner Aufgabe<sup>103</sup>. Wenn es nicht reicht, dass Empfänger dem Amtsgeheimnis unterliegen, stellt sich immer noch die Frage, ob dies notwendig ist. Mit anderen Worten stellt sich die Frage, ob Personen, welche die Täter-eigenschaften nicht aufweisen und somit der Strafdrohung nicht unterliegen, rechtmässig als Hilfspersonen beigezogen werden können. Der Bundesrat verneint dies in seiner Botschaft zum ISG betreffend externe Hilfspersonen im Bereich IKT, indem er bei deren Einsatz eine Offenbarung bejaht und die Möglichkeit einer rechtfertigenden Einwilligung der vorgesetzten Behörde insgesamt verwirft, so dass er neben einer Strafbarkeitslücke betreffend die Hilfspersonen auch ein Strafbarkeitsrisiko der verwaltungsinternen Mitarbeitenden konstatiert<sup>104</sup>. Gleichzeitig anerkennt der Bundesrat, dass Outsourcing in vielen Bereichen nicht nur allgemein üblich, sondern geradezu zwingend sei<sup>105</sup>. Kein Ausweg aus diesem Dilemma scheint mir angesichts des strafrechtlichen Analogieverbots, die Hilfspersonenregelung von Art. 321 StGB analog auf Art. 320 StGB anzuwenden<sup>106</sup>. Ob es nicht überzeugender ist, den Beizug von Hilfspersonen unter gewissen Voraussetzungen<sup>107</sup> zuzulassen, wird hier nicht weiter behandelt, weil mit dem ISG auch der Täterkreis des Art. 320 StGB um die Hilfspersonen erweitert wird<sup>108</sup>. Cloud-Anbieter werden somit wie bei der parallelen Regelung in Art. 321 StGB als Hilfspersonen qualifiziert werden können<sup>109</sup>. Eine tatbestandliche Offenbarung rechtmässig beigezogenen Hilfspersonen gegenüber dürfte inskünftig somit ausgeschlossen sein<sup>110</sup>. Frag-

---

muss indes gelten, dass Personendatenbearbeitungen nur soweit zulässig sind als nötig, eine beigezogene Informatikerin, aber auch ein konkret unzuständiger Veranlager, darf nicht überschliessend – z.B. aus persönlicher Neugier – Steuerdaten sichten.

<sup>103</sup> MÉTILLE, S. 612 f. Vgl. auch BSK StGB-OBERHOLZER, Fn. 87, Art. 320 N 10 : « dienstlich gerechtfertigt ». In der parallelen Diskussion zu den Berufsgeheimnissen spricht sich die überwiegende Lehre für ein analoges Verständnis aus, vgl. ROSENTHAL, Cloud, N 65 f., m.Hw. und Diskussion der a.M. WOHLERS.

<sup>104</sup> BBI 2017 3077 f.

<sup>105</sup> BBI 2017 3077.

<sup>106</sup> So aber wohl MÉTILLE, S. 613 f.

<sup>107</sup> Insbesondere Geheimhaltungsvereinbarungen, verstärkt durch Konventionalstrafen, wodurch das Amtsgeheimnis vertraglich auf die Hilfspersonen ausgeweitet wird.

<sup>108</sup> Vgl. oben bei Fn. 92.

<sup>109</sup> Vgl. SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 27 f., 29.

<sup>110</sup> Vgl. zur analogen Fragestellung bei Art. 321 StGB in diesem Sinne SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, S. 29, m.Hw. auf die a.M. von WOHLERS. Einer vertieften Untersuchung vorbehalten bleibt die Frage, wer alles als Hilfsperson gelten kann, bspw. bei einem ausländischen Cloud-Anbieter in Gesellschaftsform. Dies betrifft



lich ist diese Schlussfolgerung, wenn sich die Hilfspersonen im Ausland aufhalten. Denn diesfalls könnte die Hilfsperson in Anwendung ausländischen Rechts zur Offenbarung verpflichtet sein, ohne sich dagegen wirksam auf das schweizerische Amtsgeheimnis berufen zu können, und zudem dürfte eine strafrechtliche Sanktionierung im Ausland schwierig sein<sup>111</sup>. Unter Vorbehalt einer vertieften Prüfung sehe ich aber keine schlagenden Argumente, die Qualifikation als Hilfsperson von ihrer Strafbarkeit oder der Durchsetzbarkeit des Strafanspruchs ihr gegenüber abgängig zu machen. Eine Limitierung auf Hilfspersonen in der Schweiz bzw. Cloud-Anbieter auf schweizerischem Territorium ist insofern für mich daher unter diesem Aspekt nicht naheliegend. Selbst wenn zulässigerweise geheime Personendaten soweit nötig einem Cloud-Anbieter bzw. dessen Personal zugänglich gemacht werden, ist die Gefahr einer unzulässigen Bekanntgabe bzw. Offenbarung nicht gebannt. Denn die Behörde muss für genügende Vorkehrungen sorgen, damit nicht unbefugte Zugriffe durch Dritte oder Bekanntgaben an Dritte erfolgen. Es kann sich dabei z.B. um unerlaubte Zugriffe des Personals des Cloud-Anbieters, Hacker-Angriffe oder Zugriffe ausländischer Behörden handeln<sup>112</sup>. In der Lehre ist umstritten, ob es sich bei Art. 320 StGB um ein Tätigkeits- oder ein Erfolgsdelikt handelt, wobei für die Qualifikation als Erfolgsdelikt u.a. grammatikalisch und mit Praktikabilitätsüberlegungen argumentiert werden kann<sup>113</sup>. Vorliegend wird dieser Auffassung gefolgt, womit das Offenbaren eine effektive Kenntnisnahme erfordert. Nach Auffassung des Bundesrats genügt indes bereits das Verschaffen einer Möglichkeit der Kenntnisnahme<sup>114</sup>, wobei die dafür zitierte Lehrmeinung OBERHOLZER, jedenfalls in der konsultierten, heute aktuellen Ausgabe der Kommentierung, m.E. das Gegenteil aussagt<sup>115</sup>: Der zitierte Autor führt zwar zunächst aus, der Täter müsse das Geheimnis « zur Kenntnis bringen oder [...] die Kenntnisnahme zumindest ermöglichen ». Der nächste Satz lautet dann aber: « Auf welchem Weg dies geschieht, ist unbeachtlich, es **genügt**, dass ein Unberechtigter aufgrund des Verhaltens des Amtsträgers Kenntnis von einer unter den Geheimnisbegriff fallenden Tatsache

---

einerseits die Mitarbeitenden des Cloud-Anbieters, aber auch dessen Vertragspartner, an die ggf. gewisse Leistungen weiter ausgelagert werden.

<sup>111</sup> MÉTILLE, S. 614, auch zum Folgenden. Zudem entfällt im Ausland auch die Möglichkeit, sich auf im schweizerischen Prozessrecht geregelte Rechte zu berufen.

<sup>112</sup> Für Beispiele traditioneller und neuer Herausforderungen der Datensicherheit im Zusammenhang mit Cloud-Lösungen vgl. ROSENTHAL, Cloud, N 75 ff.

<sup>113</sup> ERARD, N 567 i.V.m. N 459 ff. Vgl. auch den Hinweis von ROSENTHAL, Cloud, N 11, unter Verweis auf BGer 6B\_1403/2017, E. 1.2.2.

<sup>114</sup> BUNDESRAT, Botschaft ISG, BBl 2017 3077, Fn. 36. ROSENTHAL, CLOUD, N 11, relativiert die Bedeutung der Fragestellung im Hinblick auf die regelmässig erfolgenden Klartextzugriffe beim Cloud-Anbieter und die Möglichkeit eines Lawful Access im Ausland.

<sup>115</sup> BSK StGB-OBERHOLZER, Fn. 87, Art. 320 N 10, auch zum Folgenden.

**erlangt** »<sup>116</sup>. Aus der analogen Welt stammende Beispiele für Offenbarungen sind zwar eingängig, wie wenn jemand Dokumente mit geheimen Informationen am Arbeitsplatz liegen lässt und die Kenntnisnahme unberechtigter Dritter in Kauf nimmt. Sie helfen in der digitalen Realität aber nur beschränkt weiter. In einer technisch komplexen, arbeitsteiligen Situation lässt sich nicht mit relativ einfachen Massnahmen die unzulässige Offenbarung genügend sicher verhindern, im genannten Beispiel etwa durch eine *clean desk policy* bzw. die Aufbewahrung der Dokumente in einem abgeschlossenen Bereich. Eine intuitive Erfassung und Beurteilung der Situation ist kaum möglich, nötig ist ein strukturiertes Vorgehen, welche alle relevanten Faktoren in ihren wechselseitigen Bezügen zum Tragen bringt<sup>117</sup>. Ein möglicher Ansatz ist die risikoorientierte Prüfung, ob genügende rechtliche, technische und organisatorische Vorkehrungen getroffen wurden, um das Risiko der unzulässigen Offenbarung im Sinne der Eintrittswahrscheinlichkeit ausreichend zu reduzieren<sup>118</sup>. Zu den notwendigen Vorkehrungen gehören m.E. auch Vorgaben anderer Gesetze zum Schutz der Geheimnisse, sie hat der Gesetzgeber für eine zureichende Risikominimierung als notwendig erachtet.

Nur eine *vorsätzliche* Begehung ist strafbar, wobei Eventualvorsatz genügt. In Anlehnung an ROSENTHAL wird der Eventualvorsatz wohl dann ausgeschlossen werden können, wenn die Verantwortlichen das Risiko einer Offenbarung sorgfältig prüften, angemessene (fortdauernde) Massnahmen dagegen ergriffen und das Restrisiko als genügend tief erachteten, um darauf vertrauen zu können, dass es sich nicht realisieren werde<sup>119</sup>. Um dies nachweisen zu können, wird eine Dokumentation der Umstände wichtig sein. Wann und nach welchen Kriterien im Kontext der behördlichen Cloud-Nutzung ein genügend tiefes Restrisiko erreicht wurde, kann hier nicht vertieft geprüft bzw. behandelt werden. Immerhin lässt sich nach meinem Dafürhalten zustimmen, dass ein risikobasierter Ansatz mit Art. 320 StGB vereinbar ist. Wie bereits erwähnt bleiben zum Schutz der Vertraulichkeit der Daten und mithin des Amtsgeheimnisses bestehende besondere Vorschriften vorbehalten. Werden solche bewusst missachtet, beispielsweise eine gesetzliche Lokalisierungsvorschrift, kann dies m.E. den (Eventual-)Vorsatz begründen. Denn diesfalls hat der Gesetzgeber die Risikobeurteilung punktuell selbst vorgenommen. Im Allgemeinen dürfen m.E. Mitarbeitende der Verwaltung oder Behördenmitglieder darauf vertrauen, dass der Gebrauch der zur Verfügung gestellten und zu

---

<sup>116</sup> BSK StGB-OBERHOLZER, a.a.O., Hervorhebungen nicht im Original.

<sup>117</sup> Vgl. zu dieser Thematik ROSENTHAL, Cloud, N 114.

<sup>118</sup> Nach ROSENTHAL, Cloud, N 129, ist auf die für Risikobeurteilung nebst der Eintrittswahrscheinlichkeit üblicherweise zu berücksichtigende Schadenshöhe im Kontext der Strafnormen zu verzichten, da jede Offenbarung tatbestandsmässig ist.

<sup>119</sup> ROSENTHAL, Cloud, N 82 ff. Die Überlegungen des Autors beziehen sich zwar auf Berufsgeheimnisse inkl. StGB 321 und nicht Amtsgeheimnisse, sind m.E. aber auch betreffend den Amtsgeheimnisschutz gültig.

nutzenden Arbeitsinstrumente rechtmässig ist. Die strafrechtliche Verantwortlichkeit ist zwar nicht explizit auf gewisse Entscheidungsträger beschränkt, aber im Ergebnis werden diejenigen Personen im Fokus stehen, die über die Einführung einer Cloud-Lösung entscheiden sowie jene, die bestimmenden Einfluss darauf haben<sup>120</sup>.

Es kommen die allgemeinen gesetzlichen oder aussergesetzlichen *Rechtfertigungsgründe* in Frage, Art. 320 Ziff. 2 regelt insbesondere den Fall der Einwilligung der vorgesetzten Behörde. Mit Blick auf allfällige systematische Offenlegungen bei Cloud-Lösungen interessant scheint mir namentlich die *gesetzlich erlaubte Handlung* gemäss Art. 14 StGB, wonach sich rechtmässig verhält, wer handelt, wie es gesetzlich geboten oder erlaubt ist, auch wenn die Tat nach dem StGB oder einem anderen Gesetz mit Strafe bedroht ist. Nach Art. 11 VDTI etwa dürfen nicht allgemein zugängliche Daten externen Leistungserbringern zugänglich gemacht werden, wenn dies zur Erbringung der Leistung erforderlich ist, die für die Daten verantwortliche Behörde oder die vorgesetzte Stelle schriftlich zugestimmt hat und angemessene vertragliche, organisatorische und technische Vorkehrungen getroffen wurden, um eine weitere Verbreitung der Daten zu verhindern<sup>121</sup>. Mit dem DSG lässt sich nicht analog Art. 11 VDTI argumentieren, weil die Auftragsbearbeitung in Art. 10a Abs. 1 Bstb. b DSG ausdrücklich Geheimhaltungspflichten, wie das Amtsgeheimnis gemäss Art. 320 StGB, vorbehält. Die *Einwilligung* der vorgesetzten Behörde erweist sich insgesamt aus rechtlichen und faktischen Gründen nicht als gangbarer Weg<sup>122</sup>. Gleiches gilt für die Einwilligung der Betroffenen<sup>123</sup>. Der von der Rechtsprechung und Lehre anerkannte Rechtfertigungsgrund der *Wahrung berechtigter Interessen*<sup>124</sup> dürfte mangels klar überwiegender Interessen der Verwaltung auch ausser Betracht fallen, ebenso wie die Anrufung einer *Sozialadäquanz* bei der Nutzung von Cloud-Diensten<sup>125</sup>.

---

<sup>120</sup> Betreffend die Strafbestimmungen des nDSG vgl. BBl 2017 7099 und kritisch dazu ROSENTHAL/GUBLER, S. 58, wonach in erster Linie nicht die Unternehmensleitung, sondern die in ausführender Position faktisch Entscheidenden betroffen sind. Jedenfalls für die Mitarbeitenden, welche die zur Verfügung gestellten Arbeitsinstrumente (zu) nutzen (haben), ändert dies nichts.

<sup>121</sup> Zur Streitfrage, ob nicht nur eine « formellgesetzliche » Regelung als Rechtfertigung im Sinne von Art. 14 StGB in Frage kommt vgl. BSK StGB-NIGGLI/GÖHLICH, Fn. 87, N 5 ff. zu Art. 14.

<sup>122</sup> Vgl. dazu BUNDESRAT, Botschaft ISG, BBl 2017 3077 f. Der Entscheid des Regierungsrats des Kantons Zürich zur Zulassung von Cloud-Lösungen (KANTON ZÜRICH, Cloud-Lösungen, passim) fiele demnach als Rechtfertigungsgrund im Rahmen von Art. 320 StGB ausser Betracht.

<sup>123</sup> MÉTILLE, Fn. 66, S. 615.

<sup>124</sup> Vgl. BSK StGB-OBERHOLZER, Fn. 87, N 17 zu Art. 320.

<sup>125</sup> MÉTILLE, Fn. 66, S. 616. Inwieweit sich eine Verwaltung bzw. Beamtinnen und Beamte auf die Sozialadäquanz berufen könnten, scheint mir ohnehin fraglich, da bei hoheitlichem Handeln keine sozialen Normen im eigentlichen Sinn in Frage stehen.

## C. Fazit

Zu den besonderen Anforderungen an die behördliche Cloud-Nutzung gehört die Wahrung des Amtsgeheimnisses. Behördliche Geheimnispflichten ergeben sich sowohl aus dem Verwaltungsrecht als auch aus dem Strafrecht, namentlich aus Art. 320 StGB, der vorliegend näher betrachtet wird. Es handelt sich dabei um ein echtes Sonderdelikt, Täter können nur Behördenmitglieder und Beamte sein, IKT-Leistungserbringer gehören nach geltendem Recht nicht dazu. Dies wird sich mit dem Inkrafttreten der mit dem ISG erfolgten Erweiterung des Täterkreises auf Hilfspersonen ändern, da auch Cloud-Anbieter und ihr Personal als solche zu qualifizieren sind. Eine Übermittlung von Personendaten an als Hilfsperson zu qualifizierende Cloud-Anbieter wird unter den erwähnten Bedingungen für eine Bekanntgabe unter Amtsgeheimnisverpflichteten keine tatbestandliche Offenbarung mehr darstellen. Die Gefahr einer Verletzung des Amtsgeheimnisses besteht allerdings weiterhin, es drohen unbefugte Zugriffe durch Dritte oder Bekanntgaben an Dritte. Tatbestandlich ist nach hier vertretener Auffassung die effektive Kenntnisnahme nötig, d.h. es handelt sich bei Art. 320 StGB um ein Erfolgsdelikt. Welche Vorkehrungen nötig sind, um eine Verletzung des Amtsgeheimnisses auszuschliessen, kann angesichts der Komplexität der zu beurteilenden Sachverhalte nicht generell beurteilt werden. M.E. ist dafür ein strukturiertes Vorgehen unter Einsatz von Instrumenten, die auf einem risikobasierten Ansatz beruhen und die erkannten und mit geeigneten Massnahmen reduzierten Risiken bewerten, grundsätzlich geeignet und mit Art. 320 StGB vereinbar. Dabei sind spezifische verwaltungsrechtliche Vorschriften zum Schutz der Vertraulichkeit mit einzubeziehen und zu respektieren. Strafrechtlich zur Rechenschaft gezogen werden können Personen, die bestimmenden Einfluss auf die Cloud-Nutzung haben. Mitarbeitende, welche die zur Verfügung gestellten Arbeitsinstrumente nutzen, dürfen davon ausgehen, dass dies rechtmässig ist.

## IV. Informationsschutz

### A. Einleitung

Personendaten<sup>126</sup> sind Informationen im Sinne der Regelungen zum Informationsschutz<sup>127</sup>. Nachfolgend weise ich deshalb summarisch auf die

---

<sup>126</sup> Jede Art von Angaben (Informationen oder Aussagen) über eine Person, vgl. BELSER/EPINEY/WALDMANN, §7, N 37.

<sup>127</sup> Informationen sind Aufzeichnungen auf Informationsträgern und mündliche Äusserungen (Art. 3 Bstb. a ISchV).

geltenden bundesrechtlichen Regelungen sowie auf das neue Informationssicherheitsgesetz hin. Eingehender wird sich der Bericht « Rechtlicher Rahmen für die Cloud » damit befassen, der derzeit im Rahmen der Cloud-Strategie des Bundesrates von der Bundeskanzlei erarbeitet wird<sup>128</sup>.

## B. Geltendes Recht

Aus den einschlägigen Erlassen ergeben sich Anforderungen für die Nutzung von Cloud-Lösungen. So ist die Cyberrisikenverordnung (CyrV) anwendbar<sup>129</sup> und es muss periodisch<sup>130</sup> ein Sicherheitsverfahren durchlaufen werden. Dazu gehört insbesondere eine Schutzbedarfsanalyse<sup>131</sup>. Bei erhöhtem Schutzbedarf braucht es weitergehende Massnahmen, Restrisiken sind auszuweisen<sup>132</sup>.

Relevant für Cloud-Lösungen sind auch die Klassifizierungen von Informationen nach der Informationsschutzverordnung (ISchV): « interne » Informationen dürfen nur Berechtigten zugänglich sein, « vertrauliche » Informationen müssen vorgängig verschlüsselt werden, und sind sie « geheim », braucht es zusätzlich eine Bewilligung der Koordinationsstelle<sup>133</sup>.

## C. Das Informationssicherheitsgesetz (ISG)

Das Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18.12.2020 führt verschiedene heute noch geltende Regelungen zusammen. Es will als Einheitsgesetz die Zersplitterung im Bereich der Informationssicherheit auf Stufe des Bundes reduzieren. Das ISG und sein Ausführungsrecht sollen in der ersten Hälfte 2023 in Kraft treten<sup>134</sup>.

Sein Zweck ist es, die sichere Bearbeitung der Informationen und den sicheren Einsatz der Informatikmittel zu gewährleisten<sup>135</sup>. Im Unterschied zum DSG

---

<sup>128</sup> Vgl. Cloud-Strategie, Fn. 2, MS 5.

<sup>129</sup> Art. 3 Bstb. h CyrV.

<sup>130</sup> Art. 14e CyrV.

<sup>131</sup> Art. 14b CyrV.

<sup>132</sup> Art. 14d CyrV.

<sup>133</sup> S. Anhang zur ISchV. Gemäss einer internen Weisung des ISB vom 1.4.2020 ist für « geheime » Informationen die Nutzung einer Cloud unzulässig.

<sup>134</sup> Mit punktueller vorzeitiger Inkraftsetzung, vgl. Medienmitteilung des Bundesrats vom 6.4.2022, Bundesrat beschliesst Teilinkraftsetzung des Informationssicherheitsgesetzes.

<sup>135</sup> Art. 1 ISG.

und nDSG schützt es einzig öffentliche Interessen<sup>136</sup>, wozu allerdings auch die Erfüllung der gesetzlichen und vertraglichen Verpflichtungen der Behörden und Organisationen des Bundes zum Schutz von Informationen gehört<sup>137</sup>. Dies erfasst auch die Wahrung der Vertraulichkeit und Integrität von Personendaten<sup>138</sup>. Mithin geht es darum, die Vertrauenswürdigkeit der Bundesbehörden zu schützen.

Was das Verhältnis zum DSG angeht, so ist das ISG ergänzend anwendbar<sup>139</sup>. Ausgangspunkt ist die Feststellung, dass das DSG betreffend die Bearbeitung von Personendaten das Spezialgesetz ist<sup>140</sup>. Das DSG regelt indes auch die Vertraulichkeit, Verfügbarkeit und Integrität der Personendaten<sup>141</sup>. Die Personendaten sind gleichzeitig auch Informationen im Sinne des ISG, welches seinerseits ihre Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit schützt. Indem das Ausführungsrecht zum ISG bezogen auf das jeweilige Schutzniveau<sup>142</sup> eine Standardisierung nach dem Stand von Wissenschaft und Technik verwirklichen soll, wird es das Datenschutzrecht ergänzen können, welches bislang keine solche Standardisierung kennt. Dem ist bei der derzeit laufenden Überarbeitung der totalrevidierten VDSG zum nDSG Rechnung zu tragen.

Betreffend Cloud-Lösungen ist m.E. davon auszugehen, dass es sich dabei ohne Weiteres um Informatikmittel im Sinne des ISG handelt<sup>143</sup>. Daran anknüpfend erscheint insbesondere das im ISG geregelte Sicherheitsverfahren von Bedeutung, wonach die verpflichteten Behörden ein Verfahren zur Gewährleistung der Informationssicherheit beim Einsatz von Informatikmitteln festlegen müssen<sup>144</sup>. Dies umfasst u.a. den Schutzbedarf der Informationen sowie die Sicherheitsmassnahmen und ihre Überprüfung<sup>145</sup>. Der Schutzbedarf ist im Übrigen für das zu erreichende Schutzniveau der wohl wichtigste, aber nicht der einzige zu berücksichtigende Aspekt, ebenfalls Rechnung zu tragen ist namentlich der Zweckmässigkeit, Wirtschaftlichkeit und Benutzerfreundlichkeit<sup>146</sup>.

---

<sup>136</sup> Art. 1 Abs. 2 ISG.

<sup>137</sup> Art. 1 Abs. 2 Bstb. e.

<sup>138</sup> Vgl. BUNDESRAT, Botschaft ISG, BBl 2017, 3011, auch zum Folgenden.

<sup>139</sup> Art. 4 Abs. 2 ISG.

<sup>140</sup> BUNDESRAT, Botschaft ISG, BBl 2017, 2977 auch zum Folgenden.

<sup>141</sup> Art. 7 DSG, Art. 8 ff. VDSG.

<sup>142</sup> Massgeblich für den Schutzbedarf ist die potenzielle Beeinträchtigung der öffentlichen Interessen gem. Art. 1 Abs. 2 ISG, wobei aufgrund von Art. 1 Abs. 2 Bstb. e und Art. 4 Abs. 2 der bereichsspezifische Schutzbedarf ggf. durch andere Erlasse wie namentlich das DSG bzw. nDSG vorgegeben wird (vgl. Botschaft zum ISG, BBl 2017, 3016).

<sup>143</sup> Vgl. die Legaldefinition in Art. 5 Bstb. a.

<sup>144</sup> Art. 16 Abs. 1 ISG.

<sup>145</sup> Art. 16 Abs. 2 ISG.

<sup>146</sup> Art. 6, insbes. Abs. 4.

## D. Fazit

Auch wenn nach dem Gesagten die Regeln zum Informationsschutz mitunter Personendaten schützen, bleibt der Brückenschlag zwischen den beiden Rechtsgebieten schwierig. Denn die Regeln über den Informationsschutz dienen dem *öffentlichen Interesse*<sup>147</sup>, welches den Schutz der Privatsphäre nur indirekt miterfasst. Zwar wird man ein hohes öffentliches Interesse an der Vertrauenswürdigkeit der Bundesbehörden und mithin am Vertrauensverhältnis zwischen ihnen und den Rechtsunterworfenen bejahen können. Die digitale Transformation der Verwaltung dürfte zudem ohne das Vertrauen der Bevölkerung politisch nur schleppend realisierbar sein, wie beispielsweise die Abstimmung zur E-ID<sup>148</sup> gezeigt hat<sup>149</sup>. Aber das Recht zum Informationsschutz und insbesondere das ISG kann nach dem Gesagten nur beschränkt auch den Schutz der Persönlichkeit im Zusammenhang mit der Bearbeitung von Personendaten gewährleisten. Bekannte Instrumente des Informationsschutzes, namentlich die Schutzbedarfsanalyse (« Schuban »), sind nicht darauf ausgerichtet. Inwieweit es sinnvoll ist, sie mit datenschutzrechtlichen Aspekten anzureichern, wird hier offengelassen. Jedenfalls müssen die Anforderungen des Datenschutzes eigenständig geprüft und ausgewiesen werden.

## V. Schluss

Nach der vorliegend vertretenen Auffassung vermag sich ein risikobasierter Ansatz in den für Cloud-Projekte relevanten Rechtsbereichen des Datenschutz-, Straf- und Informationsschutzrechts zu entfalten. Daraus darf nicht zugleich geschlossen werden, dass dies überall in gleicher Weise geschieht. Im Datenschutzrecht und Informationsschutzrecht ist der risikobasierte Ansatz für Massnahmen betreffend die Datensicherheit ausdrücklich vorgesehen, bei anderen datenschutzrechtlichen Normen wie dem Verhältnismässig-

---

<sup>147</sup> Vgl. zum geltenden Recht Art. 1 Abs. 1 ISchV, « *Schutz von Informationen des Bundes und der Armee, soweit er im Interesse des Landes geboten ist* ». Allgemeiner gehalten ist die CyrV, die allerdings namentlich das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR 120) ausführt (vgl. Ingress CyrV und Art. 30 BWIS).

<sup>148</sup> Die Vorlage über das E-ID Gesetz wurde mit 64.4% Nein-Stimmen abgelehnt, <<https://www.bk.admin.ch/ch/d/pore/va/20210307/det639.html>> (*letztmals besucht am 5.2.2022*).

<sup>149</sup> Gemäss der zuständigen Bundesrätin habe das Stimmvolk eine gewisse Malaise zur fortschreitenden Digitalisierung zum Ausdruck gebracht, <<https://www.srf.ch/news/abstimmungen/elektronische-identitaet/nein-zum-e-id-gesetz-keller-sutter-daempft-hoffnung-auf-schnelle-e-id-alternative>> (*letztmals besucht am 5.2.2022*).

keitsgrundsatz kann er als inhärent betrachtet werden oder, wie bei den Vorschriften über die Auftragsbearbeitung und die grenzüberschreitende Personen­datenübermittlung, im Rahmen einer teleologisch-systematischen Auslegung und als prägendes Leitprinzip des totalrevidierten Datenschutzrechts zur Anwendung gelangen. Auch bei der Frage der Verletzung des Amtsgeheimnisses und mithin der Vertraulichkeit nach Art. 320 StGB lässt sich m.E. ein risiko­basierter Ansatz für die strafrechtliche Zurechnung begründen, was mit Blick auf den explizit risikobasierten Schutz der Vertraulichkeit als Teil der Datensicherheit ein stimmiges Bild ergibt. Die Methodik, Kriterien und Grenzen müssen gestützt auf die jeweils in Frage stehenden Rechtsnormen, die mitunter verschiedene Regelungszwecke und Interessen verfolgen, durch Auslegung ermittelt werden und können heute noch nicht als geklärt gelten. In der Praxis entwickelte und zunehmend auch bei der behördlichen Beurteilung von Cloud-Vorhaben eingesetzte Instrumente zur Risikoanalyse sind zu begrüßen, können sich aber nicht vom Gesetz und seiner Auslegung ablösen bzw. an seine Stelle treten.

## VI. Literatur

**BAERISWYL Bruno**, Wenn die Rechtsauslegung « nebulös » wird, *digma* 2019, S. 118 ; **BELSER Eva Maria/EPINEY Astrid/WALDMANN Bernhard**, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011 ; **BREITBARTH Paul**, A Risk-Based Approach to International Data Transfers, EDPL 4/2021, S. 539 ff. ; **EIGENMANN Matthias**, Enhanced Privacy for Data Analytics, How Confidential Computing Can Enhance Data Protection Compliance for Data Analytics, LSR 1/2022 | S. 27 ff. ; **ERARD Frédéric**, Le secret médical, Zürich 2021 ; **HELBLING Peter**, in: PORTMANN/UHLMANN (Hrsg.), Bundespersonalgesetz, Stämpflis Handkommentar, Bern 2013 ; **LOCHER Peter**, Kommentar zum Bundesgesetz über die direkte Bundessteuer, III. Teil – Art. 102-222 DBG, Basel 2015 ; **MAURER-LAMBROU Urs**, Schweiz : Gutachten des Bundesamts für Justiz zum US-Cloud Act, ZD-Aktuell 2021, 05471 (zit. « US-Cloud Act ») ; **MAURER-LAMBROU Urs**, Switzerland foresees risks in potential US Cloud Act executive agreement for its data adequacy, *Privacy Laws & Business*, October 2021, S. 12 f. (zit. « US Cloud Act ») ; **MAURER-LAMBROU Urs/BLECHTA Gabor-Paul** (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3.A., Basel 2014 (zit. « BSK DSGVO-Bearbeiter/in ») ; **MEIER Philippe**, Protection des données, Fondements, principes généraux et droit privé, Bern 2010 ; **MÉTILLE Sylvain**, L'utilisation de l'informatique en nuage par l'administration publique, AJP/PJA 2019, 609 ff. ; **MÉTILLE Sylvain**, Le traitement de données personnelles sous l'angle de la (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020, *Semaine Judiciaire* 2021 II 1 ff. ; **MONTAVON Michael**, Cyberadministration et protection des données. Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyennes et des autorités de contrôle, Zürich 2021 ; **NIGGLI Alexander/WIPRÄCHTIGER Hans**, Basler Kommentar, Strafrecht II, Art. 137-392 StGB, Jugendstrafgesetz, 4.A., 2019 Basel (zit. « BSK StGB-Bearbeiter/in, Art ... N ... ») ; **ROSENTHAL David**, Das neue Datenschutzgesetz, in : Jusletter 16.11.2020 ; **ROSENTHAL David**, Mit Berufsgeheimnissen in die Cloud : So geht es trotz US CLOUD Act, in : Jusletter 10. August 2020 (zit. « Cloud ») ; **ROSENTHAL David/GUBLER Seraina**,



Die Strafbestimmungen des neuen DSG, SZW/RSDA 1/2021, S. 52 ff. ; **RUSSINOVICH Mark/COSTA Manuel/FOURNET Cédric/CHISNALL David/DELIGNAT-LAVAUD Antoine/CLEBSCH Sylvan/VASWANI Kapil/BHATIA Vikas**, Toward Confidential Cloud Computing, acmqueue, january-february 2021, S. 1 ff. ; **SCHRÖDER Markus**, Der risikobasierte Ansatz in der DS-GVO, Risiko oder Chance für den Datenschutz ?, ZD 11/2019, 503 ff. ; **SCHWARZENEGGER Christian/THOUVENIN Florent/STILLER Burkhard/GEORGE Damian**, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Anwaltsrevue 2019, S. 25 ff. ; **TRECHSEL Stefan/PIETH Mark** (Hrsg.), Schweizerisches Strafgesetzbuch, Praxis-kommentar, Zürich/St.Gallen 2021 (zit. « PK StGB-Bearbeiter/in, Art. ... N ... ») ; **TRÜEB Hans Rudolf/ZOBL Martin**, Steuerdaten in der Cloud?, digma 2016, S. 102 ff. ; **WOHLERS Wolfgang**, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB) / Externalisation du traitement des données et secret professionnel (art. 321 CPS), digma 2016, S. 3 ff. und 37 ff.

## VII. Materialien

**ARTICLE 29 DATA PROTECTION WORKING PARTY**, Statement on the role of a risk-based approach in data protection legal frameworks, 30.5.2014 ; **BUNDESRAT**, Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2953 ff. (zit. « Botschaft ISG ») ; **BUNDESRAT**, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, 6941 ff. (zit. « Botschaft DSG ») ; **BUNDESRAT**, Cloud-Strategie der Bundesverwaltung, herausgegeben am 11.12.2020 vom Informatiksteuerungsorgan des Bundes ISB (zit. « Cloud-Strategie ») ; **BUNDESAMT FÜR JUSTIZ (BJ)**, Bericht zum CLOUD Act, Gutachten des Bundesamts für Justiz vom 17.9.2021, <<https://www.bj.admin.ch/dam/bj/de/data/publiservice/publikationen/berichte-gutachten/gutachten/2021-09-17-us-cloud-act.pdf.download.pdf/2021-09-17-us-cloud-act-d.pdf>> (*letztmals besucht am 21.2.2022*) ; **EDÖB**, Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge, 27. August 2021 (zit. « Übermittlung ») ; **EDÖB**, Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandsbezug nach Art. 6 Abs. 2 lit. a DSG, Juni 2021 (zit. « Anleitung »), N08 ; **EDPS**, Decision concerning the investigation into Frontex's move to the cloud (Case 2020-0584), 1.4.2022 ; **EDPS**, Leitlinien zur Nutzung von Cloud-Computing-Diensten durch die Organe und Einrichtungen der EU, 16.3.2018 ; **FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT**, White Paper Datenschutz-Folgenabschätzung, Eggenstein 2016, Ziff. 3.3. ; **INFORMATIKSTEUERUNGSORGAN DES BUNDES (ISB)**, Bericht zur Bedarfsabklärung für eine « Swiss Cloud », Dezember 2020 ; **KANTON ZÜRICH, RRB Nr. 542/2022** vom 30.3.2022, Einsatz von Cloud-Lösungen in der kantonalen Verwaltung, (Microsoft 365), Zulassung, Ziff. 1, <<https://www.zh.ch/bin/zhweb/publish/regierungsratsbeschluss-unterlagen./2022/542/RRB-2022-0542.pdf>> (*letztmals besucht am 15.4.2022*) (zit. « Cloud-Lösungen ») ; **PRIVATIM**, Merkblatt Cloud-spezifische Risiken und Massnahmen vom 3.2.2022, <[http://www.privatim.ch/wp-content/uploads/2022/02/privatim\\_Cloud-Merkblatt\\_v3\\_0\\_20220203\\_def\\_DE-1.pdf](http://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def_DE-1.pdf)> (*letztmals am 21.2.2022 besucht*).



---

# L'informatique en nuage à l'État de Vaud

## État des lieux, enjeux et solutions

NICOLAS SAVOY

Juriste spécialiste

Direction générale du numérique et des systèmes d'information

État de Vaud

MÉLANIE GARCIA

Juriste spécialiste

Direction générale du numérique et des systèmes d'information

État de Vaud

LUDIVINE EPINEY

Chargée de missions

Direction générale du numérique et des systèmes d'information

État de Vaud

CATHERINE PUGIN

Déléguée au numérique

Direction générale du numérique et des systèmes d'information

État de Vaud

### Table des matières

<b>I. Introduction .....</b>	<b>121</b>
<b>II. Cadre technique – L'informatique cantonale vaudoise.....</b>	<b>122</b>
A. La Direction générale du numérique et des systèmes d'information.	122
B. Plan directeur cantonal des systèmes d'information.....	126
<b>III. Cadre politique – La stratégie numérique .....</b>	<b>127</b>
A. Stratégie numérique .....	127
B. Souveraineté.....	128
<b>IV. Cadre juridique.....</b>	<b>129</b>
A. Généralités .....	129
B. Problématiques choisies.....	130
1. Sous-traitance .....	130
2. Communication transfrontière.....	134
a) Généralités.....	134

b)	Communication vers et/ou accès depuis un pays offrant un niveau de protection adéquat.....	135
c)	Communication vers et/ou accès depuis un pays n’offrant pas un niveau de protection adéquat .....	136
aa)	Garanties contractuelles.....	136
aaa)	Généralités.....	136
bbb)	Les clauses contractuelles types ( <i>Standard Contractual Clauses – SCC</i> ).....	136
ccc)	Les règles d’entreprises contraignantes ( <i>Binding Corporate Rules – BCR</i> ).....	137
aa)	<i>Swiss – US Privacy Shield</i> et arrêt Schrems II.....	138
bb)	Schrems III ?.....	140
3.	Contractualisation .....	140
a)	Qualification du contrat informatique .....	140
b)	Difficulté de négociation .....	141
c)	Clauses contractuelles choisies .....	142
d)	Contrat de sous-traitance de données personnelles .....	144
4.	Marchés publics .....	147
5.	Secret de fonction .....	149
<b>V.</b>	<b>Réponses.....</b>	<b>153</b>
A.	Politique d’utilisation de solution informatique externalisée .....	153
1.	Généralités .....	153
2.	Grille d’analyse de la Politique d’utilisation de solution informatique externalisée.....	154
3.	Comité d’experts délégués au numérique (CEDN) .....	156
B.	Politique de la donnée.....	157
C.	Cloud souverain – Étude d’opportunité .....	157
<b>VI.</b>	<b>Conclusion.....</b>	<b>158</b>
<b>VII.</b>	<b>Bibliographie .....</b>	<b>160</b>
A.	Littérature.....	160
B.	Documents officiels .....	161
<b>VIII.</b>	<b>Annexes .....</b>	<b>163</b>
A.	Politique d’utilisation de solution informatique externalisée de la Direction générale du numérique et des systèmes d’information de l’État de Vaud. ....	163
B.	Check-list pour contrat de sous-traitance de solution informatique externalisée de l’Autorité de protection des données et de droit à l’information du Canton de Vaud. ....	191
C.	Étude d’opportunité pour un <i>cloud</i> souverain – document de cadrage, Conférence latine des directeurs du numérique. ....	195

## I. Introduction

Dans le contexte global de la transition numérique, les administrations publiques, à l'instar du secteur privé, n'échappent pas à la modernisation de leurs infrastructures et de leurs processus. Les solutions informatiques utilisées doivent évoluer, pour des raisons de sécurité, de coûts, d'efficacité et d'expérience utilisateur. Cette évolution est marquée depuis plusieurs années par le développement de l'informatique en nuage (*cloud computing*)<sup>1</sup>.

Les solutions informatiques dans le nuage permettent une rationalisation, une prévisibilité des coûts ainsi qu'une souplesse au niveau du déploiement, des mises à jour, de l'adaptation et du maintien de la solution considérée. En effet, la création et l'hébergement de solutions informatiques à l'interne d'une organisation n'est pas toujours possible ni pertinent d'un point de vue technique ou économique.

De manière plus générale, de plus en plus de solutions informatiques sont désormais proposées dans le nuage. Pour les administrations publiques, le choix de cette technologie exige une réflexion large et pluridisciplinaire, que ce soit au niveau de la protection des données, du secret de fonction, de l'aspect contractuel, de l'application de règles sur les marchés publics ou encore pour des raisons d'opportunités politiques et techniques.

Au niveau de la Confédération suisse, l'informatique tend à se développer principalement dans le nuage (*Cloud-first*). Après une première étude (*Swiss Cloud*) ayant établi que le pays n'avait pas la taille nécessaire pour le développement d'une infrastructure en nuage *ad hoc*, un appel d'offres pour le projet « Public Clouds Confédération » (OMC-200007) a abouti à l'attribution d'un marché pour un *cloud* public à quatre acteurs américains et un chinois<sup>2</sup>. Cette décision a contribué à l'ouverture d'un débat important sur cette technologie, ses enjeux et les conséquences pour les administrations publiques et les entités privées en Suisse.

Dans sa séance du 30 mars 2022, le Conseil d'État du Canton de Zürich a pris la décision d'autoriser son administration à déployer la solution en nuage *Microsoft 365*<sup>3</sup>. Constatant que les solutions informatiques se développent toujours plus dans le nuage et qu'il devient de plus en plus difficile de s'en passer,

---

<sup>1</sup> Futura-Science, Cloud Computing : qu'est-ce que c'est ?, <<https://www.futura-sciences.com/tech/definitions/informatique-cloud-computing-11573/>> (consulté le 26 avril 2022).

<sup>2</sup> Chancellerie fédérale, Transformation numérique et gouvernance de l'informatique, Cloud, <<https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-87412.html>> (consulté le 12 avril 2022) ; Références Simap : ID 204859, No de publication 1136825.

<sup>3</sup> Kanton Zürich, Regierungsratsbeschluss Nr. 542/2022, Einsatz von Cloud-Lösungen in der kantonalen Verwaltung, (Microsoft 365), Zulassung, 30.03.2022, <<https://www.zh.ch/>

le Conseil d'État zurichois a effectué une pesée des intérêts et procédé à une évaluation des risques, en particulier au regard d'un potentiel accès aux données par des autorités étrangères<sup>4</sup>. Sur la base des résultats obtenus, il considère que les risques liés à l'utilisation de la solution *Microsoft 365* demeurent faibles et que le déploiement peut avoir lieu, moyennant notamment la création d'un poste de responsable de la sécurité du *cloud*.

S'agissant de l'État de Vaud, le Plan directeur cantonal des systèmes d'information<sup>5</sup> et la stratégie numérique<sup>6</sup> du Conseil d'État du Canton de Vaud donnent les actions à effectuer en tenant compte d'une multitude de principes, comme la sécurité, la protection des données ou encore la gouvernance du numérique.

La présente contribution a pour objectif de présenter la manière dont l'État de Vaud se saisit du sujet de l'informatique en nuage. Elle pose le cadre technique de l'informatique cantonale (II.) et les aspects politiques y relatifs (III.), afin de contextualiser les défis et les enjeux posés par l'informatique en nuage dans l'administration cantonale vaudoise. Elle aborde certains aspects juridiques pertinents sous l'angle de la protection des données, des aspects contractuels, des marchés publics et du secret de fonction, tant d'un point de vue théorique que d'un point de vue d'une pratique vaudoise en pleine évolution (IV.). Elle se penche enfin sur les différentes réponses apportées par l'État de Vaud aux défis posés par cette thématique (V.), avant de conclure (VI.).

## **II. Cadre technique – L'informatique cantonale vaudoise**

### **A. La Direction générale du numérique et des systèmes d'information**

La Direction générale du numérique et des systèmes d'information (DGNSI), au sein du Département de la culture, des infrastructures et des ressources humaines (DCIRH), regroupe l'ensemble des ressources humaines et techniques du domaine des technologies de l'information. Conformément au Règlement du 21 janvier 2009 relatif à l'informatique cantonale (RIC ; BLV 172.62.1), elle assure la disponibilité des moyens informatiques et de télécommunications nécessaires quotidiennement au bon fonctionnement de l'administration et met en œuvre, avec les services bénéficiaires, des solutions

---

de/politik-staat/gesetze-beschluesse/beschluesse-des-regierungsrates/rrb/regierungsratsbeschluss-542-2022.html> (consulté le 17 mai 2022).

<sup>4</sup> IAPP, Resources Center, Transfer Impact Assessment Templates, <<https://iapp.org/resources/article/transfer-impact-assessment-templates/>> (consulté le 17 mai 2022).

<sup>5</sup> Voir II. B.

<sup>6</sup> Voir III. A.

contribuant à rendre les processus de l'administration plus simples et plus efficaces, pour elle-même et pour les administrés-es. Depuis 2018, elle coordonne également la mise en œuvre de la stratégie numérique cantonale, une politique publique présentée au chapitre III<sup>7</sup>.

Il convient de préciser que l'informatique des hautes écoles, l'informatique pédagogique du Département de la formation, de la jeunesse et de la culture (DFJC) et l'informatique des Hospices sont exclus du champ d'application du RIC<sup>8</sup>.

En d'autres termes, la DGNSI est une entité-cadre à vocation transversale : elle collabore avec les autres métiers de l'administration cantonale pour les aider à implémenter les solutions informatiques qui leur permettent de travailler. Ces solutions seront utilisées au quotidien par les services et, bien souvent, elles impliqueront un traitement de données personnelles.

La Cour des comptes du Canton de Vaud résume cette relation DGNSI – services métiers bénéficiaires comme suit<sup>9</sup> : *« Les projets de SI métier impliquent trois parties prenantes principales : le service métier dont le système d'information doit évoluer, la DGNSI dont l'informatique est le métier et, selon les projets, un ou des fournisseurs de solution. La décision de centraliser, à quelques exceptions près, toutes les ressources informatiques au sein de la DGNSI implique que les services métier, porteurs des projets, lui donnent mandat de conduire les projets de SI métier. C'est ainsi que le-la chef-fe de projet et les spécialistes informatiques émanent de la DGNSI. Celle-ci peut de son côté sous-traiter le développement de la solution informatique nécessaire au projet à un fournisseur, qui collaborera sur le projet avec les services métier. La DGNSI en assume alors la responsabilité vis-à-vis des services métier. Le règlement relatif à l'informatique cantonale (RIC) adopté en janvier 2009 définit les attributions de chacune des parties et précise les responsabilités réciproques. »*

---

<sup>7</sup> Voir III. A.

<sup>8</sup> NB : le Centre Hospitalier Universitaire Vaudois (CHUV) fait partie de l'État de Vaud mais il possède sa propre Direction des systèmes d'informations.

<sup>9</sup> Rapport Cdc N° 67, p. 7.

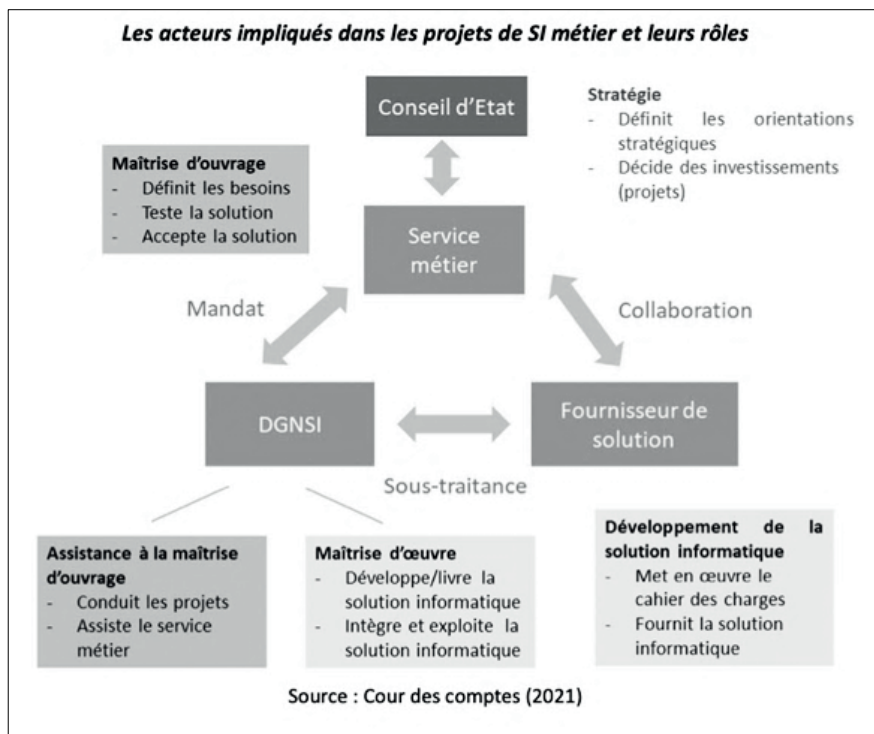


Figure 1 : Les acteurs impliqués dans les projets de SI métier et leurs rôles

La DGNSI, dans son rôle d'expert et d'accompagnant, est chargée de mettre en œuvre les orientations fixées par le Conseil d'État et de conseiller les services métiers, conformément aux art. 6, 7 et 21 RIC. Elle a la charge de « documenter et analyser les systèmes informatiques et leurs fonctionnalités afin de permettre l'élaboration de schémas directeurs métiers en partenariat avec les services bénéficiaires », « élaborer des solutions propres à chaque métier » et de « gérer les relations avec les fournisseurs de biens et services en matière de technologies de l'information et de la communication », étant donc seule habilitée à gérer les contrats. En outre, elle est chargée « d'édicter des directives dans le domaine informatique »<sup>10</sup>.

<sup>10</sup> Rapport Cdc N° 74, p. 28.



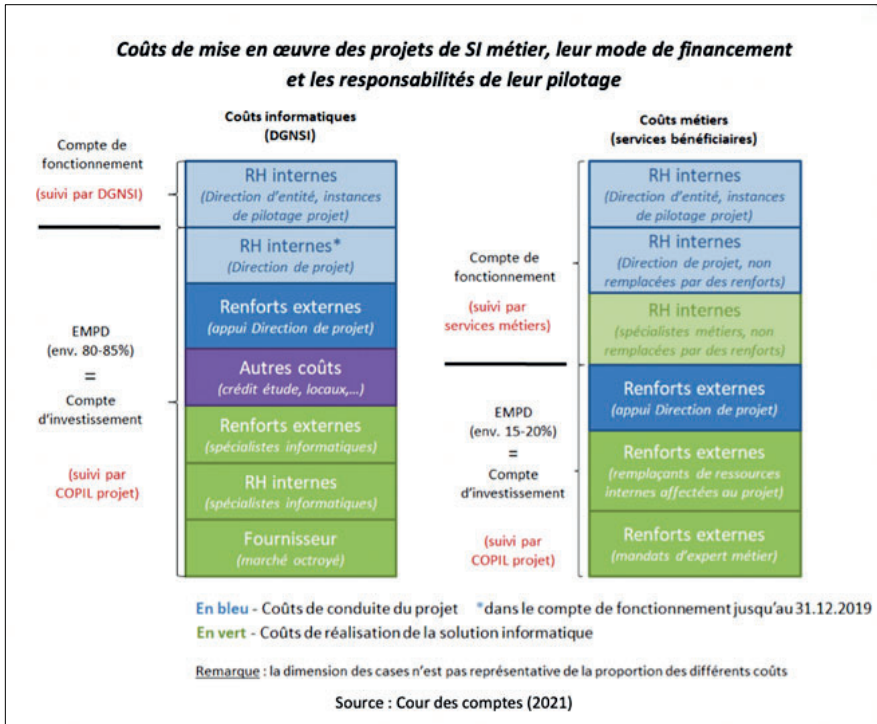


Figure 2 : Coûts de mise en œuvre des projets de SI métier, leur mode de financement et les responsabilités de leur pilotage

Les services métiers, en tant qu'utilisateurs finaux, « définissent les besoins en matière de sécurité (disponibilité, intégrité, confidentialité) » et sont, de par leur statut de propriétaire des données, « responsables de la qualité, de l'harmonisation et de l'optimisation de leurs processus en vue notamment de leur informatisation », conformément à l'art. 10 al. 1 RIC. De même, ils doivent « documenter et analyser leur stratégie, leurs processus, leur organisation et leurs besoins fonctionnels afin de permettre l'élaboration de leur schéma directeur sectoriel (métier) » selon l'art. 10 al. 2 RIC. Les services métiers bénéficiaires de la solution informatique en nuage seront, dans la plupart des cas, les responsables du traitement des données<sup>11</sup>. L'implication de ces derniers dans les projets informatiques est donc essentielle pour atteindre la maturité visée en matière de protection des données, de sécurité informatique et dans la mise en œuvre de la stratégie numérique.

<sup>11</sup> Annexe A., p. 19.

Enfin, la DGNSI a également la charge du développement de la cyberadministration, en proposant à la population un portail sécurisé des prestations en ligne de l'État de Vaud<sup>12</sup>.

## **B. Plan directeur cantonal des systèmes d'information**

Conformément au RIC, le plan directeur cantonal des systèmes d'information décline, pour chaque législature, les objectifs du gouvernement en objectifs généraux pour le système d'information cantonal et en objectifs spécifiques pour les éléments communs aux systèmes d'information propres à chaque métier de l'administration cantonale vaudoise (ACV)<sup>13</sup>.

La transition numérique, la protection des données, les cybermenaces et l'apparition de nouvelles technologies témoignent d'un environnement en pleine mutation. Le besoin de compétences sur ces sujets en interne a clairement été identifié.

Afin de pouvoir répondre à ces enjeux et besoins, la transformation des systèmes d'information de l'État de Vaud doit être poursuivie pour atteindre un degré de maturité satisfaisant en matière d'agilité, de sécurité et d'innovation. Cela se décline en quatre objectifs de résultats globaux :

- un niveau de sécurité adéquat pour assurer l'indispensable disponibilité, confidentialité, intégrité et conformité des systèmes d'information de plus en plus critiques pour le fonctionnement de l'État, et sa relation avec les partenaires et les usagers ;
- une recherche d'efficacité globale tant au niveau de l'informatique qu'au niveau des services utilisateurs et bénéficiaires de l'État ;
- une plus grande agilité du SI pour répondre efficacement, rapidement et en toute sécurité aux besoins d'évolution métiers et technologiques ; et
- une innovation stimulée pour accompagner la transition numérique et la simplification administrative en expérimentant et en intégrant des technologies novatrices.

D'un point de vue financier, le marché des technologies de l'information évolue vers des coûts à l'usage (*pay-as-you-go* ou *pay per use*), des services *cloud* et

---

<sup>12</sup> État de Vaud, Prestations en ligne, simplifiez-vous la vie !, <<https://www.vd.ch/themes/etat-droit-finances/cyberadministration/>> (consulté le 13 avril 2022).

<sup>13</sup> État de Vaud, Le Plan directeur des systèmes d'information est adopté, <<https://www.vd.ch/toutes-les-autorites/departements/departement-des-infrastructures-et-des-ressources-humaines-dirh/direction-generale-du-numerique-et-des-systemes-dinformation-dgnsi/actualites/news/11311i-le-plan-directeur-des-systemes-dinformation-est-adopte/>> (consulté le 30 mai 2022).

quelques grands monopoles. C'est une transformation qui a des impacts sur la structure de financement et sur l'architecture des systèmes d'information.

Depuis 2010, l'État de Vaud possède son propre centre de données, permettant de répondre aux besoins et exigences de l'administration cantonale vaudoise tout en garantissant une maîtrise technique, économique et écologique. Pourtant, la volonté de l'administration publique de moderniser une activité ou une tâche publique la mène à vouloir adopter des solutions informatiques externalisées dans le nuage.

L'informatique en nuage est considérée comme un des éléments importants pour développer la plateforme numérique de l'État de Vaud et son écosystème, en exploitant tout le potentiel de ces solutions lorsque cela est possible. En effet, une solution informatique dans le nuage permet, lorsque les exigences légales sont respectées et les risques maîtrisés, de mettre à disposition de manière très agile des produits et services de qualité à coûts généralement contenus. Pour exploiter ce potentiel dans un cadre défini, l'État de Vaud s'est doté d'une politique d'utilisation de solution informatique externalisée<sup>14</sup>. Les standards de l'administration cantonale, ainsi que leur mise en œuvre en tenant compte des choix disponibles dans le nuage, sont en développement. Les infrastructures doivent être adaptées pour permettre l'intégration et la mise à disposition de ces solutions dans le nuage. Enfin, il s'agit de développer les compétences techniques et contractuelles en la matière.

### **III. Cadre politique – La stratégie numérique**

#### **A. Stratégie numérique**

La transition numérique est un facteur de changement important et touche l'ensemble de la société, les entreprises mais également les organisations publiques et parapubliques. Les missions de l'État de Vaud, qui consistent non seulement à garantir la cohésion sociale et à œuvrer pour le bien commun sur son territoire, par les valeurs fortes qu'il défend, comme l'égalité de traitement, l'inclusion sociale et la protection de sa population, doivent être poursuivies et assurées dans le monde numérique. Pour permettre à l'État de mener son action de manière cohérente, le Conseil d'État du Canton de Vaud s'est doté en 2018 d'une stratégie numérique<sup>15</sup>.

---

<sup>14</sup> Voir V. A. ; Annexe A.

<sup>15</sup> État de Vaud, Le Canton se dote d'une stratégie numérique ambitieuse qui favorise l'innovation et protège les Vaudois, <<https://www.vd.ch/strategie-numerique-du-canton-de-vaud-digitale-strategie-des-kantons-waadt/>> (consulté le 30 mai 2022).

Dans cette stratégie, le Conseil d'État pose trois principes forts : la souveraineté, la sécurité et la solidarité. Il rappelle ainsi que le rôle de l'État ne change pas dans le monde numérique et fixe différentes ancrures sur lesquelles il souhaite concentrer son action : le développement d'une gouvernance claire, l'accompagnement des personnes et des entreprises, les infrastructures et leur sécurité et finalement la mise en œuvre d'une politique générale de la donnée.

Le Canton de Vaud joue un rôle précurseur en se dotant ainsi d'une stratégie numérique. Elle ne s'applique pas exclusivement à la transformation numérique de l'administration, qui, comme toute organisation actuellement, vit des changements profonds avec la numérisation de ses processus, mais s'adresse bel et bien à l'ensemble de la société vaudoise.

En effet, le Conseil d'État souhaite s'assurer que l'État, en tant que garant de la cohésion sociale, continue d'assumer son rôle dans le monde numérique, en évitant qu'une fracture numérique ne s'installe au sein de la population ou des entreprises.

Loin de prôner un tout-numérique (*Digital Also vs Digital Only*), le Conseil d'État souhaite que cette transition numérique se déroule de manière consciente en préservant les intérêts des parties prenantes et en anticipant les enjeux nombreux et parfois encore méconnus posés par ces nouveaux outils.

À l'intersection des ancrures relatives aux données et aux infrastructures, l'informatique en nuage et son développement rapide permettent de questionner la souveraineté numérique du canton mais également les relations de dépendance toujours plus fortes qui se tissent avec l'évolution actuelle de l'informatique<sup>16</sup>.

## **B. Souveraineté**

Avec la numérisation et le développement de la cyberadministration, une tendance à la centralisation des données et de certaines activités au niveau de la Confédération s'observe depuis quelques années. L'art. 3 de la Constitution fédérale (Cst. ; RS 101) garantit la souveraineté des cantons et la stratégie numérique vaudoise rappelle que cette souveraineté persiste dans le monde numérique. Il s'agit là d'un enjeu majeur : rester en contrôle et en maîtrise des changements apportés par le numérique, que ce soit en termes d'outils, de technologies, de processus ou plus globalement de comportements, est une gageure quotidienne.

La présence sur le marché d'acteurs majeurs devenus incontournables engendre une dépendance qui remet également en question cette souveraineté. Ces acteurs

---

<sup>16</sup> Voir V. C. ; Annexe C.

proposent, de manière toujours plus exclusive, des solutions basées sur l'informatique en nuage<sup>17</sup>. Ces dernières permettent de rester concurrentiels en se basant sur des nouveaux modèles économiques.

Cette dépendance est de plus en plus questionnée même si le contexte informatique actuel s'est construit dans une forme d'interdépendance constante. Aujourd'hui, certains politiques s'expriment en faveur de choix de solutions informatiques plus locales et résilientes. L'informatique en nuage est un cas d'usage particulièrement intéressant pour aborder la question de la souveraineté numérique, notion qui reste par ailleurs à définir<sup>18</sup>. En effet, du fait de sa nature décentralisée, elle soulève rapidement le problème de la territorialité. Les données sont hébergées et traitées en dehors du territoire suisse, ce qui pose la question des frontières, de l'accès à ces données et de la législation applicable. La territorialité implique des enjeux géostratégiques complexes et qui existent également dans le monde numérique quand on constate que les accès à certains services ou sites internet sont restreints dans certains pays. Si l'échange de biens « physiques » peut parfois être bloqué entre deux pays, il en va de même s'agissant des accès numériques, ce qui priverait un État de données indispensables à son fonctionnement continu.

## IV. Cadre juridique

### A. Généralités

La Loi vaudoise du 11 septembre 2007 sur la protection des données (LPrD ; BLV 172.65) est applicable, puisqu'il est abordé ici un traitement de données personnelles effectué par une entité de l'administration cantonale vaudoise, conformément à son champ d'application (art. 3 LPrD). Dans le cadre de l'informatique en nuage, c'est le responsable de traitement au sens de l'art. 4 ch. 8 LPrD, *in casu* une entité de l'État de Vaud, qui externalise une activité de traitement de données personnelles auprès d'un éditeur de solution informatique de type en nuage, le sous-traitant.

En effet, l'éditeur d'une solution informatique en nuage qui propose ses services à l'État de Vaud est, dans la plupart des cas, considéré comme un sous-traitant au sens de l'art. 4 ch. 9 LPrD, puisqu'il traite des données personnelles pour le compte du responsable de traitement<sup>19</sup>.

---

<sup>17</sup> ICTJournal, Pandémie ou pas, le marché du cloud public progresse rapidement, <<https://www.ictjournal.ch/etudes/2021-05-20/pandemie-ou-pas-le-marche-du-cloud-public-progresse-rapidement>> (consulté le 10 mai 2022).

<sup>18</sup> Voir V. C. ; Annexe C.

<sup>19</sup> MONTAVON, p. 465 s. ; HK DSG-ROSENTHAL/JÖHRI, art. 10a, N 19.

Plus rare dans le domaine du *cloud*, certaines tâches externalisées par l'État pourraient se faire par le biais d'une délégation de tâche publique. Dans ces circonstances, l'éditeur de la solution informatique en nuage sera vraisemblablement et potentiellement considéré comme (co-)responsable de traitement. Ce cas de figure particulier ne sera pas traité ici. Cela mériterait une contribution dédiée, tant le sujet soulève des problématiques et des défis en matière juridique, politique et légistique<sup>20</sup>.

Il convient de souligner que la LPrD ne s'applique pas directement à un éditeur privé sous-traitant de l'État de Vaud. Il sera par exemple soumis à la Loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1), qui régit notamment le traitement de données personnelles effectué par des personnes physiques et morales privées<sup>21</sup>.

Cependant, il est clair que le sous-traitant devra démontrer qu'il permet à l'État de Vaud d'être conforme à la LPrD s'il entend offrir ses services à ce dernier, notamment par la signature d'un contrat de sous-traitance de protection des données et la production de certifications en matière de sécurité<sup>22</sup>. En effet, le responsable de traitement ne saurait contourner les exigences posées par la LPrD en externalisant le traitement de données sous prétexte que l'éditeur sous-traitant est une personne morale de droit privé non soumise à la LPrD<sup>23</sup>.

Dans les sous-chapitres suivants, la sous-traitance, la communication transfrontière, les aspects contractuels, les marchés publics et le secret de fonction seront abordés d'un point de vue de l'informatique en nuage dans le contexte de l'administration cantonale vaudoise. Les solutions envisagées sont brièvement abordées sous le prisme des pratiques de l'État de Vaud pour chaque problématique rencontrée. Les éléments évoqués ici font partie intégrante des réponses apportées au chapitre V. ci-après, qui s'attardera plutôt sur les aspects de processus internes quant aux analyses et aux choix à effectuer cas échéant.

## **B. Problématiques choisies**

### *I. Sous-traitance*

L'art. 18 al. 1 LPrD prévoit que le traitement de données personnelles peut être confié à un tiers, c'est-à-dire un sous-traitant, aux conditions cumulatives suivantes :

---

<sup>20</sup> Voir à ce sujet notamment MONTAVON, p. 252 s., 513 s.

<sup>21</sup> MONTAVON, p. 248 s.

<sup>22</sup> Voir IV. B.

<sup>23</sup> MONTAVON, p. 488 s.

- le traitement par le sous-traitant est prévu par la loi ou par un contrat ;
- le responsable du traitement est légitimé à traiter lui-même les données concernées ; et
- aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

La loi peut prévoir la sous-traitance et en fixer les contours. Si ce n'est pas le cas, un contrat de sous-traitance de protection des données doit être conclu avec le sous-traitant.

Dans le domaine des solutions *cloud*, la relation avec l'éditeur de la solution est dans la plupart des cas contractuelle. Un contrat, qui règle principalement les aspects commerciaux et techniques, est négocié. L'éditeur propose souvent également un contrat de sous-traitance des données personnelles annexé au cadre contractuel, sous la forme d'un « *Data Processing Agreement* » ou « *Data Protection Addendum* »<sup>24</sup>.

En outre, le responsable de traitement, soit le service métier ou l'entité bénéficiaire de l'État de Vaud, doit être légitimé lui-même à traiter les données personnelles concernées pour pouvoir externaliser le traitement de données. En effet, la sous-traitance ne permet pas au responsable de traitement de s'affranchir du principe de légalité de l'art. 5 LPrD, qui exige une base légale ou l'accomplissement d'une tâche publique pour effectuer un traitement de données personnelles, par le truchement de la sous-traitance. En outre, même si cela n'est pas explicitement précisé par la LPrD, la sous-traitance du traitement de données envisagé doit en respecter les principes généraux<sup>25</sup>.

Il est utile de rappeler ici que la LPrD est une loi-cadre qui pose les principes et le régime général de la protection des données dont le périmètre et la mise en œuvre sont en général développés dans des lois spécifiques ou sectorielles<sup>26</sup>. En principe, elle ne constitue pas en soi une base juridique pour autoriser un traitement de données en particulier<sup>27</sup>.

Il convient donc de s'assurer qu'une base légale sectorielle « métier », ou l'existence d'une tâche publique, donne la compétence à l'entité de l'État de Vaud de pouvoir effectuer le traitement de données personnelles dont l'externalisation auprès d'un éditeur d'une solution *cloud* est envisagée. Cette base légale sectorielle indiquera, notamment, quelles sont les données personnelles que le service métier est en droit de traiter et, en l'occurrence, de sous-traiter<sup>28</sup>.

---

<sup>24</sup> Voir IV. B. 3.

<sup>25</sup> EPINEY/FASNACHT, in BELSER/EPINEY/WALDMANN, § 10, N 49.

<sup>26</sup> MONTAVON, p. 213.

<sup>27</sup> MONTAVON, p. 218.

<sup>28</sup> Voir nuances à ce sujet MONTAVON, p. 219 s.

Il appartient au service métier bénéficiaire de s'assurer, entre autres, que les bases légales sont en place et que l'externalisation est possible sous l'angle des exigences légales, stratégiques et politiques qui lui sont propres. Pour rappel, l'entité métier bénéficiaire sera en principe le responsable du traitement au sens de la LPrD, car utilisatrice « *primaire* » des données personnelles concernées par la solution *cloud*. Le rôle et les responsabilités de la DGNSI sont cependant essentiels dans ce processus, notamment du point de vue de la gestion technique et contractuelle de la relation avec l'éditeur<sup>29</sup>.

Enfin, aucune obligation légale ou contractuelle de garder le secret ne doit interdire le recours à la sous-traitance<sup>30</sup>. En présence d'une telle obligation, le recours à une solution externalisée dans le *cloud* n'est pas d'emblée exclu, mais une analyse de la licéité de la sous-traitance à l'aune de la disposition spéciale doit être effectuée, notamment en présence de secrets dits qualifiés. En outre, toutes les dispositions contractuelles, techniques et organisationnelles pertinentes devront être prévues pour protéger les données soumises à un secret le cas échéant<sup>31</sup>.

Il semble important d'aborder ici brièvement la notion de sous-traitant ultérieur ou sous-traitance dite « en cascade ». Concrètement, il s'agit de la situation d'un éditeur d'une solution *cloud*, soit le sous-traitant « *primaire* », qui fait appel à des sous-traitants qui lui sont propres pour fournir la prestation. Si cette configuration n'est pas interdite par la LPrD, elle augmente le nombre d'intervenants et d'interactions opérationnelles et juridiques. Il s'agit, en soi, d'un risque supplémentaire en matière de protection des données qu'il convient d'intégrer rapidement dans la réflexion<sup>32</sup>.

Il est d'ailleurs intéressant de constater que l'art. 9 al. 3 nLPD<sup>33</sup> prévoit que le sous-traitant ne peut lui-même sous-traiter un traitement à un tiers qu'avec l'autorisation préalable du responsable de traitement<sup>34</sup>. Il s'agit là d'une

---

<sup>29</sup> Voir II. A. ; Annexe A. p. 19 ; Rapports Cdc N° 67 et 74.

<sup>30</sup> Voir IV. B. 5. ; De manière exemplative et non exhaustive, il peut s'agir du secret de fonction (art. 18 de la Loi vaudoise du 24 septembre 2002 sur l'information LInfo ; BLV 170.21 et art. 320 du Code pénal suisse du 21 décembre 1937 CP ; RS 311.0), du secret fiscal (art. 157 de la Loi vaudoise du 4 juillet 2000 sur les impôts cantonaux LI ; BLV 642.11, art. 110 de la Loi fédérale du 14 décembre 1990 sur l'impôt fédéral direct LIFD ; RS 642.11 et 39 de la Loi fédérale du 14 décembre 1990 sur l'harmonisation des impôts directs des cantons et des communes LIHD ; RS 642.14) ou encore du secret des données personnelles en matière d'assurances sociales (art. 33 de la Loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales LPGA ; RS 830.1).

<sup>31</sup> Voir IV. B. 5.

<sup>32</sup> BLATMANN, *in* : PK IDG, § 6 N 7.

<sup>33</sup> Il est prévu que le nouveau droit de la protection des données entre en vigueur le 1<sup>er</sup> septembre 2023.

<sup>34</sup> Message LPD 2020, FF 2020 7397, p. 7401.



disposition dont la teneur est similaire à celle de l'art. 28 al. 2 du Règlement 2016/679 (RGPD)<sup>35</sup>. Afin ne pas vider la notion de sous-traitance de sa substance et dans l'attente d'une révision de la LPrD, il convient, pour l'État de Vaud, d'appréhender la sous-traitance également sous le prisme des dispositions fédérales et européennes dans leur dernière mouture, en incluant ainsi la problématique de la sous-traitance ultérieure de manière systématique.

Concrètement, afin de permettre au responsable de traitement d'effectuer un état des lieux et de procéder à une analyse de risque, le sous-traitant doit être en mesure de fournir une liste complète des sous-traitants ultérieurs engagés, notamment quant aux rôles de ces sous-traitants ultérieurs et de leur localisation<sup>36</sup>. Le cadre contractuel doit prévoir *a minima* un rappel exprès que le sous-traitant « primaire » reste responsable des activités du sous-traitant ultérieur envers le responsable de traitement. En outre, un mécanisme de notification et d'approbation par le responsable de traitement en cas d'ajout ou de retrait d'un sous-traitant ultérieur doit être prévu dans le contrat avec l'éditeur sous-traitant. Des clauses de sortie doivent être prévues dans le cas où le choix d'un sous-traitant ultérieur devait comporter trop de risques pour le responsable de traitement<sup>37</sup>.

Dans la pratique, l'éditeur se réserve bien souvent le droit de sous-traiter ultérieurement par défaut et le contrat prévoit que le responsable de traitement donne son consentement général à la sous-traitance ultérieure<sup>38</sup>.

La limite entre la liberté économique de l'éditeur de solution informatique en nuage et la nécessaire protection des données du point de vue du responsable de traitement est donc ténue.

---

<sup>35</sup> CNIL, Règlement européen sur la protection des données, Guide du sous-traitant, Édition septembre 2017, <[https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide\\_sous-traitant-cnil.pdf](https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf)> (consulté le 24 mai 2022) ; Règlement européen 2016/679 (RGPD) du parlement européen et du conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

<sup>36</sup> Notamment en cas de support/maintenance impliquant un accès aux données depuis un pays n'offrant pas de niveau de protection adéquat ; Voir IV. B. 2.

<sup>37</sup> ROSENTHAL/STUDER/LOMBARD, N 60.

<sup>38</sup> Voir IV. B. 3.

## 2. Communication transfrontière

### a) Généralités

L'utilisation d'une solution d'informatique en nuage, ou *cloud*, est une externalisation d'un traitement de données par rapport aux systèmes d'information de l'État de Vaud. Cela implique en plus, dans certains cas, une communication de données personnelles à l'étranger<sup>39</sup>. Le flux, le transfert ou la communication transfrontière de données personnelles désigne le fait pour des données personnelles, déjà traitées ou en vue d'un traitement, de passer, par la volonté du responsable de traitement, de l'ordre juridique d'un État souverain à celui d'un autre État ou d'un autre sujet de droit international, peu importe la nature des données, le mode traitement ou le destinataire concret des données<sup>40</sup>.

Conformément à l'art. 17 al. 1 LPrD, la communication de données personnelles faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement vers un pays tiers ne peut avoir lieu que si le pays tiers en question assure un niveau de protection adéquat. Le niveau de protection doit faire l'objet d'une évaluation selon un ensemble de circonstances relatives à un traitement donné, notamment sous l'angle des catégories de données, de la finalité, de la durée du traitement ou encore des mesures de sécurité qui sont respectées dans l'État de destination<sup>41</sup>. L'adhésion d'un pays à la Convention 108 fait, par exemple, présumer l'existence d'un niveau de protection adéquat<sup>42</sup>. La responsabilité de ces vérifications revient au responsable de traitement<sup>43</sup>.

L'art. 17 al. 2 LPrD pose les exceptions à cette interdiction de principe à un traitement de données personnelles dans ou depuis un pays n'offrant pas de niveau de protection adéquat. Parmi ces exceptions, le consentement de la personne concernée (art. 17 al. 2 let. a LPrD) et les garanties contractuelles (art. 17 al. 2 let. g LPrD) peuvent notamment entrer en ligne de compte dans le cadre d'une solution externalisée dans le nuage<sup>44</sup>.

---

<sup>39</sup> BSK DSG-MAURER-LAMBROU/STEINER, art. 6, N 1 ss.

<sup>40</sup> MEIER, N 1267, p. 441.

<sup>41</sup> MEIER, N 1295, p. 447.

<sup>42</sup> MEIER, N 1296, pp. 447-448. Sur la convention 108+, WALTER.

<sup>43</sup> MEIER, N 1294, p. 447.

<sup>44</sup> Il convient de faire preuve de toute la réserve nécessaire dans l'emploi de ces exceptions dans cette situation, notamment le consentement (art. 17 al. 2 let. a). Si le consentement n'est pas d'emblée exclu dans le cadre d'une activité de traitement de données effectuée pas une entité publique, il pose d'évidents problèmes pratiques, étant donné que l'État de Vaud traite souvent un volume conséquent de données personnelles par activité de traitement tant à l'interne qu'à l'externe et qu'une base légale prévoit presque toujours le traitement de données personnelles. Dès lors, dans la situation d'un traitement de données prévu par une loi, il semble difficilement concevable de se baser par la suite

**b) Communication vers et/ou accès depuis un pays offrant un niveau de protection adéquat**

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) propose une liste des pays considérés comme offrant un niveau de protection adéquat<sup>45</sup>. Dans le cas d'un transfert de données personnelles dans un pays figurant dans la liste, moyennant un examen périodique de la situation et la mise en place d'un contrat de sous-traitance de protection des données réglant les autres questions par le responsable de traitement, la communication transfrontière est licite et peut avoir lieu sans mesures supplémentaires sur ce point<sup>46</sup>.

À titre d'exemple, dans le cadre d'un transfert de données vers un pays de l'UE ou de l'EEE, on peut considérer que cela se fera sur un territoire offrant un niveau de protection adéquat. Il convient de souligner qu'il est nécessaire d'acquiescer la certitude que les données ne seront pas réexportées ensuite vers un pays tiers n'offrant pas de niveau de protection adéquat, comme le rappelle le PFPDT dans son guide pour l'examen de la licéité de la communication transfrontière de données (art. 6, al. 2, let. a LPD) auquel nous renvoyons<sup>47</sup>.

La problématique est particulièrement saillante en ce qui concerne les activités « accessoires » de la prestation *cloud* et la sous-traitance ultérieure. Si les données sont hébergées dans des serveurs en Suisse ou sur le territoire de l'Union européenne mais que l'activité de maintenance ou de support de la solution *cloud*, impliquant un accès en clair aux données personnelles se produit depuis un pays n'offrant pas un niveau de protection des données adéquat, cela revient,

---

sur le consentement pour une communication transfrontière ultérieure, en cas d'externalisation du traitement. Cela impliquerait la coexistence de deux systèmes d'information pour une activité de traitement, pour les personnes qui auraient consenti et celles qui ne l'auraient pas fait.

<sup>45</sup> Préposé à la protection des données et à la transparence (PFPDT), Liste des États, <[https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2021/20211115\\_Staatenliste\\_f.pdf.download.pdf/20211115\\_Staatenliste\\_f.pdf](https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2021/20211115_Staatenliste_f.pdf.download.pdf/20211115_Staatenliste_f.pdf)> (consulté le 24 mars 2022).

<sup>46</sup> À noter que selon l'art. 16 al. 1 nLPD, le PFPDT ne sera plus compétent pour constater l'adéquation d'un pays en matière de protection des données, cette tâche revenant au Conseil fédéral sous l'empire de la nouvelle loi ; DI TRIA, nLPD.

<sup>47</sup> Préposé fédéral à la protection des données et à la transparence, Guide pour l'examen de la licéité de la communication transfrontière de données (art. 6 al. 2, let. a, LPD), <<https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2021/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20FR%20V1.1.pdf.download.pdf/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20FR%20V1.1.pdf>> (consulté le 24 mars 2022).

*de facto* et *de jure*, à une communication de données personnelles dans un pays n'offrant pas de niveau de protection adéquat<sup>48</sup>.

Dès lors, il convient d'obtenir de l'éditeur de la solution informatique en nuage toutes les informations pertinentes s'agissant du traitement de données, y compris les localisations de ses entités, serveurs, sous-traitants ultérieurs, zones d'opération, flux, *etc.*, afin de pouvoir évaluer correctement la situation.

De manière générale et dans tous les cas où cela est possible, il convient de privilégier un hébergement et un traitement des données exclusivement dans et depuis le territoire suisse ou *a minima* un pays offrant, dans sa législation, un niveau de protection adéquat.

**c) Communication vers et/ou accès depuis un pays n'offrant pas un niveau de protection adéquat**

aa) Garanties contractuelles

aaa) Généralités

Les garanties contractuelles permettent d'encadrer le transfert des données personnelles dans un pays n'offrant pas un niveau de protection des données adéquat. Elles peuvent notamment prendre la forme de clauses contractuelles types (*Standard Contractual Clauses – SCC*) ou de règles d'entreprises contraignantes (*Binding Corporate Rules – BCR*) dans le cadre d'une communication transfrontalière au sein d'un groupe d'entreprises.

bbb) Les clauses contractuelles types (*Standard Contractual Clauses – SCC*)

Les clauses contractuelles types sont des contrats de protection des données validés par la Commission européenne et par le Préposé à la protection des données et à la transparence. Elles ont pour rôle de garantir une base contractuelle lors de communication vers un pays n'offrant pas un niveau de protection adéquat<sup>49</sup>.

---

<sup>48</sup> MEIER, N 1269, p. 441-442.

<sup>49</sup> Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil (Texte présentant de l'intérêt pour l'EEE), JO L 199 du 7 juin 2021, p. 31 ss.

Il convient de noter que les clauses contractuelles types de l'UE sont reconnues par le PFPDT mais leur utilisation n'est cependant pas obligatoire<sup>50</sup>. Cette reconnaissance permet notamment d'être exempté d'informer le PFPDT de l'utilisation des nouvelles SCC lors de chaque transfert<sup>51</sup>. Elles doivent en outre être légèrement adaptées pour se conformer aux exigences suisses<sup>52</sup>.

Depuis le 27 septembre 2021, le PFPDT ne reconnaît plus l'applicabilité des anciennes SCC dans l'élaboration de nouveaux contrats. Toutefois, une période transitoire jusqu'au 31 décembre 2022, permet aux entités concernées de mettre à jour leurs anciennes conventions afin de se conformer aux nouvelles exigences<sup>53</sup>.

Ces clauses ne seront parfois pas suffisantes. En effet, elles restent de nature contractuelle et ne peuvent faire obstacle à des mesures prises par les autorités de l'État destinataire<sup>54</sup>.

ccc) Les règles d'entreprises contraignantes (*Binding Corporate Rules* – BCR)

Les règles d'entreprises contraignantes sont des politiques de protection des données auxquelles adhèrent les entreprises établies dans l'UE pour les transferts de données à caractère personnel en dehors de l'UE, au sein d'un groupe d'entreprises<sup>55</sup>. Ces règles doivent inclure tous les principes généraux de protection des données et les droits des personnes concernées afin d'assurer la présence de garanties appropriées pour les transferts de données. Elles doivent être juridiquement contraignantes et appliquées par chaque membre concerné du groupe d'entreprises. Ces règles ne s'appliquent donc pas à des sous-traitants ultérieurs externes de l'éditeur *cloud* considéré.

---

<sup>50</sup> Préposé fédéral à la protection des données et à la transparence, Transmission à l'étranger, <<https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html>> (consulté le 21 avril 2022).

<sup>51</sup> REICHLIN/KASPER.

<sup>52</sup> REICHLIN/KASPER.

<sup>53</sup> REICHLIN/KASPER.

<sup>54</sup> FISCHER/LUBISHTANI ; Voir bb) Swiss – US Privacy Shield et arrêt Schrems II *infra*.

<sup>55</sup> CNIL, <<https://www.cnil.fr/fr/les-regles-dentreprise-contraignantes-bcr>> (consulté le 20 mai 2022) ; MÉTILLE, Internet, p. 91-92.

aa) *Swiss – US Privacy Shield* et arrêt Schrems II

Le « *Swiss – US Privacy Shield* » était un programme volontaire de transfert de données personnelles, permettant d’assurer que les entreprises étasuniennes participantes et certifiées selon ce programme, étaient présumées traiter les données de manière adéquate<sup>56</sup>.

Or, dans l’arrêt C-311/18 (arrêt « Schrems II ») du 16 juillet 2020, la Cour de Justice de l’Union Européenne (CJUE) a invalidé le « *EU – US Privacy Shield* », équivalent du « *Swiss – US Privacy Shield* » pour l’Europe<sup>57</sup>. En effet, la CJUE a constaté que ce système ne permettait pas d’établir un niveau de protection adéquat, par l’existence de programmes de surveillance de masse menés par les entités gouvernementales étasuniennes et par l’absence de moyens de droit permettant aux personnes concernées de s’y opposer devant les tribunaux<sup>58</sup>.

Le 8 septembre 2020, le Préposé fédéral à la protection des données et à la transparence (FPDPT) s’est prononcé sur le « *Swiss – US Privacy Shield* ». Il constate, à l’instar de la CJUE, que le « *Swiss – US Privacy Shield* » n’offre pas de niveau de protection des données adéquat conformément à la LPD et que la situation viole notamment les art. 13 al. 2 et 29 ss Cst<sup>59</sup>.

S’agissant des alternatives, telles que les clauses contractuelles types ou les règles d’entreprises contraignantes vues ci-dessus, il rappelle encore qu’elles « ...n’offrent pas de protection contre un accès aux données personnelles par les autorités étrangères dès lors que le droit public de l’État d’importation prévaut et autorise ce type d’accès sans garanties suffisantes en termes de transparence et de protection juridique. Ceci s’applique à la communication de données personnelles non seulement aux États-Unis, mais également dans de nombreux autres États, désignés ci-après comme « hors liste », présentant un niveau insuffisant de protection juridique. Par conséquent, il faut admettre que, dans bien des cas, les SCC et les clauses similaires ne remplissent pas les

---

<sup>56</sup> Préposé fédéral à la protection des données et à la transparence, Transmission des données aux États-Unis, <<https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland/transmission-des-donnees-aux-etats-unis.html>> (consulté le 21 avril 2022).

<sup>57</sup> CJUE, affaire C-311/18, du 16 juillet 2020, *Data Protection Commissioner contre Facebook Ireland Ltd et Maximilian Schrems*, ECLI:EU:C:2020:559.

<sup>58</sup> FISCHER ; MONTAVON, p. 516.

<sup>59</sup> Préposé fédéral à la protection des données et à l’information, Transmission à l’étranger, Prise de position sur la transmission de données personnelles vers les États-Unis et d’autres États n’offrant pas un niveau adéquat de protection des données au sens de l’art. 6, al. 1 LPD, <[https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/Positionspapier\\_PS\\_%20ED%C3%96B\\_FR.pdf.download.pdf/Positionspapier\\_PS\\_%20ED%C3%96B\\_FR.pdf](https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/Positionspapier_PS_%20ED%C3%96B_FR.pdf.download.pdf/Positionspapier_PS_%20ED%C3%96B_FR.pdf)> (consulté le 21 avril 2022).

*exigences de garanties contractuelles au sens de l'art. 6, al. 2, let. a LPD pour une transmission des données vers des États hors liste. »*

En effet, si l'annulation du « *EU – US Privacy Shield* » fait suite à l'impossibilité pour les entreprises américaines d'empêcher la surveillance et la collecte de données par des organes gouvernementaux et l'impossibilité pour les personnes concernées de faire valoir efficacement leurs droits, il est difficile d'imaginer comment des clauses contractuelles pourraient réussir là où un programme tel que le « *Swiss / EU – US Privacy Shield* » a échoué. C'est d'ailleurs le message de la CJUE dans l'arrêt précité : les clauses contractuelles types ne sont pas annulées, mais le responsable de traitement et/ou le sous-traitant devra effectivement vérifier au cas par cas si « *...le droit du pays tiers de destination assure une protection appropriée, au regard du droit de l'Union, des données à caractère personnel transférées sur le fondement de clauses types de protection des données, en fournissant, au besoin, des garanties supplémentaires à celles offertes par ces clauses.* »<sup>60</sup>.

Le comité européen de la protection des données (CEPD – EDPB) a publié un document intitulé « Foire aux questions » sur l'affaire « Schrems II » permettant d'appréhender les éléments importants de l'arrêt précité<sup>61</sup>. Pour donner suite à la décision de la CJUE précitée, il a également publié un ensemble de recommandations complémentaires pouvant permettre d'assurer la conformité lors d'une communication hors de l'Union européenne, telles que la conduite d'une analyse de risques, des mesures contractuelles, techniques et organisationnelles supplémentaires<sup>62</sup>.

Il convient donc d'effectuer une veille juridique afin de suivre les développements au niveau suisse et européen en la matière et d'effectuer un état des lieux soigneux de la situation en cas de communication transfrontière ou lors du recours à un service d'un éditeur *cloud* étasunien.

<sup>60</sup> CJUE, affaire C-311/18, du 16 juillet 2020, *Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems*, ECLI:EU:C:2020:559, § 134.

<sup>61</sup> Comité européen de la protection des données, Document FAQ sur l'arrêt de la Cour de justice de l'Union européenne C-311/18 (Schrems II), <[https://edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems\\_fr](https://edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems_fr)> (consulté le 21 avril 2022).

<sup>62</sup> Comité européen de la protection des données, Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, <[https://edpb.europa.eu/sites/default/files/consultation/edpb\\_recommandations\\_202001\\_supplementarymeasures-transfer-tools\\_fr.pdf](https://edpb.europa.eu/sites/default/files/consultation/edpb_recommandations_202001_supplementarymeasures-transfer-tools_fr.pdf)> (consulté le 21 avril 2022) ; FISCHER/LUBISHTANI.

bb) Schrems III ?

Le 25 mars 2022, la Commission européenne et les États-Unis ont annoncé qu'ils avaient convenu d'un accord de principe sur un nouveau cadre de protection des données pour les communications transatlantiques, afin de tirer les enseignements de la décision de la CJUE dans l'affaire « Schrems II » précitée, le « *Trans-Atlantic Data Privacy Framework* »<sup>63</sup>.

À l'heure où nous écrivons ces lignes, les documents juridiques sont en cours de rédaction. Il conviendra de suivre là aussi les développements en la matière et les conséquences pour la Suisse et l'État de Vaud.

Par le biais d'un communiqué de l'association NOYB dont il est le fondateur, Maximilian Schrems a d'ores et déjà réagi à cette annonce et indiqué qu'il contestera ce nouveau cadre transatlantique en cas de non-conformité au droit européen<sup>64</sup>.

### 3. *Contractualisation*

#### a) **Qualification du contrat informatique**

Le contrat informatique *cloud* se rapproche de certains contrats nommés en droit suisse. Cela étant, bien qu'il soit reconnu par l'ordre juridique suisse, il reste un contrat innomé et n'est pas réglementé dans le Code des obligations (CO ; RS 220) ou dans une loi spéciale<sup>65</sup>.

L'importance de la qualification juridique du contrat informatique permet notamment d'identifier les dispositions impératives qui lui sont propres et auxquelles aucune des parties ne peut déroger<sup>66</sup>. La nature juridique du contrat se détermine par le type de prestation, la technologie informatique et les caractéristiques particulières moyennant un prix<sup>67</sup>.

Les contrats innomés dans le domaine informatique peuvent tant se rapprocher du contrat de mandat que du contrat d'entreprise. Lorsque la prestation a pour objectif de développer un logiciel livré « clé en main » cela s'apparenterait plus

---

<sup>63</sup> Commission européenne, Communiqué de presse, Déclaration conjointe de la Commission européenne et des États-Unis sur le cadre transatlantique de protection des données personnelles, [https://ec.europa.eu/commission/presscorner/detail/fr/ip\\_22\\_2087](https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_2087) (consulté le 21 avril 2022).

<sup>64</sup> NOYB, le « Privacy Shield 2.0 » ? – Première réaction par Max Schrems, <<https://noyb.eu/fr/le-privacy-shield-20-premiere-reaction-par-max-schrems>> (consulté le 21 avril 2022).

<sup>65</sup> MÉTILLE, Administration, p. 618 ; JACCARD/ROBERT, p. 98.

<sup>66</sup> MÉTILLE, Administration, p. 618 ; JACCARD/ROBERT, p. 101.

<sup>67</sup> MÉTILLE, Administration, p. 618 ; JACCARD/ROBERT, p. 97.



à un contrat d'entreprise, puisque par exemple, le prestataire s'engage à exécuter un ouvrage contre un prix<sup>68</sup>. En revanche, lorsque la prestation s'apparente à du service comme c'est le cas pour les contrats de licence *cloud*, le contrat d'entreprise n'est plus adapté puisqu'il n'existe pas d'obligation de résultat, mais bien une obligation de moyen. Le prestataire s'engage donc à fournir une activité en vue d'obtenir un résultat sans forcément attendre de résultat vérifiable<sup>69</sup>. Les éléments mentionnés ci-dessus valent également pour le contrat de maintenance. Outre l'obligation de résultat, le mode de résiliation ainsi que le régime sur la responsabilité diffèrent également<sup>70</sup>.

## b) Difficulté de négociation

Les grandes questions que soulève la relation contractuelle avec les éditeurs peuvent, pour certaines, être réglées dans les différents contrats. La phase contractuelle est donc décisive puisqu'elle permet d'y intégrer la volonté des parties ainsi que tous les éléments essentiels du contrat et de s'assurer que les exigences définies au préalable soient respectées. Dans une grande majorité des cas, ce sont les grands éditeurs qui imposent leurs dispositifs contractuels par le biais de contrats d'adhésion à des offres standardisées. Par leur position dominante sur le marché, la probabilité d'obtenir un contrat sur mesure de la part de l'un de ces principaux éditeurs est fortement réduite pour l'administration publique. Ainsi, bien que cette dernière dispose de conditions générales qui lui sont propres, dans la pratique, il existe une difficulté majeure à imposer son propre dispositif contractuel. Par conséquent, il est parfois complexe de comprendre l'exact périmètre des prestations de l'éditeur. C'est le cas, par exemple, sur la détermination des pays où peuvent être transférées/traitées certaines données<sup>71</sup>. C'est pour cette même raison qu'il est important, avant toute contractualisation, d'analyser avec précision l'intégralité des contrats (contrat principal, contrat-cadre, contrat spécifique, SLA<sup>72</sup>, contrat de sous-traitance de protection des données personnelles) afin d'identifier s'il existe un risque juridique et trouver une solution en cas de fort impact sur la continuité de l'exploitation de l'État.

---

<sup>68</sup> MÉTILLE, Administration, p. 619.

<sup>69</sup> MÉTILLE, Administration, p. 619 ; JACCARD/ROBERT, p. 99.

<sup>70</sup> Pour une analyse détaillée des différentes qualifications du contrat : MÉTILLE, Administration ; JACCARD/ROBERT.

<sup>71</sup> CNIL, Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing, <[https://www.cnil.fr/sites/default/files/typo/document/Recommandations\\_pour\\_les\\_entreprises\\_qui\\_envisagent\\_de\\_souscrire\\_a\\_des\\_services\\_de\\_Cloud.pdf](https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf)> (consulté le 11 avril 2022).

<sup>72</sup> Accord de niveau de service (*Service Level Agreement* – SLA).

Les éléments essentiels qui ne peuvent pas être négociés dans les offres standardisées peuvent servir de point de comparaison auprès des différentes offres disponibles sur le marché afin de se déterminer sur un choix qui prendrait en compte les obligations légales du client<sup>73</sup>.

Dans tous les cas, il est recommandé, dans la relation commerciale, de prévoir dans son dispositif contractuel toutes les mesures techniques et organisationnelles dans une annexe au contrat ou par renvoi à des normes standards (p. ex. ISO 27001, 27002) dont l'éditeur garantit la certification<sup>74</sup>.

### c) **Clauses contractuelles choisies**

L'analyse des clauses ne se limite pas à la protection des données, au secret de fonction, ou encore aux SLA<sup>75</sup>, mais également à toutes les clauses sur la généralité du contrat définies dans le Code des obligations ainsi que celle spécifique aux contrats informatiques<sup>76</sup>.

Le risque doit donc être mesuré au cas par cas et, en pratique, l'analyse des éléments se fait au regard de la criticité du service, du modèle de déploiement, du type de données, mais également en fonction du modèle de service.

Pour la présente contribution, nous avons choisi de nous limiter à la présentation de certaines clauses particulièrement critiques. Dès lors, l'examen des points suivants ne saurait être exhaustif<sup>77</sup>. Lorsque l'éditeur propose un contrat, il s'agit d'analyser rigoureusement les clauses suivantes<sup>78</sup> :

#### – Cadre contractuel et hiérarchie

L'analyse hiérarchique des documents contractuels et/ou informationnels de l'éditeur a pour objectif de vérifier que l'ordre de priorité des documents soit clairement établi et fixé dans le document contractuel hiérarchiquement supérieur. En effet, les éditeurs de solution informatique en nuage font souvent référence à des spécifications, descriptions, ou documents en ligne de leurs sites internet qui peuvent être modifiés unilatéralement et qui dès lors ressemblent

---

<sup>73</sup> CNIL, <[https://www.cnil.fr/sites/default/files/typo/document/Recommandations\\_pour\\_les\\_entreprises\\_qui\\_envisagent\\_de\\_souscrire\\_a\\_des\\_services\\_de\\_Cloud.pdf](https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf)> (consulté le 11 avril 2022).

<sup>74</sup> BENHAMOU/ERARD/KRAUS ; ROSENTHAL/STUDER/LOMBARD, N 179.

<sup>75</sup> Voir à ce sujet, JACCARD/ROBERT.

<sup>76</sup> MÉTILLE, Administration, p. 619 ; JACCARD/ROBERT, p. 99.

<sup>77</sup> Voir à ce sujet, STRAUB.

<sup>78</sup> Il convient de souligner que dans la pratique, la totalité des clauses qui composent les contrats doivent être analysées avec minutie.

fortement à des clauses unilatérales. Un état des lieux permettra par exemple de déterminer les mesures nécessaires.

– Périmètre contractuel

Une description détaillée des services faisant partie du contrat permet notamment de pouvoir qualifier la nature juridique du contrat informatique<sup>79</sup> et d'y définir les droits et les obligations de chacune des parties<sup>80</sup>. La portée de cette clause a également pour intérêt d'anticiper les prestations ainsi que les coûts qui ne seraient pas identifiés dans le présent contrat ou lors des négociations<sup>81</sup>.

– Droit d'utilisation

La délimitation du droit d'utilisation demande une attention particulière. Ainsi, il est judicieux de s'assurer qu'une notification de la part de l'éditeur soit prévue en cas de dépassement dans la consommation des licences. Le but étant d'être conforme si l'éditeur devait auditer l'État de Vaud sur l'utilisation des licences. Les conséquences d'un éventuel dépassement contraindraient l'administration à payer des prestations supplémentaires non planifiées<sup>82</sup>. Dans le cas où un nombre de licences a été défini et qu'une notification de dépassement n'est pas envisageable, il est important de mettre en place à l'interne une gouvernance sur le suivi des licences.

– Modification contractuelle

Dans certains cas de figure, mais surtout lorsqu'il s'agit d'un éditeur étranger, un examen particulier doit être mené pour identifier si ce dernier renvoie à un lien *URL* de son site internet dont le contenu peut être modifié unilatéralement. Dans une grande majorité des cas, un amendement contractuel ou une modification du contrat devrait se faire par écrit et doit être consenti par les deux parties. Il s'agira de s'assurer que l'éditeur, dans cette présente clause, ne puisse modifier les termes du contrat sans un accord préalable de l'État de Vaud.

– Loi sur l'information et la transparence

Les clauses de non-divulgaration généralement présentes dans des contrats standardisés ne seront pas forcément opposables en cas de demande d'accès aux documents. En effet, certains documents peuvent vraisemblablement être considérés comme des documents officiels soumis à la Loi vaudoise du 24 septembre 2002 sur l'information (LInfo ; BLV 170.21)<sup>83</sup>. Le principe de transparence n'est cependant pas absolu puisqu'il fait l'objet d'une série

---

<sup>79</sup> JACCARD/ROBERT, p. 107.

<sup>80</sup> Voir à ce sujet, JACCARD/ROBERT ; MÉTILLE, Administration.

<sup>81</sup> JACCARD/ROBERT, p. 108.

<sup>82</sup> MÉTILLE, Administration, p. 620.

<sup>83</sup> TAF, arrêt A-1432/2016 du 5 avril 2017, c. 8.4.1,

d'exceptions, prévues à l'art. 16 LInfo qui permettent de prendre en compte les intérêts publics et privés prépondérants au maintien du secret. En effet, lorsque des documents officiels contiennent des données dignes de protection, comme des éléments critiques concernant la sécurité informatique, le refus d'accès total ou partiel peut se justifier<sup>84</sup>. Cependant, la décision de non-transmission doit rester l'exception, afin de ne pas vider le principe de transparence de sa substance.

– For et droit applicable

Dans tous les cas, il s'agit de préférer l'application du droit matériel suisse<sup>85</sup> à un droit étranger ainsi qu'un for en Suisse romande, du point de vue de l'État de Vaud. Si le droit suisse ne s'applique pas et/ou si un for à l'étranger est prévu, il s'agit dès lors de ne transmettre des données soumises au secret de fonction que de manière chiffrée<sup>86</sup>. La décision de l'acceptation du risque de l'application d'un droit étranger et/ou d'un for à l'étranger doit être prise par le-la chef-fe de service. Dans la mesure du possible, il convient d'obtenir *a minima* un for alternatif (par exemple for du défendeur) et l'application du droit matériel suisse.

#### **d) Contrat de sous-traitance de données personnelles**

Pour effectuer un état des lieux des contrats de sous-traitance, la DGNSI utilise une check-list de solution informatique externalisée de l'Autorité de protection des données et de droit à l'information du Canton de Vaud (APDI)<sup>87</sup>.

Cette liste de questions en cascade permet de déterminer les points problématiques tels que la présence ou non de données soumises au secret de fonction (art. 18 LInfo et 320 CP) ou encore la présence d'un contrat de sous-traitance du traitement de données satisfaisant. Il convient de souligner que cette *check-list* est un appui et ne dispense pas d'approfondissements si la situation de fait ou de droit l'exige. Par exemple, il peut être opportun de mener une analyse de risques de protection des données si le volume des données est important ou en présence de données sensibles<sup>88</sup>. Il convient de préciser que la LPrD ne se prononce par explicitement sur le contenu du contrat de sous-traitance de protection des données. Cela étant, à l'aide des documents disponibles au niveau

---

<sup>84</sup> TF, 1C\_235/2021 du 17 mars 2022, c. 3.2.

<sup>85</sup> MONTAVON, p. 511.

<sup>86</sup> Voir IV. B. 5.

<sup>87</sup> Annexe B. ; Voir également à ce sujet PRIVATIM.

<sup>88</sup> Voir à ce sujet, DI TRIA, AIPD.

fédéral<sup>89</sup> et européen<sup>90</sup>, et des réflexions menées en interne avec les autorités concernées, il est possible d'en dégager les clauses les plus importantes.

Si l'éditeur propose un contrat de sous-traitance de protection des données, il s'agit de procéder à une vérification des dispositions suivantes<sup>91</sup> :

- Détermination des parties : les parties au contrat doivent être suffisamment définies, afin de savoir à qui le traitement de données personnelles est effectivement sous-traité et ainsi déterminer les rôles et responsabilités de chacune des parties (responsable de traitement/sous-traitant).
- But de la sous-traitance : le but de la sous-traitance, les données concernées et le cadre dans lequel les données seront transmises doivent être définis. Le sous-traitant ne sera autorisé à traiter des données que dans ce cadre.
- Obligations des parties : le sous-traitant doit s'engager à traiter les données selon les principes généraux de protection des données prévus par la LPrD et selon les instructions du responsable de traitement, le service métier bénéficiaire. Le sous-traitant doit notamment s'engager à ne pas utiliser les données dans un autre but que celui communiqué par le responsable de traitement, cela même pour des données pseudonymes et/ou anonymes<sup>92</sup>. Le sous-traitant doit s'engager à mettre en place toutes les mesures de sécurité techniques et organisationnelles pour s'assurer de l'intégrité, de la disponibilité et la confidentialité des données et d'informer dans les plus brefs délais le responsable du traitement de tout manquement dans la sécurité des données, de tout accès indu et de toute perte de données. Le sous-traitant devra également informer le responsable du traitement de toute transmission de données à un tiers, même non prévue dans le contrat (par exemple, dans le cas d'une demande officielle comme une autorité judiciaire).
- Sous-traitance ultérieure<sup>93</sup> : il convient de limiter voire d'exclure la sous-traitance ultérieure et cas échéant, d'en préciser les contours dans le contrat. Le sous-traitant s'engagera également à transmettre au responsable du traitement la liste des sous-traitants ultérieurs. Il faut encore rappeler que le sous-traitant « primaire » reste entièrement responsable du respect

---

<sup>89</sup> PRIVATIM.

<sup>90</sup> CNIL, Sous-traitance : Exemple de clauses, <<https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses>> (consulté le 23 mai 2022).

<sup>91</sup> Liste non exhaustive ; Voir IV. B. 1.

<sup>92</sup> Par exemple, il conviendrait de s'assurer contractuellement que l'éditeur s'engage à ne pas exploiter les informations confidentielles qu'il pourrait obtenir dans l'exécution du contrat, mais uniquement à les utiliser dans l'accomplissement légitime de sa prestation. Il est donc fortement recommandé d'interdire l'éditeur ainsi que ses sous-traitants de toute formes de traitements qui leurs sont propres.

<sup>93</sup> Voir IV. B. 1.

de la LPrD et de l'éventuel secret de fonction par ses propres sous-traitants<sup>94</sup>.

- Lieux de traitement des données<sup>95</sup> : si le traitement a lieu à l'étranger, le sous-traitant doit fournir une liste de l'ensemble des pays dans lesquels des données pourront être consultées (par exemple, à des fins de maintenance ou de support) et/ou hébergées tant par lui que par ses sous-traitants ultérieurs. Si le traitement de données personnelles a lieu dans des pays disposant d'un niveau de protection adéquat les données peuvent être communiquées à l'étranger, sous réserve des données soumises au secret de fonction et pour autant que cet aspect transfrontalier soit acceptable d'un point de vue politique. Si les données sont traitées dans des pays ne disposant pas d'un niveau de protection adéquat, des garanties supplémentaires doivent être obtenues contractuellement pour s'assurer que le sous-traitant et ses éventuels sous-traitants respectent les règles de la LPrD (contrat de communication transfrontière de données)<sup>96</sup>. Une attention particulière sera accordée aux données soumises au secret de fonction<sup>97</sup>. En cas de traitement en Suisse, aucune mesure particulière supplémentaire n'est requise à ce stade. Il faut néanmoins prévoir une garantie dans ce sens dans le contrat et s'assurer que les éventuels sous-traitants en cascade traitent les données uniquement en Suisse.
- Droit de contrôle : le responsable du traitement doit avoir la possibilité de s'assurer que le sous-traitant et ses éventuels sous-traitants ultérieurs respectent bien le contrat et les obligations de protection des données. Il faut notamment pouvoir accéder à tous les documents permettant de vérifier le respect des obligations (journal d'évènements, rapports d'audits, *etc.*). Un audit doit également pouvoir être mené par le responsable du traitement auprès du sous-traitant et de ses éventuels sous-traitants ultérieurs. L'APDI doit aussi avoir la possibilité d'effectuer des contrôles ; une clause permettant la conduite d'un audit par cette dernière doit donc être prévue dans le contrat.
- Droits des personnes concernées : le sous-traitant doit être en mesure d'appuyer le responsable du traitement afin que ce dernier puisse répondre aux demandes formulées par les personnes dont les données sont sous-traitées et à fournir, dans les plus brefs délais, au responsable de traitement toutes les informations et données nécessaires pour répondre à leurs demandes. Il s'agit notamment du droit d'accès à ses propres données, du droit de destruction de données illicites, du droit de modification des données, *etc.*

---

<sup>94</sup> Voir IV. B. 5.

<sup>95</sup> Voir IV. B. 2.

<sup>96</sup> Voir IV. B. 2.

<sup>97</sup> Voir IV. B. 5.

- Responsabilités : le sous-traitant doit mettre en place toutes les mesures techniques et organisationnelles adéquates en lien avec la sécurité et les exigences de la LPrD pour le traitement des données transmises dans le cadre de la sous-traitance. Il doit également être prévu que le sous-traitant est également responsable pour les faits des sous-traitants ultérieurs qu'ils soient autorisés ou non. Une indemnisation pleine et entière pour l'ensemble des dommages directs et indirects subis par le responsable du traitement et causés par le sous-traitant ou un sous-traitant ultérieur devrait être prévue.
- Résiliation du contrat : le contrat doit prévoir un droit de résiliation par le responsable du traitement, moyennant le respect d'un préavis, sauf dans les cas où de justes motifs (à prévoir dans le contrat ; problèmes graves de sécurité par exemple) permettent de résilier immédiatement le contrat. Les conséquences de la résiliation du contrat doivent être prévues, notamment la restitution, le rapatriement et la destruction dans les plus brefs délais de toutes les données et toutes les copies de ces données. Il est aussi utile de prévoir la transition vers un autre sous-traitant. En particulier, il peut être intéressant de prévoir un délai suffisamment long pour permettre à l'État de Vaud de choisir et implémenter une autre solution *cloud* ou *on premise*. Enfin, il convient également de prendre connaissance des éventuels frais de sortie qui peuvent être des coûts supplémentaires non prévus.
- For et droit applicable : Voir IV. B. 3. c).

Dans la pratique, lorsque le contrat de sous-traitance de données personnelles ne correspondrait pas aux standards d'exigences de l'État de Vaud, il conviendrait dans un premier lieu d'exiger d'éventuels amendements et/ou modifications. En cas de négociations infructueuses, il est fortement recommandé d'en refuser la signature<sup>98</sup>.

#### 4. *Marchés publics*

En tant que pouvoir adjudicateur, l'administration publique est soumise à la législation sur les marchés publics pour les acquisitions de services informatiques en nuage<sup>99</sup>. En effet, ces derniers entrent notamment dans le champ d'application de l'Accord international révisé du 15 avril 1994 sur les marchés publics (AMP ; RS 0.632.231.422), de l'Accord intercantonal des 25 novembre 1994/15 mars 2001 sur les marchés publics (AIMP ; RO 2003 196), ainsi que de la Loi vaudoise du 24 juin 1996 sur les marchés publics (LMP-VD ;

---

<sup>98</sup> Il est cependant toujours possible de proposer le contrat de sous-traitance de protection des données de l'État de Vaud.

<sup>99</sup> POLTIER, N 60, p. 33.

BLV 726.01) et son Règlement d'application du 7 juillet 2004 (RLMP-VD ; BLV 726.01.01).

Le service métier qui souhaite utiliser une solution *cloud* dispose donc d'une certaine liberté dans la définition de ses besoins et dans la configuration du marché. Il est donc libre de choisir ce qui doit être réalisé et obtenu de la part des futurs soumissionnaires dans le cadre d'une procédure d'appel d'offres. Cette dernière a pour but de garantir une utilisation rationnelle des fonds publics mais œuvre également pour une concurrence saine par l'ouverture du marché<sup>100</sup>.

La configuration du marché ainsi que les besoins métiers identifiés doivent, en sus des dispositions relatives aux marchés publics, respecter les législations transversales comme la loi sur la protection des données ainsi que toutes les exigences liées au secret de fonction. Ces dernières ont pour conséquence, contrairement aux droits des marchés publics, de restreindre le périmètre du marché notamment pour des motifs de sécurité de l'information et de dépendance à de potentiels acteurs étrangers. L'adjudicateur devra donc faire en sorte d'harmoniser et garantir la correcte application de diverses législations qui lui sont applicables et qui peuvent parfois paraître contradictoires.

La territorialité des données et la souveraineté numérique sont des défis centraux et incontournables pour les administrations publiques. En effet, la maîtrise des données et la sécurité vont très souvent dépendre du type de technologie, mais surtout de l'éditeur de la solution et *de facto* de sa localisation. Comme susmentionné, le pouvoir adjudicateur est en principe libre des critères qu'il mentionnera dans l'appel d'offres, mais au regard de la problématique de dépendance à des acteurs privés étrangers, il est important de rechercher dans un premier temps une équivalence suisse ou européenne ainsi que de démontrer sa valeur ajoutée. Sous l'angle de la protection des données, du secret de fonction et des marchés publics, l'utilisation du *cloud* requiert donc des dispositifs de sécurité techniques et organisationnels pouvant restreindre géographiquement le marché.

Comme présenté dans le chapitre sur la souveraineté numérique, l'aspect décentralisé du *cloud* comporte des enjeux de territorialité notamment sous l'angle de la LPrD<sup>101</sup>. Il est donc primordial, dans les différents documents qui constituent l'appel d'offres, de prévoir des critères restrictifs qui garantissent le respect des diverses exigences en sachant que lors de la publication, aucun des futurs soumissionnaires n'est connu<sup>102</sup>. Ces exigences transversales se traduisent notamment par la mise en place de conditions de participation pouvant

---

<sup>100</sup> POLTIER, Avant-Propos, p. V ; Art. 1 de l'Accord intercantonal sur les marchés publics (AIMP), BLV 726.91.

<sup>101</sup> Voir III. B.

<sup>102</sup> Rapport Cdc N° 67, p. 25.



parfois aller à l'encontre de l'essence même de l'ouverture mutuelle des marchés. En effet, ces critères ont pour résultat de restreindre volontairement le marché à certains futurs soumissionnaires potentiels, qui ne pourraient pas être en mesure de garantir la bonne application des exigences de protection des données ou du secret de fonction<sup>103</sup>.

Néanmoins, il est important de rappeler qu'il est formellement interdit de recourir à des spécifications techniques discriminatoires propres à tailler le marché sur mesure pour un soumissionnaire bien précis ou qui ont pour effet de pénaliser ou avantager certains soumissionnaires par rapport à d'autres sans justification<sup>104</sup>. Ainsi, la réduction du périmètre de la concurrence peut parfois se justifier pour les raisons susmentionnées. Dès lors, la complexité de l'élaboration du cahier des charges réside pour le service métier de l'État dans l'harmonisation des diverses législations.

L'adjudication de gré à gré exceptionnelle en faveur d'une solution informatique spécifique ne sera volontairement pas abordée dans ce paragraphe, mais elle permet notamment de choisir directement un soumissionnaire connu si elle respecte les conditions de l'art. 8 RLMP-VD<sup>105</sup>.

## 5. *Secret de fonction*

Conformément à l'art. 18 de la LInfo, il est interdit aux collaboratrices de la fonction publique ainsi qu'aux délégataires d'une tâche publique de divulguer des informations ou des documents officiels dont ils ont eu connaissance dans l'exercice de leur fonction, et qui doivent rester secrets en raison de la loi ou d'un intérêt public ou privé prépondérant. Cette obligation de garder le secret subsiste après la cessation des rapports de service. La violation du secret de fonction au sens de ce qui précède est sanctionnée par l'art. 320 CP<sup>106</sup>.

Seule une information qui n'est connue ou accessible qu'à un cercle restreint de personnes, que son détenteur veut garder secret et qui y a un intérêt légitime

---

<sup>103</sup> Par exemple, c'est le cas lorsque la valeur du marché dépasse les valeurs seuils fixées par les accords internationaux contractés par la Suisse et qui ont pour effet principal d'ouvrir les marchés publics suisses aux entreprises étrangères. Dans ce cas si on exigeait, dans les conditions de participations, que seul un soumissionnaire dont le traitement de données serait exclusivement en Suisse pourrait entrer en ligne de compte, le critère discriminant viendrait réduire le périmètre du marché bien que l'on soit dans les seuils internationaux.

<sup>104</sup> Art. 11 al. 1 lit. a AIMP.

<sup>105</sup> POLTIER, N 251, p. 157 ; JAQUIER, p. 1.

<sup>106</sup> À titre d'exemple, « *Le collaborateur en télétravail accorde une attention particulière au respect du secret de fonction et à la confidentialité des données traitées.* » (art. 118e RLPers-VD).

sera considérée comme secrète et protégée par les dispositions précitées. Cette information doit encore avoir été acquise dans le cadre de l'exercice de la fonction<sup>107</sup>.

Le secret de fonction sert deux objectifs. Premièrement, il a pour but de protéger le bon fonctionnement de l'administration. Deuxièmement, il est fondamental pour protéger la personnalité des personnes privées qui sont obligées de communiquer des informations à l'État<sup>108</sup>.

Il convient de souligner que l'entrée en vigueur des lois fédérales et cantonales en matière de transparence et de droit à l'information a renversé le paradigme du « secret d'État » depuis deux décennies désormais. La portée du secret de fonction a donc été réduite, étant donné que le principe est la publicité des documents officiels<sup>109</sup>.

Pour être punissable, la divulgation d'une information protégée par un secret doit se faire envers une personne non autorisée. Dès lors, en matière de *cloud*, il s'agit de déterminer si l'éditeur, généralement qualifié de sous-traitant en matière de protection des données, peut être considéré comme un auxiliaire du détenteur du secret de fonction, par analogie à ce qui est prévu pour le secret professionnel (art. 321 CP). Il convient de préciser que le Tribunal fédéral considère que l'obligation de tenir le secret n'a pas besoin d'être inscrite dans une loi au sens formel. L'art. 320 CP englobe tous les secrets confiés à un fonctionnaire ou dont il a pris connaissance en raison de sa fonction, indépendamment de savoir si une norme spéciale l'oblige à garder le secret<sup>110</sup>.

ERARD et MONTAVON ont dressé un état des lieux de la doctrine sur la question<sup>111</sup>. Les avis sont aussi divers que variés, notamment sur la notion d'auxiliaire du secret de fonction, des spécificités propres à certaines branches de l'économie (secteur bancaire, santé publique, secret professionnel de l'avocat, *etc.*) et enfin les implications et conséquences d'une externalisation auprès d'un auxiliaire situé en Suisse ou à l'étranger quant à l'application d'une norme pénale.

Cette problématique est plus actuelle qu'il n'y paraît : le 9 mars 2022, la Conseillère nationale verte Léonore Porchet a posé la question suivante au Conseil national<sup>112</sup>,

---

<sup>107</sup> MÉTILLE, *Administration*, p. 611.

<sup>108</sup> MOOR/BELLANGER/TANQUEREL, p. 608.

<sup>109</sup> MONTAVON, p. 492-493.

<sup>110</sup> FRANCEY ; ATF 142 IV 65, c. 5.2.

<sup>111</sup> ERARD, p. 191 ss. et p. 507 ss ; MONTAVON, p. 496-510.

<sup>112</sup> Conseil national, Heure des questions, Porchet Léonore, 22.7249, <<https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20227249>> (consulté le 26 avril 2022).

*« La pratique juridique est divisée : une violation de l'art. 320 du Code pénal peut-elle découler de l'utilisation de services de cloud et d'hébergement de données à l'étranger ? Ce flou fait courir un risque pénal réel aux fonctionnaires. Le Conseil fédéral considère-t-il que l'usage d'un service de cloud à l'étranger par une entité soumise à l'art. 320 CP en constitue une violation ou est-ce devenu tellement courant que l'art. 320 CP doit être interprété restrictivement ? »*

Le 14 mars 2022, la Conseillère fédérale Karin Keller-Sutter a répondu comme suit<sup>113</sup> :

*« Selon le droit en vigueur, les fournisseurs de services TIC externes à l'administration ne sont en principe pas considérés comme des fonctionnaires de fait, ceci selon l'article 110 chiffre 3 du code pénal. Dès lors, ils ne sont aujourd'hui pas tenus de garder les secrets de fonction qu'ils détiennent dans l'exercice de leur activité, selon l'article 320 chiffre 1 du code pénal. Considérant que le droit actuel était lacunaire sur ce point, le Parlement a modifié l'article 320 du code pénal. À l'avenir, les auxiliaires pourront également répondre de violation du secret de fonction. Cette révision devrait entrer en vigueur en 2023 et s'appliquera également à un prestataire de services TIC à l'étranger. Le Conseil fédéral est conscient du fait que la mise en œuvre du droit pénal suisse contre un prestataire à l'étranger peut se heurter à des difficultés pratiques. Cela étant dit, dans le cadre du droit futur comme du droit actuel, il appartiendra aux tribunaux de juger au cas par cas s'il y a ou non infraction à l'article 320 du code pénal. »*

La nouvelle mouture de l'art. 320 CP prévoira donc expressément la notion d'auxiliaire du secret de fonction<sup>114</sup>. Ces derniers seront légalement soumis au secret de fonction : la révélation du secret dans ce cadre ne sera en principe pas punissable. Toutefois, il s'agira de choisir l'éditeur avec soins si des données, informations ou documents soumis au secret de fonction devaient lui être confiés<sup>115</sup>.

Si cet éclaircissement est bienvenu, la question du secret de fonction dans le cadre d'une communication transfrontière reste ouverte. En effet, si l'éditeur auxiliaire du secret de fonction est étranger (et soumis à un droit étranger) ou si les données soumises au secret se trouvent à l'étranger, il semble difficile d'opposer une norme de droit suisse à une requête officielle et valable d'une

<sup>113</sup> Conseil national, Heure des questions, Keller-Sutter Karin, 22.7249, <<https://www.parlament.ch/fr/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=56301>> (consulté le 26 avril 2022).

<sup>114</sup> Message LSI 2020, FF 2020 9665, p. 9700.

<sup>115</sup> MÉTILLE, Administration, p. 614.

autorité étrangère sur son territoire et de sanctionner cette entité de l'éditeur sise à l'étranger.

Par conséquent et de ce point de vue, seul l'appel à un auxiliaire suisse qui se trouve en Suisse permettrait de s'assurer de la bonne protection du secret, moyennant un choix, une instruction et un contrôle soigneux de la part du détenteur « *primaire* »<sup>116</sup>.

Toutefois, une interdiction totale d'externalisation des données soumises au secret de fonction hors du territoire suisse ou de faire appel à un éditeur étranger semble disproportionnée pour deux raisons : premièrement, tous les éditeurs *cloud* n'ont pas d'intérêts à s'implanter sur le territoire suisse, cela pour diverses raisons économiques et pratiques. Cela impliquerait, par défaut, de renoncer à des offres de certains éditeurs à la pointe dans leur domaine de compétence. Ensuite, le fait d'héberger des données auprès d'un éditeur *cloud* étranger dont les serveurs sont en Suisse n'est pas une garantie absolue contre une violation du secret de fonction, par un accès indu ou la coopération de l'éditeur avec un gouvernement étranger<sup>117</sup>.

Le chiffrement des données pourrait-il apporter une réponse à cette problématique ? Si l'éditeur *cloud* ne possède pas la clé de chiffrement et qu'il n'a aucune possibilité d'accéder aux données en clair, il n'y aura pas de violation du secret de fonction, même en cas d'hébergement à l'étranger<sup>118</sup>. Si cela est correct d'un point de vue théorique et dans le cas d'un simple service d'hébergement de données, il en est tout autre en réalité. En effet, la plupart des services *cloud* proposés vont plus loin et offrent de véritables solutions logicielles et de traitements complexes. Dès lors, l'éditeur doit être en mesure de déchiffrer les données afin de permettre la bonne exécution du contrat et pour assurer le support<sup>119</sup>. De manière générale, dans les situations où l'État de Vaud n'a pas la possibilité de gérer lui-même la clé de chiffrement (*Bring Your Own Key* – BYOK<sup>120</sup>), la prudence impose de partir du principe que l'éditeur aura un moyen d'accéder aux données en clair.

Afin de réduire le risque, des garanties contractuelles avec l'éditeur *cloud* doivent être implémentées. En premier lieu, ce dernier doit s'engager à n'accéder aux données que lorsque cela est strictement nécessaire à l'exécution de la prestation. Ensuite, en fonction du secret et des risques en jeu, les collaborateurs-trices de l'éditeur peuvent être tenu-e-s de signer un accord de confidentialité avec rappel des enjeux sur cette problématique.

---

<sup>116</sup> MÉTILLE, Administration, p. 614.

<sup>117</sup> MONTAVON, p. 507.

<sup>118</sup> MÉTILLE, Administration, p. 615.

<sup>119</sup> MÉTILLE, Administration, p. 615 ; MONTAVON, p. 508-509.

<sup>120</sup> ROSENTHAL, p. 37.

Le contrat peut également prévoir des peines conventionnelles suffisamment sévères et dissuasives afin de limiter le risque de violation du secret par l'éditeur<sup>121</sup>. Dans la pratique, même si nous constatons un gain de maturité des éditeurs de solutions *cloud* sur ces questions, la notion de secret de fonction et plus généralement les exigences particulières d'une entité publique restent relativement floues et difficiles à appréhender pour des entreprises privées et parfois étrangères.

Enfin, il appartient au service métier bénéficiaire de l'État de Vaud d'effectuer un état des lieux et une analyse de risques concernant cette problématique. En effet, c'est le service bénéficiaire qui a la connaissance et la compétence s'agissant de l'appréhension de ses propres règles sectorielles. La DGNSI pourra toutefois attirer son attention et l'appuyer dans ses réflexions dans l'optique de la décision d'opter ou non pour une solution *cloud* au regard des circonstances.

## V. Réponses

### A. Politique d'utilisation de solution informatique externalisée

#### 1. Généralités

Pour un besoin fonctionnel spécifique, le service métier a parfois le choix entre des solutions informatiques dites classiques « *on premise* » et des solutions informatiques externalisées. Par solutions informatiques externalisées, on entend notamment les services d'un éditeur de solution informatique en nuage qui se trouvent hors des systèmes d'information sous maîtrise de l'administration. L'adaptation des processus métiers lors du recours à une solution externalisée comme le *cloud* soulève divers enjeux en matière numérique, décrits notamment dans les sections II., III. et IV. de la présente contribution.

Contrairement aux solutions informatiques « *on premise* », le recours à l'informatique en nuage exige une attention particulière dans l'évaluation des risques. En effet, les éditeurs susceptibles d'offrir des services à la mesure d'une entité comme l'État de Vaud font parfois partie d'entreprises situées à l'étranger. Cela entraîne une perte de maîtrise considérable ainsi qu'un enjeu de territorialité et de dépendance à des acteurs étrangers. Dès lors, des garde-fous doivent être mis en place lors du choix du fournisseur tant d'un point de vue juridique que politique.

Lorsqu'un service métier souhaite utiliser une solution *cloud*, il doit dans un premier temps effectuer une analyse de risques en amont de toute potentielle

---

<sup>121</sup> MONTAVON, p. 509-510.

contractualisation tant au regard de la loi sur les marchés publics que de la stratégie numérique<sup>122</sup>. En effet, il se peut qu'une pesée des intérêts en présence démontre qu'il n'est pas opportun d'externaliser cette tâche de l'État et de faire appel à un tiers prestataire malgré la conformité de la solution informatique externe envisagée.

Cette première étape passée, la demande du service métier est évaluée au travers de deux étapes mises en place par la DGNSI : l'analyse au travers de la grille d'analyse de la Politique d'utilisation de solution informatique externalisée puis la formulation d'un préavis par le comité d'experts délégués au numérique (CEDN), créé à cette fin<sup>123</sup>.

## 2. *Grille d'analyse de la Politique d'utilisation de solution informatique externalisée*

L'évaluation et le choix de la technologie *cloud* est une décision importante qui mérite une réflexion pluridisciplinaire tant sur le volet technique, politique que juridique. Sur la base de la politique d'utilisation de solution informatique externalisée, une grille d'analyse a été élaborée. Il s'agit d'un outil de travail permettant aux services métiers, aux architectes d'entreprise ainsi qu'aux juristes de passer la solution envisagée au crible des critères fixés par la politique d'utilisation de solution informatique externalisée<sup>124</sup>. Ces critères, ou principes, sont les suivants :

### 1. Opportunité de faire appel à un prestataire externe

Le préambule de ce document doit mentionner le projet d'étude ainsi que la justification que la solution choisie est celle qui répond le mieux aux exigences politiques, légales, métiers, sécuritaires, financières.

De plus, le service métier doit être en mesure de traiter les éventuels impacts et assumer les possibles conséquences « politiques » de l'utilisation d'une solution *cloud* notamment en cas de fuite d'information, ou encore en cas d'indisponibilité prolongée.

### 2. Intégration avec les systèmes d'information existants

Le recours à une solution *cloud* doit non seulement être aligné avec la stratégie du système d'information, à la stratégie du service métier ainsi

---

<sup>122</sup> Voir III. A.

<sup>123</sup> Voir V. B.

<sup>124</sup> Annexe A. ; Rapport Cdc N° 74, p. 74.

qu'à la stratégie numérique cantonale, mais elle doit aussi être compatible avec le système de supervision interne.

### 3. Économique

Les solutions informatiques externalisées suisses doivent être favorisées dans le respect du droit des marchés publics<sup>125</sup>.

### 4. Protection des données

La solution informatique externalisée est analysée ici sous l'angle de la protection des données. Il s'agit d'identifier les documents contractuels ou informationnels de l'éditeur permettant d'effectuer un état des lieux sur le volume, le type, les catégories et le caractère sensible ou non des données concernées et de vérifier que le traitement envisagé reste dans le cadre prévu par la loi ou la tâche publique<sup>126</sup>. De la même manière, c'est principalement à cette étape que la check-list pour contrat de sous-traitance de solution informatique externalisée est utilisée<sup>127</sup>.

### 5. Disponibilité de la solution externalisée

La délivrance des prestations de l'État ne doit pas être lourdement impactée en cas d'indisponibilité de la solution informatique externalisée.

Un plan de secours informatique (PSI ou *DRP*)<sup>128</sup> doit être défini et acceptable par le service métier en cas d'arrêt de la solution informatique *cloud* ou d'une rupture du contrat. Ce plan doit être fourni par l'éditeur en amont de la contractualisation.

Le service métier doit en outre instruire, avant la contractualisation, un plan de continuité des activités (PCA) en cas d'indisponibilité de la solution.

La qualité de service doit être clairement définie et acceptée par le service métier, par le biais d'un accord de niveau de service (*Service level agreement* – SLA).

### 6. Contractualisation

La phase contractuelle suit l'attribution du marché et commence lorsque toutes les conditions légales préliminaires sont remplies.

La contractualisation doit prévoir une analyse de risques sur l'intégralité du dispositif contractuel dans le but de prévoir des garanties suffisantes.

---

<sup>125</sup> Voir IV. B. 4.

<sup>126</sup> Voir IV.

<sup>127</sup> Annexe B.

<sup>128</sup> *Disaster Recovery Plan* (ou plan de reprise d'activité ou plan de continuité d'activité).

Les divers contrats doivent intégrer les exigences minimales en matière de sécurité et de protection des données ainsi que toutes les clauses qui régissent la partie générale<sup>129</sup>.

## 7. Dispositions sectorielles

Dans le cas où des lois ou des directives spécifiques à un service métier pourraient entraîner des conséquences sur les modalités d'utilisation et/ou de contractualisation avec la solution informatique externalisée, celles-ci doivent être examinées et traitées par le service métier.

## 3. *Comité d'experts délégués au numérique (CEDN)*

Une fois la grille d'analyse complétée par les rédacteurs, elle est remise aux membres du Comité d'experts délégués au numérique CEDN afin d'aider les services métiers à effectuer une prise de décision sur la solution informatique en nuage envisagée.

Le CEDN a été constitué en réponse aux problématiques posées par le recours aux solutions informatiques dans le cloud. Par la création du CEDN, la DGNSI a souhaité réunir différents acteurs de l'administration cantonale au sein d'un comité informel pour échanger sur cette thématique et porter la vision de la stratégie numérique auprès des services bénéficiaires de l'État de Vaud qui souhaitent développer leurs services informatiques dans le *cloud*. Ce groupe d'experts se compose de différentes parties prenantes et se réunit pour échanger sur les projets qui lui sont soumis. Les aspects de sécurité de l'information, de protection des données, de développement économique sont pris en compte lors d'une analyse détaillée<sup>130</sup>.

En se basant sur la grille d'analyse dûment remplie, ce comité évalue et émet un préavis sur l'appréciation des risques, sous l'angle politique/métier par le biais d'une réunion ou par voie de circulation selon la criticité<sup>131</sup>. Ce préavis constitue une recommandation mais n'est pas contraignant pour les services concernés. Par conséquent, un préavis positif ou négatif ne présume pas de sa potentielle mise en service.

Cette initiative permet de faire évoluer la culture de la protection des données au sein de l'État de Vaud. Elle s'inscrit également dans la volonté exprimée par

---

<sup>129</sup> Voir IV. B. 3.

<sup>130</sup> Voir V. A.

<sup>131</sup> La criticité s'apprécie notamment au regard du type de données, du périmètre contractuel, du volume du traitement, de l'ampleur du projet ainsi que du type d'éditeur.



le Conseil d'État dans sa stratégie numérique d'établir une gouvernance claire aussi au sein de son administration pour conduire sa transformation numérique<sup>132</sup>.

## B. Politique de la donnée

Conscient de l'importance fondamentale des données dans le contexte de la transition numérique et des enjeux qui y sont associés, le Canton de Vaud met en place une politique de la donnée. Son objectif est de trouver un juste équilibre entre la protection et la valorisation des données. D'une part, on assiste à une mise en données du monde qui a un impact sur le respect de la sphère privée, tel que prévu par l'art. 13 de la Constitution fédérale et par l'art. 15 de la Constitution du Canton de Vaud du 14 avril 2003 (Cst-VD ; BLV 101.01). Et d'autre part, on constate les impacts positifs que l'analyse des données peut avoir dans l'élaboration de solutions ou la compréhension de problèmes.

La mise en œuvre de cette politique de la donnée se déroulera dans différents domaines : la culture de la donnée pour faire évoluer les compétences des individus dans le traitement de leurs propres données mais également dans les traitements qu'ils sont amenés à réaliser dans le cadre de leur travail ; la gouvernance des données ; la valorisation des données par l'utilisation progressive de nouvelles technologies telles que l'intelligence artificielle ou plus généralement la science des données ; la mise à disposition de données publiques ; la veille technologique et le développement des infrastructures.

## C. Cloud souverain – Étude d'opportunité

Dans le cadre de l'élaboration de sa politique de la donnée, le Canton de Vaud a souhaité mener une réflexion sur la nécessité d'un *cloud* souverain. Par « *cloud* souverain » on entend le développement d'une informatique en nuage, où les orientations politiques des administrations publiques sont prises en compte. Il s'agit là de donner corps à la notion de souveraineté numérique, en partant de la thématique du *cloud* souverain et des différentes variables qui le caractérisent<sup>133</sup>.

Ainsi, le Canton de Vaud, dans le contexte de la Conférence latine des directeurs du numérique (CLDN) et en collaboration avec d'autres cantons, a lancé une étude d'opportunité sur cette thématique<sup>134</sup>. Dans le cadre d'une réflexion

---

<sup>132</sup> Voir également à ce sujet, Rapport Cdc N°67.

<sup>133</sup> Pour un aperçu des réflexions au niveau de l'Union européenne à ce sujet : BENHAMOU.

<sup>134</sup> Annexe C.

globale sur la souveraineté numérique mais également aux prises avec le développement de leur informatique respective, les cantons abordent aujourd'hui cette question pour d'une part définir de manière plus précise la notion de souveraineté dans le cadre des technologies *cloud* et d'autre part évaluer différentes variantes de faisabilité. L'objectif est de donner à chaque canton participant la possibilité de poser le curseur politique par rapport à sa vision et son interprétation de la souveraineté numérique, tout en explorant la possibilité de mutualisation.

Dans un premier temps, l'étude identifiera et analysera les enjeux et les dimensions liés à la mise en place d'un *cloud* souverain, d'un point de vue de l'usage et de la création, tels que la cybersécurité, la localisation des données, les types de services, les aspects financiers, le modèle économique, la dépendance, les aspects juridiques et la souveraineté numérique.

Ensuite, l'étude procédera également à un rapide tour d'horizon sur l'utilisation du *cloud* dans les différents cantons, non seulement concernant l'utilisation actuelle, mais également sur les perspectives et les besoins d'utilisation future. L'étude devra également identifier les acteurs locaux et faire une analyse de leur offre en matière de *cloud* en lien avec l'offre des acteurs internationaux, en particulier de type « *hyperscaler* ».

Dans un deuxième temps, l'étude devra identifier et analyser les enjeux liés à la création d'un *cloud* souverain, en lien avec les différentes dimensions décrites ci-dessus, sous l'angle des conséquences sur le rôle de l'État dans la société numérique.

Dans un dernier temps, elle devra donner des pistes d'action (technologiques, réglementaires, politiques, de gouvernance, *etc.*) et des variantes pour la réalisation d'un *cloud* souverain qui permette à l'État, dans le contexte fédéral suisse, de jouer son rôle sous ses différentes casquettes (administration, service public, propriétaire d'infrastructure, ...) dans le cadre d'une société numérique en construction et qui bénéficie à l'ensemble des parties prenantes.

Les résultats de cette étude, attendus à la fin 2022, permettront de poser le cadre du développement futur pour réaliser pleinement – ou dans la proportion la plus acceptable et souhaitable par l'autorité politique – un *cloud* souverain en Suisse.

## VI. Conclusion

Les solutions informatiques en nuage permettent une modernisation des systèmes d'information telle qu'exprimée dans le programme de législature 2017-2022 mais appellent dans le même temps à instaurer des garde-fous

afin de minimiser les risques encourus par l'État de Vaud, tant pour la résilience de ses systèmes d'information que pour la protection des données qu'il détient<sup>135</sup>.

La présente contribution met en évidence les enjeux et les problématiques imposées par le recours à l'informatique en nuage. Que ce soit en matière de souveraineté numérique, d'intégration technique ou de maîtrise des données, le choix du *cloud* n'est pas anodin. Il n'en va pas autrement d'un point de vue juridique : que ce soit sous l'angle des bases légales, de la protection des données, des aspects contractuels, des exigences en matière de marchés publics ou encore du secret de fonction, l'analyse requiert l'intégration d'une multitude de paramètres complexes et protéiformes.

L'implication de toutes les parties prenantes ainsi qu'une étude fine des enjeux stratégiques, politiques, économiques et juridiques est nécessaire afin d'identifier tous les éléments permettant aux entités concernées de pouvoir se déterminer en connaissance de cause et d'accepter ou non le ou les risques résiduels.

En décembre 2021, la Cour des comptes du Canton de Vaud a publié son rapport d'audit de la protection des données personnelles dans l'administration cantonale vaudoise<sup>136</sup>. Il est constaté une certaine marge d'amélioration, notamment en matière de contrats de sous-traitance et d'analyse de risques pour l'administration cantonale vaudoise. Les recommandations formulées portent principalement sur deux aspects. D'une part, certaines bases légales doivent être mises à jour et adaptées. Les documents contractuels types de la DGNSI doivent par exemple, eux aussi, subir une cure de jouvence. D'autre part, la Cour des comptes souligne l'importance de posséder une véritable culture de la protection des données en recommandant notamment une cartographie des données traitées et leur criticité, ainsi qu'une meilleure formation des collaborateurs-trices en matière de protection des données, de sécurité informatique et de secret de fonction.

Enfin, l'étude d'opportunité « *cloud* souverain » apportera certainement des éléments de réponse pour les administrations publiques aux prises avec le choix de l'informatique en nuage et permettra d'identifier les leviers permettant de se moderniser tout en limitant les risques. Il s'agit de poursuivre les efforts entrepris depuis une dizaine d'années afin de gagner en maturité à tous les niveaux,

---

<sup>135</sup> Programme de législature 2017-2022 du Conseil d'État du Canton de Vaud, <<https://www.vd.ch/toutes-les-autorites/conseil-detat/programme-de-legislature-2017-2022/>> (consulté le 27 avril 2022).

<sup>136</sup> Rapport No 74 : La protection des données personnelles dans l'Administration cantonale vaudoise, ([https://www.vd.ch/fileadmin/user\\_upload/organisation/cour\\_comptes/1\\_Rapports\\_d\\_audit/74\\_Rapport.pdf](https://www.vd.ch/fileadmin/user_upload/organisation/cour_comptes/1_Rapports_d_audit/74_Rapport.pdf)), consulté le 27.04.2022.

dans le but de bâtir une administration moderne, agile, efficiente et respectueuse des droits fondamentaux des personnes concernées dont elle traite les données.

## VII. Bibliographie

### A. Littérature

**Bruno BAERISWYL/Beat RUDIN (éds)**, Praxiskommentar zum Informations- und Datenschutzgesetz des Kanton Zürich, IDG, Zürich 2012 (cité : AUTEUR, *in* : PK IDG) ; **Eva Maria BELSER/Astrid EPINEY/Bernhard WALDMANN (éds)**, Datenschutzrecht – Grundlagen und öffentliches Recht, Berne 2011 (cité : AUTEUR, *in* : BELSER/EPINEY/WALDMANN) ; **Yaniv BENHAMOU**, Souveraineté numérique et altruisme des données (« Data Altruism ») : proposition UE de « Data Governance Act », 4 décembre 2020 *in* : <www.swissprivacy.law/39> ; **Yaniv BENHAMOU/Frédéric ERARD/Daniel KRAUS**, L’avocat a-t-il aussi le droit d’être dans les nuages ?, Revue de l’avocat, 2019/3, p. 119 ; **Livio DI TRIA**, L’analyse d’impact relative à la protection des données (AIPD) en droit européen et suisse, *in* : Sic ! 2020/3, p. 119 ss (cité : DI TRIA, AIPD) ; **Livio DI TRIA**, La Suisse se dote (enfin) d’une nouvelle Loi fédérale sur la protection des données – Tour d’horizon sur ce qu’elle réserve, 30 septembre 2020, *in* : <www.swissprivacy.law/12> (cité : DI TRIA, nLPD) ; **Frédéric ERARD**, Le secret médical, Étude des obligations de confidentialité des soignants en droit suisse, thèse Zürich 2021 ; **Philipp FISCHER**, Schrems II ou la quadrature du cercle, 18 octobre 2020, *in* : <www.swissprivacy.law/17> ; **Philipp FISCHER/Kastriot LUBISHTANI**, Mesures techniques, contractuelles et organisationnelles à observer suite à l’arrêt Schrems II, 7 décembre 2020, *in* : <www.swissprivacy.law/40> ; **Julien FRANCEY**, La violation du secret de fonction (art. 320 CP), *in* : <www.lawinside.ch/225/> ; **Michel JACCARD/Vincent ROBERT**, les contrats informatiques, *in* : Pichonnaz Pascal/Werroz Franz (édit), La pratique contractuelle : actualité et perspectives – Symposium en droit des contrats, Genève 2009, p. 95 ss. ; **Manuel JAQUIER**, Le « gré à gré exceptionnel » dans les marchés publics, thèse Genève, Zürich, Bâle 2018 ; **Urs MAURER-LAMBROU/Gabor P. BLECHTA (éds)**, Basler Kommentar, Datenschutzgesetz – Öffentlichkeitsgesetz, 3<sup>e</sup> éd., Bâle 2014 (cité : BSK DSG-AUTEUR) ; **Philippe MEIER**, Protection des données – Fondements, principes généraux et droit privé, Berne 2011 ; **Sylvain MÉTILLE**, L’utilisation de l’informatique en nuage par l’administration publique, *in* : PJA 2019, p. 609 ss (cité : MÉTILLE, Administration) ; **Sylvain MÉTILLE**, Internet et droit – Protection de la personnalité et questions pratiques, Genève 2017 (cité : MÉTILLE, Internet) ; **Michael MONTAVON**, Cyberadministration et protection des données, thèse Genève, Zürich, Bâle 2021 ; **Pierre MOORE/François BELLANGER/Thierry TANQUEREL**, Droit administratif, volume III, L’organisation des activités administratives. Les biens de l’État, 2<sup>e</sup> éd., Berne 2018 ; **Etienne POLTIER**, Droits des marchés publics, Berne 2014 ; **PRIVATIM**, Aide-mémoire sur les risques et les mesures spécifiques à la technologie du Cloud, version 3.0 du 3 février 2022 ; **Jeremy REICHLIN/Gabriel KASPER**, Reconnaissance des SCC par la Suisse : tour d’horizon pour les entreprises helvétiques, 15 septembre 2021 *in* : <www.swissprivacy.law/91> ; **David ROSENTHAL**, Mit Berufsgeheimnissen in die Cloud : So geht es trotz US CLOUD Act, *in* : Jusletter 10. August 2020 ; **David ROSENTHAL/Yvonne JÖHRI (éds)**, Handkommentar zum Datenschutzgesetz, Zurich 2008 (cité : HK DSG-AUTEUR) ; **David ROSENTHAL/Samira STUDER/Alexandre LOMBARD**, La nouvelle loi sur la protection des données, *in* : Jusletter 16 novembre 2020 ; **Wolfgang**

**STRAUB**, Cloud Computing – check-list pour la rédaction de contrats, *in* : Jusletter 14 juillet 2014 ; **Jean-Philippe WALTER**, La Convention 108+, une réponse adéquate à l'ère du numérique !, 6 octobre 2020, *in* : swissprivacy.law/15.


## **B. Documents officiels**

**Conseil fédéral**, Loi fédérale sur la protection des données (LPD), FF 2020 7397 (cité : Message LPD 2020) ; **Conseil fédéral**, Loi fédérale sur la sécurité de l'information au sein de la Confédération (Loi sur la sécurité de l'information, LSI), FF 2020 9665 (cité : Message LSI 2020) ; **Conseil d'État du Canton de Vaud**, Plan directeur cantonal des systèmes d'information 2018-2023, décembre 2018 ; **Conseil d'État du Canton de Vaud**, Stratégie numérique, novembre 2018 ; **Cour des comptes du Canton de Vaud**, Rapport N° 67 : Gouvernance des projets de systèmes d'information métier de l'État de Vaud (cité : Rapport Cdc N° 67) ; **Cour des comptes du Canton de Vaud**, Rapport N° 74 : La protection des données personnelles dans l'Administration cantonale vaudoise (cité : Rapport Cdc N° 74).



## VIII. Annexes

### A. Politique d'utilisation de solution informatique externalisée de la Direction générale du numérique et des systèmes d'information de l'État de Vaud



Direction générale du numérique et des systèmes d'information  
Avenue de Longemalle 1, CH-1020 Renens  
www.vd.ch - T +41 21 316 26 00

POLITIQUE

## POLITIQUE D'UTILISATION DE SOLUTION INFORMATIQUE EXTERNALISÉE

Classification : Public  
Public cible : Services de l'ACV  
Propriétaire : Responsable du macro-processus Piloter et Rationaliser le SI Cantonal  
Identifiant : DSI-02.1-2063  
Statut : Validé  
Version & Date : 1.1 du 10.03.2021  
Révision : Annuelle  
Emplacement : Référentiel documentaire DGNSI  
Fichier : 02.1 politique d'utilisation de solution informatique externalisée.doc



## TABLE DES MATIÈRES

<b>1</b>	<b>INTRODUCTION</b>	<b>3</b>
<b>2</b>	<b>RESPONSABILITÉS</b>	<b>5</b>
2.1	Rappels sur les Responsabilités	5
2.2	Rappels de la Stratégie numérique	6
2.3	Rappels sur les Procédures de marchés public	7
2.4	Processus décisionnel	8
<b>3</b>	<b>PRINCIPES</b>	<b>9</b>
3.1	Vue d'ensemble	9
3.2	P1 : Opportunité de faire appel à un tiers prestataire	10
3.3	P2 : Rationalisation et intégration du SI	11
3.4	P3 : Économique	12
3.5	P4 : Protection des données	13
3.6	P5 : Disponibilité de la solution informatique externalisée	14
3.7	P6 : Contractualisation	15
3.8	P7 : Dispositions sectorielles	16
<b>4</b>	<b>ANNEXES</b>	<b>17</b>
4.1	Définitions	17
4.2	Sources documentaires	20
4.3	Cas d'application du RGPD	20
4.4	Modèle de coût d'évaluation	25
4.5	Questions souvent posées (FAQ)	26





# 1 INTRODUCTION

## OBJECTIFS

La présente politique fixe les principes d'utilisation d'une solution informatique externalisée.

## DOMAINE D'APPLICATION

Tous types de solutions informatiques externalisées utilisées par les services métier de l'ACV (hors UNIL et à venir le CHUV) et par convention, les services de l'ordre judiciaire.

Par solutions informatiques externalisées, on entend :

- Les services du Cloud (IaaS, PaaS, SaaS)
- Les services et solutions hors d'un data centre sous maîtrise de l'Administration Cantonale Vaudoise (ex : hébergement de solution, prestation externalisée, ...).

## PUBLIC CIBLE

Chef de services,  
Membre du CEDN,  
Responsable d'étude ou de projet d'une solution informatique externalisée,  
Architecte d'entreprise, Architecte de sécurité.

## VALIDITE

Dès adoption

## RÉFÉRENCÉS

RIC	<a href="#">Règlement relatif à l'informatique cantonale</a>
LPrD	<a href="#">Loi sur la protection des données personnelles</a>
LInfo	<a href="#">Loi sur l'information</a>
CP	<a href="#">Code pénal suisse</a>
SN	<a href="#">Stratégie Numérique</a>
DSI-02.4-2064	<a href="#">Check-list pour un contrat de sous-traitance de solution informatique externalisée</a>
DSI-02.4-2065	<a href="#">Grille d'analyse de la Politique d'utilisation de solution informatique externalisée</a>
Druide 1.2.3	<a href="#">Procédure et décisions d'adjudication des marchés publics de l'Etat de Vaud</a>
LMP-VD	<a href="#">Loi sur les marchés publics</a>
RLMP-VD	<a href="#">Règlement d'application de la loi du 24 juin 1996 sur les marchés publics</a>

## DÉFINITIONS



Politique / Interne ACV / Validé / N° DSI-02.1-2063 / Version 1.1 du 10.03.2021

**POLITIQUE D'UTILISATION DE SOLUTION INFORMATIQUE EXTERNALISÉE**

<i>CEDN</i>	Comité d'Experts Délégués au Numérique
<i>PCE</i>	Proposition au Conseil d'État
<i>PPD</i>	<u>Préposé à la Protection des Données</u>
<i>On premise</i>	En français « Sur site ». Solution informatique installée sur les serveurs du data centre de la DGNSI

Direction générale du numérique et des systèmes d'information - DGNSI  
Avenue de Longemalle 1, CH-1020 Renens  
www.vd.ch - T +41 21 316 26 00

Page 4/28



## 2 RESPONSABILITÉS

### 2.1 Rappels sur les Responsabilités

Le Règlement de l'Informatique Cantonal (RIC) précise les partages de responsabilités sur les missions et sur les acquisitions de biens et services informatiques.

#### 2.1.1 Missions

Service métier	Direction Générale du Numérique et des Systèmes d'Information
<p>Le service métier est le <b>responsable de traitement</b> des données qu'il gère au sens de la LPrD.</p> <p>Il est dès lors, de la <b>responsabilité</b> du service métier de s'assurer que les <b>traitements de données</b> (collecte, conservation, communication, etc.) auxquels il procède, respectent la LPrD, notamment des principes de la <b>légalité</b>, de la <b>proportionnalité</b> et de la <b>finalité</b><sup>1</sup>.</p> <p>Il lui appartient également de définir ses besoins <b>spécifiques</b> en matière de <b>sécurité des données</b> (disponibilité, intégrité et confidentialité)<sup>2</sup>.</p> <p>La DGNSI peut accompagner le service dans ces activités.</p>	<p>La DGNSI n'est pas le <b>responsable de traitement</b> des données traitées par les services métiers.</p> <p>De manière générale, le rôle de la DGNSI est notamment<sup>3</sup> :</p> <ol style="list-style-type: none"> <li><b>D'élaborer des solutions propres à chaque service</b> en recherchant systématiquement la rationalisation et la mutualisation à l'intérieur comme à l'extérieur de l'Administration cantonale vaudoise (ACV) ; et</li> <li><b>De gérer les relations avec les fournisseurs de biens et de services</b> (sous-traitance) en matière de technologies de l'information et de la communication.</li> </ol> <p>Il est dès lors, de la responsabilité de la DGNSI de proposer des <b>solutions techniques</b> permettant aux services métier de répondre aux obligations découlant du droit de la protection des données et de s'assurer que l'éventuelle <b>sous-traitance</b> réalisée par la DGNSI auprès de tiers pour le <b>compte des services métiers</b> répond aux conditions en matière de protection des données.</p>

<sup>1</sup> Selon articles 5, 6 et 7 LPrD

<sup>2</sup> Selon article 10 LPrD

<sup>3</sup> Selon article 7 RIC



### 2.1.2 Acquisition de biens et services informatiques

Service métier	Direction Générale du Numérique et des Systèmes d'Information
<p>En tant que responsable de traitement, le service métier, même si il ne signe pas le contrat, <b>engage sa responsabilité sur les aspects liés à la sous-traitance</b> (un usager pourrait contester la licéité de la sous-traitance auprès du service métier).</p> <p>A ce titre, le service métier doit donner son accord express à la DGNSI pour sous-traiter les traitements relatifs aux données personnels et son acceptation quant aux engagements pris contractuellement pour les respecter.</p>	<p>La DGNSI<sup>4</sup> <b>assure l'ensemble des relations avec les fournisseurs et gère l'ensemble des contrats</b> correspondants.</p> <p>En tant que signataire du contrat, la DGNSI est co-responsable (avec le service métier) sur les aspects liés à la sous-traitance.</p>

## 2.2 Rappels de la Stratégie numérique

La stratégie numérique vise à identifier en continu les impacts de la transition numérique par une analyse des forces centrifuges et centripètes qui s'exercent sur la société, et, si nécessaire, à compléter ou réorienter les politiques publiques qu'il porte et l'ordre normatif, par des actions ancrées autour de cinq thématiques transversales et interdépendantes :

- Les Données
- Les Infrastructures et la sécurité
- L'Accompagnement des personnes
- L'Accompagnement des entreprises
- La Gouvernance

Notamment, sur cette première ancre (les données), le Conseil d'État, en coordination avec les mesures déployées au niveau fédéral et par les autres cantons, entend doter le canton de Vaud d'une politique publique de la donnée, **fondée notamment sur les principes de souveraineté et de sécurité.**

<sup>4</sup> Selon article 21 RIC



## 2.3 Rappels sur les Procédures de marchés public

Les services de l'État sont soumis à la législation sur les marchés publics, notamment l'accord international sur les marchés publics (AMP), l'accord inter cantonal sur les marchés publics (AIMP), la loi vaudoise sur les marchés publics (LMP-VD) et son règlement d'application (RLMP\_VD). Les services de l'administration sont au surplus tenus d'appliquer la directive DRUIDE 1.2.3 « Procédure et décisions d'adjudication des marchés publics de l'État de Vaud » pour tous leurs marchés. Il est ainsi vivement recommandé de prendre connaissance de cette dernière avant le début du lancement de la procédure marché public.

### 2.3.1 Configuration du marché

Le pouvoir adjudicateur (le service métier) dispose d'une grande liberté dans la définition de ses besoins et dans la configuration du marché à mettre en soumission. Les pouvoirs adjudicateurs sont en principe libres de décider de ce qui doit être réalisé et obtenu ; il leur appartient toutefois de définir leurs besoins et les spécifications techniques permettant de les réaliser. Le pouvoir adjudicateur précise les spécifications techniques exigées dans les documents d'appel d'offres (art. 16 al. 1 RLMP-VD). Il faut comprendre, sous cette notion, les exigences techniques avec l'aide desquelles l'objet du marché (le matériel, le produit ou une livraison) peut être désigné de telle sorte qu'il remplisse pour le donneur d'ordre son utilisation spécifique ; en font partie les garanties de qualité, l'utilisation, l'efficacité, la sécurité, etc. Le recours à des spécifications techniques discriminatoires est cependant prohibé. Il est ainsi interdit de tailler le marché sur mesure pour un soumissionnaire déterminé ; le marché peut être réalisé de diverses manières et chaque soumissionnaire doit pouvoir concourir avec ses qualités propres. Ainsi, le pouvoir adjudicateur (le service métier) ne doit pas définir dans son cahier des charges des spécifications techniques à caractère discriminatoire qui ont pour effet reconnaissable de pénaliser, respectivement d'avantager certains soumissionnaires par rapport à d'autres sans justification. Dans son cahier des charges, le pouvoir adjudicateur doit définir ses besoins, notamment tels qu'il a pu les préciser à l'aide des 7 principes de la présente politique.

Dans le cadre de la configuration d'un marché à mettre en concurrence, des contacts préalables entre le pouvoir adjudicateur et un ou plusieurs fournisseurs sont non seulement de nature à créer des suspicions de partialité de l'adjudicateur mais également à influencer la rédaction du cahier des charges en faveur d'un acteur du marché. Pour cette simple raison, le fait, pour un service adjudicateur de l'État, de commencer à évaluer avec un fournisseur une solution informatique externalisée à travers la « Grille d'analyse de la Politique d'utilisation de solution informatique externalisée » avant de lancer un marché devrait être évité. Tout contact du pouvoir adjudicateur avec des futurs soumissionnaires avant une procédure marché public est en effet de nature à porter atteinte au principe fondamental d'égalité de traitement entre les soumissionnaires (art. 6, al. 1, let. a LMP-VD) et pourrait par la suite être reproché à l'adjudicateur.

#### Choix entre une solution informatique externalisée et une solution informatique « classique »

Pour une même expression de besoins fonctionnels, l'économie/les sociétés d'informatique peu.t.vent proposer des solutions informatiques « classiques » (« *on premise* ») ou des solutions informatiques externalisées.

Quand bien même une solution informatique externalisée répond aux principes de sécurité et de protection des données, il se peut qu'une pesée des intérêts en présence démontre qu'il n'est pas opportun d'externaliser cette tâche de l'État, à faire appel à un tiers prestataire (voir principe P1). Dans ce cas, le cahier des charges devra mentionner que la solution doit être installée dans le *data center* de la DGNSI (solution « *on premise* ») et annoncer les motifs qui justifient ce choix (renonciation à une solution informatique externalisée).



### 2.3.2 Proposition d'une solution informatique externalisée par un service métier à la DGNSI

Il est rappelé que le service métier exprime des exigences fonctionnelles et que la DGNSI recherche et propose les solutions techniques en adéquation avec lesdites exigences (cf. § 2.1 « Rappel issu du RIC »). Il revient au pouvoir adjudicateur de définir le type de marché ainsi que sa valeur (HT) afin de déterminer la procédure applicable (procédure de gré à gré, sur invitation, ouverte ou sélective) à son marché, conformément aux indications contenues dans la Druide 1.2.3. À noter qu'en matière informatique, seuls les marchés de services et de fournitures trouveront à s'appliquer.

### 2.3.3 Cas exceptionnel d'une solution informatique externalisée choisie directement par le service métier

Une adjudication de gré à gré exceptionnel en faveur d'une solution informatique spécifique et choisie directement par le service métier peut intervenir si elle respecte les conditions de l'art. 8 RLMP-VD. Dans cette hypothèse, la grille d'analyse de la Politique d'utilisation de solution informatique externalisée peut être utilisée et des contacts (négociations) peuvent avoir lieu avec le fournisseur. Les principes énoncés dans la présente politique devront également être respectés.

## 2.4 Processus décisionnel

Le processus décisionnel lié à l'analyse de l'utilisation d'une solution informatique externalisée suit 3 étapes :

- Étape 1 : Analyse de la solution par les parties prenantes
  - Évaluer le respect des principes de la politique (à travers la Grille d'analyse de la Politique d'utilisation de solution informatique externalisée)
- Étape 2 : Évaluation et préavis du comité d'experts délégués au numérique (CEDN)
  - Apprécier les risques, sous l'angle politique/métier
  - En réunion ou par voie de circulation selon la criticité
- Étape 3 : Arbitrage par le CE pour les cas sensibles
  - Le cas échéant, PCE portée par le service avec préavis de la commission d'experts (CEDN)

**Remarque importante :** Un préavis positif du CEDN pour la solution informatique externalisée ne présume pas de sa mise en service.

Par exemple, lors de l'étape d'initialisation du projet, du processus d'élaboration de la solution (EMS), une analyse de risques sécurité est menée et peut « disqualifier » la solution informatique externalisée.



## 3 PRINCIPES

### 3.1 Vue d'ensemble

L'utilisation d'une solution informatique externalisée doit respecter 7 principes clés :

- P1 : Opportunité de faire appel à un tiers prestataire
  - Ce principe est instruit par le service métier
- P2 : Rationalisation et intégration du SI
  - Ce principe est instruit pour partie par le service métier et par la DGNSI
- P3 : Économique
  - Ce principe est instruit pour partie par la DGNSI (P3.1) et par le service métier (P3.2)
- P4 : Protection des données
  - Ce principe est instruit pour partie par le service métier (P4.1) et par la DGNSI (P4.2)
- P5 : Disponibilité de la solution informatique externalisée
  - Ce principe est instruit pour partie par la DGNSI et par le service métier
- P6 : Contractualisation
  - Ce principe est instruit par la DGNSI et validé par le service métier
- P7 : Dispositions sectorielles
  - Ce principe est instruit par le service métier



## 3.2 P1 : Opportunité de faire appel à un tiers prestataire

### 3.2.1 P1.1 : Le service métier doit être en mesure de traiter les éventuels impacts et assumer les possibles conséquences « politique » de l'utilisation d'une solution informatique externalisée (par exemple en cas d'événement<sup>5</sup>).

- Il est rappelé que même si une solution informatique externalisée répond aux principes de protection des données (P4) et de sécurité (P1.2, P2, P5), il se peut qu'une pesée des intérêts démontre qu'il n'est pas opportun d'externaliser certaines tâches de l'état et de faire appel à un tiers prestataire (voir § 2.3.1 « Configuration du marché »).
- En cas d'incertitude, le service métier peut demander l'avis du CEDN.

### 3.2.2 P1.2 : Les documents secrets<sup>6</sup> ne doivent pas être véhiculés<sup>7</sup> dans une solution informatique externalisée.

- Toutes exceptions à ce principe doivent faire l'objet d'un accord clairement formalisé entre le service métier et le CEDN.

<sup>5</sup> Fuite d'information, indisponibilité prolongée de la prestation, ...

<sup>6</sup> Les documents secrets sont classifiés comme tels par le service métier selon le tableau de classification établi par la DGNSI.

<sup>7</sup> Par «véhiculé» on entend tout transit, stockage, modification ou archivage de documents.





### 3.3 P2 : Rationalisation et intégration du SI

**La solution informatique externalisée doit s'intégrer au SI existant et contribuer à sa rationalisation.**

- La solution informatique externalisée doit être alignée avec la stratégie du SI et à la stratégie du service métier.
- La solution informatique externalisée ne doit pas faire redondance avec une solution standard existante.
- La solution informatique externalisée doit être, au moins, compatible avec la gestion des accès et des identités de l'ACV (IAM).
- La solution informatique externalisée doit être, au moins, compatible avec le système de supervision de l'ACV.



### 3.4 P3 : Économique

#### 3.4.1 P3.1 : Les solutions informatiques externalisées suisses doivent être favorisées dans le respect de la loi sur les marchés publics.

- Voir les « Rappels sur les Procédures de marchés public » (§2.3)
- Pour un même périmètre fonctionnel, rechercher une équivalence suisse de la solution informatique externalisée.
- Solliciter les acteurs locaux ou créer les conditions cadre pour mettre en œuvre la solution informatique externalisée en Suisse.

#### 3.4.2 P3.2 : La solution informatique externalisée doit démontrer sa valeur ajoutée.

- Une analyse VAP<sup>8</sup> de la solution informatique externalisée doit être réalisée.

---

<sup>8</sup> VAP : Valeur Ajoutée du Projet



### 3.5 P4 : Protection des données

#### 3.5.1 P4.1 : Une solution informatique externalisée véhiculant des données personnelles doit répondre aux exigences soumises à la LPrD et/ou soumises au secret<sup>9</sup>

- Les questions préalables listées dans la check-list pour un contrat de sous-traitance de solution informatique externalisée doivent être validées.
- Toutes exceptions à ce principe doivent faire l'objet, au cas par cas, d'une appréciation et d'un accord clairement formalisé entre le CEDN et le service métier.

#### 3.5.2 P4.2 : Un ISE<sup>10</sup> doit être utilisé comme identifiant à travers une solution informatique externalisée.

- L'ISE peut se traduire par un hexagramme généré aléatoirement. Chaque utilisateur de solutions informatiques externalisées possède un hexagramme dédié, pérenne et unique parmi tous les utilisateurs.
- L'ISE peut se traduire par l'adresse email de l'utilisateur.
- L'IUP<sup>11</sup> ne doit pas être utilisé comme identifiant à travers une solution informatique externalisée.

<sup>9</sup> Secret de fonction (selon articles 18 LInfo et 320 Code Pénal) et/ou Secret professionnel (selon article 321 Code Pénal).

<sup>10</sup> Identifiant de Solution Externalisée

<sup>11</sup> Identifiant Unique et Pérenne.



### 3.6 P5 : Disponibilité de la solution informatique externalisée

#### La délivrance des prestations de l'État ne doit pas être lourdement impactée en cas d'indisponibilité de la solution informatique externalisée.

- Un plan (ou une esquisse de PSI<sup>12</sup>) doit être défini et acceptable par le service métier en cas d'arrêt de la solution informatique externalisée ou d'une rupture du contrat. Ce plan doit être fourni par le prestataire en amont de la contractualisation.
- En corolaire du plan fourni par le prestataire de solution informatique externalisée, le service métier doit instruire, avant la contractualisation, un plan de continuité des activités (PCA) en cas d'indisponibilité de la solution.
- La réversibilité de la solution doit être prévue dès le début du projet.
- Pour une solution informatique externalisée considérée comme critique par le métier, la pérennité du prestataire de cette solution doit être établie<sup>13</sup>. Dans les autres cas, il peut être envisagé de collaborer avec un prestataire de solution informatique externalisée de type «start-up» s'il offre un service différenciateur ou apporte une réelle valeur ajoutée.
- La qualité de service<sup>14</sup> doit être clairement définie et acceptée par le service métier.

<sup>12</sup> PSI : Plan de Secours Informatique (ou DRP en anglais pour Disaster Recovery Plan).

<sup>13</sup> La pérennité se base sur des éléments comme l'évolution du chiffre d'affaire, la rentabilité, le nombre de collaborateurs l'ancienneté de la société, le nombre de clients, ....

<sup>14</sup> La qualité de service se base sur les accords de niveau de services (SLA en anglais) et/ou les objectifs de niveau de services (ou SLO en anglais) de la solution informatique externalisée.



### 3.7 P6 : Contractualisation

**La contractualisation d'une solution informatique externalisée est assurée par la DGNSI et doit prévoir des garanties suffisantes.**

- Voir les « Rappels sur les Procédures de marchés public » (§2.3)
- Le contrat doit intégrer les exigences minimales en matière de sécurité et de protection des données selon la check-list pour un contrat de sous-traitance de solution informatique externalisée fourni par la PPD<sup>15</sup>. Si le prestataire ne propose pas de contrat, le modèle de contrat de délégation de traitement fournis dans la check-list pour un contrat de sous-traitance de solution informatique externalisée peut être utilisé.
- Le contrat doit prévoir le droit suisse comme applicable et le for juridique en Suisse<sup>16</sup>. En cas de négociations infructueuses sur un ou plusieurs point-s, une dérogation est possible avec une analyse préalable du SJL, du CEDN et l'accord clairement formalisé par le chef du service métier.

<sup>15</sup> Notamment les données personnelles et en particulier si les données ne sont pas chiffrées.

<sup>16</sup> De préférence en Suisse Romande.



### 3.8 P7 : Dispositions sectorielles

**La solution informatique externalisée doit répondre aux dispositions sectorielles.**

- Dans le cas où des lois ou des directives spécifiques à un service métier<sup>17</sup> peuvent avoir des conséquences sur les modalités d'utilisation et/ou de contractualisation avec la solution informatique externalisée, celles-ci doivent être examinées et traitées par le service métier.

<sup>17</sup> Il est rappelé qu'une directive sectorielle n'a pas force de loi.



## 4 ANNEXES

### 4.1 Définitions

Les définitions suivantes sont celles communément admises et partagées par la DGNSI. Elles sont inspirées des définitions du document de la confédération sur la Stratégie d'informatique en nuage des autorités suisses 2012-2020 et du NIST.

#### 4.1.1 Cloud computing

Le Cloud Computing, ou l'informatique en nuage, est un terme général employé pour désigner la livraison de ressources et de services à la demande.

L'OFIT précise : « Le Cloud-Computing décrit l'approche de mettre à disposition des infrastructures abstraites ou non-abstraites (par exemple capacités de calcul, de stockage, de réseau ou même des logiciels) à travers le réseau et qui peuvent suivre de manière dynamique la demande. Du point de vue de l'utilisateur l'infrastructure mise à disposition semble distante et opaque, comme « voilé d'un nuage ». L'offre et l'utilisation de ces services se fait uniquement à travers d'interfaces et de protocoles définies de manière technique. La gamme des services offerts dans le cadre des prestations Cloud contient l'entiereté de la technologie informatique et contient entre autres l'infrastructure, les plateformes et les logiciels.

Une infrastructure Cloud est une collection de composantes de matériel et de logiciels qui coopèrent dans le Cloud de manière efficace. Les conditions suivantes sont essentielles et indispensables : des composantes et processus hautement automatisés et standardisés ainsi qu'un haut degré de virtualisation.

#### 4.1.2 Classes de produit (IaaS/PaaS/SaaS)

Les différentes définitions des classes de produit sont présentées ci-après :

Acronymes	Classes de produit	Description
IaaS	Infrastructure as a Service	Mise à disposition d'une infrastructure informatique, telle que le réseau (gestion des flux, ...), serveur (puissance de calcul, mémoire, ...) routeur, firewall, stockage et backup typiquement sous forme de virtualisation.
PaaS	Platform as a Service	Mise à disposition de plateformes et de services qui sont utilisés pour le développement, l'intégration et l'exploitation de composants d'application.
SaaS	Software as a Service	Mise à disposition d'applications (commerciales, de collaboration, de communication ...) en tant que services. Ces derniers sont destinés à des utilisateurs finaux.

Remarque :

- Le document de stratégie d'informatique en nuage (cité plus haut) introduit le terme de BPaaS. Ce terme n'est pas retenu à la DGNSI car, selon la déclinaison d'un BPaaS, elle peut se traduire par les 3 autres classes de produit (IaaS, PaaS, SaaS).



- Selon les vellétés du « marketing » de nouveaux acronymes apparaissent comme IAMaaS (gestion des identités et des accès sous forme de service), SMaaS (Security Management as a Service), DaaS (Desktop as a service), DaaS (Datacenter as a service). Ce type d'acronyme est à rapprocher du IaaS, PaaS ou SaaS selon le contenu de l'offre.

Afin d'avoir une compréhension plus aisée des classes de produit, des exemples sont fournis ci-dessous :

Acronymes	Type de service	Exemples	
IaaS	Infrastructure (Hébergement)	<ul style="list-style-type: none"> <li>• Data center</li> <li>• Serveurs / Machines virtuelles</li> <li>• Réseau</li> </ul>	<ul style="list-style-type: none"> <li>• Service de stockage</li> <li>• Service de pare-feu réseau</li> <li>• Service de répartition de charge</li> </ul>
PaaS	Composant applicatif / Plateforme (Construction)	<ul style="list-style-type: none"> <li>• Système d'exploitation</li> <li>• Serveur d'application</li> <li>• Base de données</li> <li>• Bus de services</li> </ul>	<ul style="list-style-type: none"> <li>• Environnement de développement</li> <li>• Service de monitoring</li> <li>• Service de caching</li> </ul>
SaaS	Application / Logiciel (Utilisation)	<ul style="list-style-type: none"> <li>• Applications de gestion (CRM, Comptabilité, RH, ...)</li> <li>• Solution technologique (GED, MDM, système de recherche, système de paiement, ...)</li> </ul>	<ul style="list-style-type: none"> <li>• Gestion des identités et des accès</li> <li>• Logiciels de messagerie, de collaboration</li> </ul>

### 4.1.3 Formes d'organisation (Cloud Public/Privé/...)

Selon l'organisation de leur exploitation et de leur utilisation les classes de produit peuvent prendre différentes formes.

Formes d'organisation	Description
Cloud Public	La solution en nuage est accessible pour le public ou un grand domaine industriel et appartient à une organisation de service en nuage.
Cloud Privé	La solution en nuage est mise en place pour un usage exclusif à une organisation. Elle est hébergée au sein de l'organisation. L'externalisation et/ou l'exploitation du cloud privé (VPC, ...) est considérée comme un Cloud Hybride.
Cloud Communautaire	La solution en nuage est partagée par plusieurs organisations et sert/soutient une communauté d'utilisateurs spécifique ayant des intérêts communs.
Cloud Hybride	La solution en nuage se compose d'un arrangement de deux ou plusieurs nuages (Privé, Public, Communautaire) reliés entre eux par des technologies normalisées ou propriétaires afin de permettre la portabilité des données et des applications.





Appliqué à l'ACV les responsabilités et les activités sont les suivantes :

Formes d'organisation	Propriété de l'infrastructure cloud	Localisation de l'infrastructure cloud	Population pouvant accéder à la solution cloud	Population paramétrant le contenu de la solution	Population gérant l'infrastructure cloud
Cloud Public	Prestataire cloud	Data center du prestataire cloud	Tous	DGNSI (ou utilisateur clé d'un service métier)	Prestataire cloud
Cloud Privé	ACV	Data center de la DSI	ACV	DGNSI (ou utilisateur clé d'un service métier)	DGNSI
Cloud Communautaire	ACV + partenaires (ex : autre canton, parapublic, ...)	Répartie entre les sites de l'ACV et ceux des partenaires	ACV + partenaires	Les « DSI » de l'ACV et des partenaires (ou utilisateurs clés)	Chaque « DSI » gère ses prestations
Cloud Hybride	Prestataire cloud pour la partie cloud public ou VPC ACV pour la partie cloud privé	Data center du prestataire cloud pour le cloud public ou VPC Data center de la DGNSI pour le cloud privé	ACV	DGNSI (ou utilisateur clé d'un service métier)	Prestataire cloud pour la partie cloud public DGNSI pour la partie cloud privé



## 4.2 Sources documentaires

La prise en compte des documents suivants peut s'avérer utile.

Intitulé	Justification	Acronyme
Règlement (UE) 2016/679 du Parlement Européen et du Conseil de l'Union Européenne du 27 avril 2016 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, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données; RGPD)	Attention, il appartient aux services métiers concernés d'effectuer une analyse sur l'éventuelle applicabilité directe du RGPD (voir § 4.3 « Cas d'application du RGPD »)	<u>RGPD</u>
Guide relatif aux mesures techniques et organisationnelles de la protection des données	Guide pour le traitement des données personnelles. Il est à destination de l'administration fédérale mais est une source enrichissante	<u>GPDT-MTO</u>

## 4.3 Cas d'application du RGPD

Les cas métier suivants permettent d'avoir une lecture synthétique des cas d'application du RGPD.

Direction générale du numérique et des systèmes d'information  
 Avenue de Longemalle 1, CH-1020 Renens  
 www.vd.ch - T +41 21 316 26 00



Cas 1	Activité	Le RGPD	Exemple ou Remarque
Un responsable de traitement d'une entité suisse, en Suisse	offre des biens ou des services à des personnes se trouvant sur le territoire de l'UE et ce quel que soit leur nationalité et leur lieu de résidence	S'applique (application de la clause d'extraterritorialité)	Entités proposant des services visant : <ul style="list-style-type: none"> <li>à faciliter l'implantation d'entreprises européennes dans le canton de Vaud</li> <li>la réservation d'offres touristiques</li> </ul>
	suit en ligne le comportement de personnes sur le territoire de l'UE et ce quel que soit leur nationalité et leur lieu de résidence (notion de profilage)	S'applique (application de la clause d'extraterritorialité)	Peu probable dans le cadre de l'activité classique des entités soumises à la LPD Le site vd.ch et le portail de cyberadministration n'ont pas retenu et mis en œuvre le profilage
	Dans les autres cas	Ne s'applique pas	

Cas 2	Activité	Le RGPD	Exemple ou Remarque
Un responsable de traitement d'une entité suisse, en Suisse, qui traite des données personnelles relatives à des personnes se trouvant sur le territoire de l'UE et ce quel que soit leur nationalité	offre des biens ou des services à des personnes se trouvant sur le territoire de l'UE et ce quel que soit leur nationalité et leur lieu de résidence	S'applique (application de la clause d'extraterritorialité)	
	suit en ligne le comportement de personnes sur le territoire de l'UE et ce quel que soit leur nationalité et leur lieu de résidence (notion de profilage)	S'applique (application de la clause d'extraterritorialité)	
	Dans les autres cas	Ne s'applique pas	

Direction générale du numérique et des systèmes d'information - DGNIS  
 Avenue de Longemalle 1, CH-1020 Renens  
 www.vd.ch - T +41 21 316 26 00



Cas 3	Activité	Le RGPD	Exemple ou Remarque
Un responsable de traitement d'une entité suisse, en Suisse, faisant appel à un sous-traitant situé dans l'UE.	Ce responsable de traitement à l'intention d'offrir des biens ou des services à des personnes se trouvant sur le territoire de l'UE et ce quel que soit leur nationalité et leur lieu de résidence par l'intermédiaire de ce sous-traitant	S'applique au responsable de traitement (application de la clause d'extraterritorialité) S'applique au sous-traitant (application de par sa localisation en UE)	
	Ce responsable de traitement à l'intention de suivre en ligne le comportement de personnes sur le territoire de l'UE et ce quel que soit leur nationalité et leur lieu de résidence (notion de profilage) par l'intermédiaire de ce sous-traitant	S'applique au responsable de traitement (application de la clause d'extraterritorialité) S'applique au sous-traitant (application de par sa localisation en UE)	
Dans les autres cas			Ne s'applique pas MAIS prévoit un contrat mentionnant le droit suisse comme applicable et le for juridique en Romandie (voir § 3.7 - P6 : Contractualisation →)



Cas 4	Activité	Le RGPD	Exemple ou Remarque
<p>Un sous-traitant situé dans l'UE</p>		<p>S'applique au sous-traitant uniquement (sauf cas 3)                      (application de par sa localisation en UE)                      Ne s'applique pas au responsable de traitement MAIS prévoir un contrat mentionnant le droit suisse comme applicable et le for juridique en en Romandie (voir § 3.7 « P6 : Contractualisation »)                      (Le RGPD ne « remonte pas » vers le responsable de traitement)</p>	



Cas 5	Activité	Le RGPD	Exemple ou Remarque
Un sous-traitant suisse, en Suisse, agissant pour le compte d'un responsable de traitement établi dans l'UE	offre des biens ou des services à des personnes se trouvant sur le territoire de l'UE et ce quel que soit leur nationalité et leur lieu de résidence	S'applique (application de la clause d'extraterritorialité)	Peu probable dans le cadre de l'activité classique des entités soumises à la LPD
	suit en ligne le comportement de personnes sur le territoire de l'UE et ce quel que soit leur nationalité et leur lieu de résidence (notion de profilage)	S'applique (application de la clause d'extraterritorialité)	
	Dans les autres cas	Ne s'applique pas sauf si un contrat prévoit l'application du RGPD (ce qui est généralement le cas)	

Cas 6	Activité	Le RGPD	Exemple ou Remarque
Une entité suisse, en Suisse	emploie des personnes se trouvant sur le territoire de l'UE et ce quel que soit leur nationalité	Ne s'applique pas	Cela comprend les frontaliers



Direction générale du numérique et des systèmes d'information  
Avenue de Longemalle 1, CH-1020 Renens  
www.vd.ch - T +41 21 316 26 00

#### 4.4 Modèle de coût d'évaluation

Les types de coûts suivants peuvent être pris en compte pour estimer le modèle de coût d'utilisation d'une prestation qu'elle soit « on premise », ad'hoc ou cloud.

Les types de coûts se répartissent comme suit.

- Coûts d'investissement
  - Matériel (clients, réseau, serveur, stockage, stockage d'archives, sauvegarde)
  - Licences de logiciel (y compris les systèmes d'exploitation et middleware)
- Coûts du projet
  - Coûts du personnel externe pour la montée en cadence<sup>1</sup>
  - Frais de personnel interne pour la montée en cadence<sup>1</sup>
  - Coûts de formation
- Coûts d'exploitation
  - Matériel
    - Maintenance
    - Consommation d'électricité
    - Refroidissement
    - Coûts d'utilisation RZ (pro rata)
  - Logiciels
    - Maintenance
- Coûts de personnel
  - Infrastructure
  - Gestion des services de personnel
  - Maintenance des solutions de coûts du personnel (hors maintenance logicielle)
- Types de coûts spéciaux
  - Coûts d'audit (protection des données, conformité)
  - Coûts d'assurance et provisions (en cas d'insolvabilité d'un sourcing externe ou fournisseur de cloud)

Direction générale du numérique et des systèmes d'information - DGNSI  
Avenue de Longemalle 1, CH-1020 Renens  
www.vd.ch - T +41 21 316 26 00

Page 25/28



## 4.5 Questions souvent posées (FAQ)

### 4.5.1 Déploiement d'une solution informatique externalisée

Une fois les principes de la politique respectés et un préavis positif sans restriction du CEDN, puis-je déployer la solution ?

Non. La grille d'analyse permet de faire un état des lieux objectif sur la conformité légale, sécuritaire et organisationnelle (de premier niveau) pour la délégation de solutions informatiques externalisées. Elle ne fait en aucun cas, validation du choix d'une solution. Elle est une partie constitutive de l'aide au choix de la solution.

Au préalable du déploiement, le processus de la DSI sur l'élaboration d'une solution doit être respecté. Notamment, le projet d'étude doit clairement indiquer que la solution informatique externalisée est la solution qui répond la mieux aux enjeux politiques, légaux, métiers, sécuritaires, de coûts et de respect des principes d'architectures.

### 4.5.2 Prestataire de la solution informatique externalisée

Y a-t-il des législations différentes entre l'utilisation d'une solution informatique externalisée dans le canton de Vaud et une solution informatique externalisée dans un autre canton suisse ?

Pour les entreprises privées offrant une solution informatique externalisée en Suisse, la LPD s'applique quel que soit le canton où est externalisée la solution.

Pour les entités de droit public qui utilisent des solutions informatiques externalisées, c'est la loi cantonale qui s'applique : LPrD pour Vaud, LIPAD pour Genève, ...

Par exemple, l'entité de droit public du canton de Vaud (au sens de l'article 3 LPrD) qui utilise solution informatique externalisée en Suisse (et ce quel que soit le canton où est externalisée la solution) délègue une partie de ses traitements des données à un tiers (le prestataire de la solution informatique externalisée) donc est soumise à l'article 18 LPrD.

Dans cette optique, l'entité de droit public du canton de Vaud doit faire respecter, au prestataire de la solution informatique externalisée, l'article 18 LPrD avec un contrat possédant des garanties suffisantes (voir § 3.7 « P6 : Contractualisation »).

Il n'y a donc pas de distinction, pour l'entité de droit public, dans l'utilisation d'une solution informatique externalisée dans son canton ou dans le reste de la Suisse.

Peut-on héberger ou utiliser d'autres services offerts par un prestataire de solution informatique externalisée avec qui l'ACV a déjà contractualisé ?

Le contrat d'une solution informatique externalisée prévoit les conditions pour l'utilisation de cette solution pour un périmètre défini au préalable. Il n'est pas autorisé d'utiliser des services complémentaires à d'autres fins.

Les fournisseurs de SaaS ne peuvent offrir un « espace » complémentaire pour mettre en service une autre solution. Si jamais, cela devenait possible, il serait interdit d'utiliser cette capacité.

Les fournisseurs de PaaS fournissent, entre autres, des capacités de stockage pouvant héberger une solution. Dans ce cas, si l'ACV souhaite utiliser ce service, un nouveau contrat ou un avenant mentionnant clairement le nouveau périmètre doit être établi.





Y a-t-il transfert de responsabilité du service métier de l'ACV au prestataire de la solution informatique externalisée ?

Non. Le service métier de l'ACV reste celui qui doit rendre compte à ses usagers (Accountable). Le prestataire de la solution informatique externalisée opère le service (Responsible). Pour illustrer, un usager ne s'adresse pas au prestataire de la solution informatique externalisée lorsqu'il y a un problème ou une question, il s'adresse toujours au service métier de l'ACV (dans ce cas, la DGNSI).

Le contrat entre le prestataire de la solution informatique externalisée et le service métier de l'ACV doit clairement exposer les conditions et les responsabilités entre chacune des parties prenante (voir § 3.7 « P6 : Contractualisation »).

#### 4.5.3 LPD et OLPD

La LPD et son ordonnance (OLPD) sont-elles applicables à l'ACV ?

Non, les champs d'application de la LPD concernent, entre autres, les personnes privées et les organes fédéraux. À ce titre, un prestataire de solution informatique externalisée en Suisse (et les services métier de la Confédération) appliquent la LPD. L'ACV, elle, applique la LPrD.

#### 4.5.4 Techniques de sécurité

Le chiffrement des données est-il un procédé permettant d'assurer que l'cn ne pourra plus retrouver ou déduire l'identification d'une personne (est-il possible de « revenir en arrière ») ?

Pour celui ou celle ne possédant pas la clef de déchiffrement, les données d'origine (en clair) restent inaccessibles. Dès qu'une clef de chiffrement est stockée chez un prestataire externe, il faut présumer qu'elle est accessible au prestataire, même s'il s'agit d'un nombre restreint d'administrateurs chez le prestataire.

Qu'elle est la différence entre chiffrement, anonymisation, pseudonymisation ?

Le **chiffrement** est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension de données impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

La sécurité d'un système de chiffrement doit reposer sur le secret de la clé de chiffrement et non sur celui de l'algorithme. Le principe de Kerckhoffs suppose en effet que l'ennemi (ou la personne qui veut déchiffrer le message codé) connaisse l'algorithme utilisé. (Source Wikipédia : <https://fr.wikipedia.org/wiki/Chiffrement>)

L'**anonymisation** de données personnelles consiste à modifier le contenu ou la structure de ces données afin de rendre très difficile ou impossible la « ré-identification » des personnes (physiques ou morales). (Source Wikipédia : <https://fr.wikipedia.org/wiki/Anonymisation>)

La **pseudonymisation** est un traitement sur des données à caractère personnel de manière à ce qu'on ne puisse pas attribuer les données à une personne (physique ou morale) sans avoir recours à des informations supplémentaires.

Le processus de pseudonymisation est moins fort que le processus d'anonymisation qui vise à empêcher totalement et de manière irréversible la possibilité d'identifier une personne. (Source Wikipédia : <https://fr.wikipedia.org/wiki/Pseudonymisation>)

Pour illustrer, la donnée en claire « Le RGPD » après un traitement de pseudonymisation (Chiffrement AES-256) devient « 45ba2fc25ec8a80bde0e14f3cda02f3a » alors qu'après un traitement d'anonymisation la donnée devient « ASASDJDFJ »

Pour conclure, les données pseudonymes permettent toujours une forme de ré-identification (même indirecte et à distance), tandis que les données anonymes ne peuvent pas être ré-identifiées.



#### 4.5.5 Formations et information

Organisation	Détail	Lien
PPDI - CEP	Formation « Loi sur la protection des données personnelles : principes et conséquences pour l'Administration cantonale vaudoise (session pilote) »	<a href="https://www.cep.vd.ch/cours/GBON-AV2GYR">https://www.cep.vd.ch/cours/GBON-AV2GYR</a>
PPDI - CEP	Formation « Transparence de l'Administration cantonale vaudoise et accès aux documents officiels »	<a href="https://www.cep.vd.ch/cours/GBON-AV2HE7">https://www.cep.vd.ch/cours/GBON-AV2HE7</a>
PPDI	Page du bureau de la Préposée à la Protection des Données et à l'Information	<a href="https://www.vd.ch/toutes-les-autorites/preposee-a-la-protection-des-donnees-et-a-l-information/">https://www.vd.ch/toutes-les-autorites/preposee-a-la-protection-des-donnees-et-a-l-information/</a>

## B. Check-list pour contrat de sous-traitance de solution informatique externalisée de l'Autorité de protection des données et de droit à l'information du Canton de Vaud



**Autorité de protection des données et de droit à l'information**

Rue Saint-Martin 6  
Case postale 5485  
1002 Lausanne

### CHECK-LIST POUR CONTRAT DE SOUS-TRAITANCE DE SOLUTION INFORMATIQUE EXTERNALISÉE

Selon l'art. 18 de la loi du 11 septembre 2007 sur la protection des données personnelles (LPrD ; BLV 172.65), pour pouvoir sous-traiter le traitement de données personnelles, il convient de disposer soit d'une base légale, soit d'un contrat. Dans la plupart des cas, aucune base légale ne prévoit la sous-traitance et la conclusion d'un contrat est dès lors nécessaire. Il est également recommandé de disposer d'un contrat même lorsque la sous-traitance est autorisée par la loi afin de s'assurer du respect des règles de protection des données par le sous-traitant, ainsi qu'en cas de communication transfrontière, garantir un niveau de protection adéquat. Le responsable du traitement (le service métier) qui sous-traite reste entièrement responsable vis-à-vis de la personne concernée du respect de la LPrD.

Le présent document<sup>1</sup> constitue uniquement une aide à la décision et permet de s'assurer que les points principaux ont été prévus dans le contrat. Il est néanmoins important de toujours prendre en compte les spécificités du cas d'espèce. Il ne saurait dès lors être exhaustif.

#### Questions préalables :

1. Des données personnelles, qu'elles soient sensibles ou non (selon la définition de l'art. 4 al. 1 let. a et b LPrD), seront-elles sous-traitées ?
  - a. Non, aucune donnée personnelle ne sera traitée. La LPrD n'est par conséquent pas applicable. Il n'y a dès lors pas besoin de disposer d'un contrat sous l'angle de la protection des données. Il convient néanmoins de disposer d'un contrat pour les autres questions juridiques.
  - b. Oui, des données personnelles seront bien sous-traitées. Il convient dès lors de passer au point 2 en lien avec le secret de fonction.
2. Des données personnelles (sensibles ou non) soumises au secret de fonction seront-elles sous-traitées ?
  - a. Non, aucune donnée soumise au secret de fonction ne sera traitée. Il n'y a alors pas d'obligation spécifique à respecter en matière de secret de fonction. Il convient néanmoins de disposer d'un contrat pour les autres questions juridiques.
  - b. Oui, des données soumises au secret de fonction seront traitées. Il convient alors de prévoir contractuellement que le sous-traitant et ses employés sont soumis au secret de fonction. Le sous-traitant devra également s'assurer du respect effectif du secret par ses employés et par ses sous-traitants en cascade.
    1. Les données soumises au secret de fonction seront-elles traitées en Suisse ?
      - a. Oui et il n'y a pas de sous-traitance en cascade à l'étranger. La sous-traitance peut être mise en place (le contrat doit

<sup>1</sup> Le présent document a été élaboré avant l'arrêt [Schrems II](#) du 16 juillet 2020 rendu par la Cour de Justice de l'Union européenne (CJUE) lequel invalide la décision d'adéquation 2016/1250 et par là même le dispositif Privacy Shield EU-US.

- inclure des règles strictes sur l'interdiction de recourir à des sous-traitants en cascade à l'étranger). Il convient dès lors de passer au point 3 en lien avec le contrat.
- b. Oui mais il y a une sous-traitance en cascade à l'étranger (par exemple, sauvegarde ou redondance des données à l'étranger). Il conviendra de chiffrer les données soumises au secret de la manière suivante :
    - i. Le chiffrement doit être réalisé en Suisse. La clé de déchiffrement doit, elle, être détenue en Suisse par l'Administration Cantonale Vaudoise (ACV), par le sous-traitant ou par un tiers. Si la clé est détenue par le sous-traitant ou par un tiers, le contrat doit inclure des règles strictes sur l'interdiction de transmettre la clé à l'étranger de manière à ce que les données ne soient déchiffrées.
    - ii. Il convient dès lors de passer au point 3 en lien avec le contrat.
  - c. Non. Il conviendra de chiffrer les données soumises au secret. Le chiffrement doit être réalisé en Suisse et la clé de déchiffrement détenue en Suisse par l'ACV ou par un tiers autre que le sous-traitant. Dans ce dernier cas, le contrat devrait à tout le moins prévoir une interdiction pour le tiers de transmettre la clé de déchiffrement au sous-traitant et une interdiction pour le sous-traitant de tenter de déchiffrer les données. Il convient dès lors de passer au point 3 en lien avec le contrat.
- Si ces conditions ne peuvent être respectées, il convient de garder à l'esprit que la transmission de données soumises au secret de fonction et non chiffrées à un tiers prestataire hors de Suisse est susceptible de constituer une violation du secret de fonction (les peines maximales sont la privation de liberté de trois ans au plus ou une peine pécuniaire ; article 320 du code pénal (CP ; RS 311.0).

3. Existe-il un contrat avec le partenaire contractuel ? Dans la majorité des cas, lorsque l'on contracte avec un sous-traitant (notamment dans le cas de fourniture de biens ou de services) un contrat écrit va être établi. Il peut souvent s'agir de conditions générales ou de simples bons de commande.
- a. Oui, un contrat existe. Dans les contrats avec de grandes sociétés, principalement de services informatiques, des clauses de protection des données sont généralement intégrées à leurs conditions générales. Le contrat contient-il des règles de protection des données ?
    - i. Non, il n'y a pas de règles de protection des données et il convient de négocier l'intégration de clauses de protection des données
    - ii. Oui, il y a des clauses. Sont-elles conformes au regard du projet<sup>2</sup> et suffisantes au regard de la LPrD (cf. ci-après points 4 et suivants) ?
      - 1. Non, les clauses ne sont pas suffisantes et il convient de les négocier ou d'en ajouter des nouvelles (cf. ci-après points 4 et suivants)
      - 2. Oui, les clauses sont suffisantes et il n'y a pas d'autres actions à prendre.

<sup>2</sup> En pratique, l'on constate par exemple que certains sous-traitants prévoient dans leurs conditions générales qu'il est interdit d'utiliser le service proposé pour traiter des données sensibles (cf. art. 4 al. 1 ch. 2 LPrD pour la définition) alors que le projet de l'administration tend justement à transmettre des données sensibles au sous-traitant. Il s'agit d'un problème contractuel qu'il convient d'analyser en tout début de projet.

- b. Non, il n'y a pas de contrat. Il convient de conclure un contrat portant sur la fourniture de biens ou de services avec le fournisseur et d'y inclure les règles de protection des données (cf. ci-après points 4 et suivants).

Contenu du contrat :

- 4. Détermination des parties. Les parties au contrat sont-elles suffisamment définies ? Cela est important notamment pour savoir à qui effectivement on sous-traite le traitement de données personnelles.
- 5. But de la sous-traitance. Il convient de définir le but de la sous-traitance, les données concernées et le cadre dans lequel les données seront transmises. Le sous-traitant ne pourra traiter des données que dans ce cadre.
- 6. Obligations des parties. Il convient de s'assurer que le sous-traitant s'engage à traiter les données selon les principes généraux de protection des données tels que prévus par la LPrD et selon les instructions du responsable de traitement (le service métier de l'ACV). Le sous-traitant doit notamment s'engager à ne pas utiliser les données dans un autre but que celui communiqué par le responsable de traitement, cela même pour des données pseudonymisées et/ou anonymisées. Le sous-traitant doit s'engager à mettre en place toutes les mesures de sécurité techniques et organisationnelles pour s'assurer de l'intégrité, de la disponibilité et la confidentialité des données et d'informer dans les plus brefs délais le responsable du traitement de tout manquement dans la sécurité des données, de tout accès indu et de toute perte de données. Le sous-traitant devra également informer le responsable du traitement de toute transmission de données à un tiers, même non prévue dans le contrat (par exemple, dans le cas d'une demande officielle comme une autorité judiciaire).
- 7. La sous-traitance en cascade. La sous-traitance en cascade est-elle autorisée ?
  - a. Non, la sous-traitance en cascade n'est pas autorisée et il convient de préciser dans le contrat qu'elle est interdite. Cette solution est dans la mesure du possible à retenir.
  - b. Oui, la sous-traitance en cascade est envisageable. Il faut alors prévoir à quelles conditions elle peut être mise en œuvre (accord ou simple information préalable, etc.). Il convient également de prévoir que, sur demande, le sous-traitant s'engage à transmettre au responsable du traitement la liste des sous-traitants en cascade<sup>3</sup>. Il faut encore rappeler que le sous-traitant reste entièrement responsable du respect de la LPrD et de l'éventuel secret de fonction par ses propres sous-traitants.
- 8. Lieux de traitement des données.
  - a. Le traitement des données aura-t-il lieu en Suisse ?
    - i. Non, le traitement a lieu à l'étranger. Il faut prévoir que le sous-traitant doit fournir une liste de l'ensemble des pays dans lesquels des données pourront être consultées (par exemple, à des fins de maintenance) et/ou hébergées tant par lui que par ses sous-sous-traitants.
      - 1. Les données seront traitées dans des pays disposant d'un niveau de protection adéquat (cf. [liste](#)) ?
        - a. Oui, les données seront traitées dans des pays disposant d'un niveau de protection adéquat et peuvent être communiquées à l'étranger, sous réserve des données soumises au secret de fonction (cf. point 2 ci-dessus)
        - b. Non, les données seront traitées dans des pays ne disposant pas d'un niveau de protection adéquat et des garanties supplémentaires doivent être obtenues contractuellement pour

<sup>3</sup> Attention, il convient de vérifier avant de conclure le contrat si de la sous-traitance en cascade est réalisée et, le cas échéant, qui sont les sous-traitants en cascade ainsi que le lieu où ils traitent les données personnelles.

s'assurer que le sous-traitant et ses éventuels sous-traitants respectent les règles de la LPrD (contrat de communication transfrontière de données). Attention aux données soumises au secret de fonction (cf. point 2 ci-dessus).

- ii. Oui, le traitement aura lieu en Suisse. Il faut néanmoins prévoir une garantie dans ce sens dans le contrat et s'assurer que les éventuels sous-traitants en cascade traitent les données uniquement en Suisse.
9. Droit de contrôle. Le responsable du traitement doit avoir la possibilité de s'assurer que le sous-traitant (et ses éventuels sous-traitants) respectent bien le contrat et les obligations de protection des données. Il faut notamment pouvoir accéder à tous les documents permettant de vérifier le respect des obligations (journal d'évènements, rapports d'audits, etc.). Un audit doit également pouvoir être mené par le responsable du traitement auprès du sous-traitant et de ses éventuels sous-traitants en cascade. L'autorité de surveillance de la LPrD (APDI) doit aussi avoir la possibilité d'effectuer des contrôles.
10. Droits des personnes concernées. Le sous-traitant doit s'engager à permettre au responsable du traitement de répondre aux demandes formulées par les personnes dont les données sont sous-traitées et à fournir, dans les plus brefs délais, au responsable de traitement toutes les informations et données nécessaires pour répondre à leurs demandes. Il s'agit notamment du droit d'accès à ses propres données<sup>4</sup>, du droit de destruction de données illicites, du droit de modification des données, etc. Il doit également s'engager à collaborer avec l'autorité de surveillance de la LPrD (APDI).
11. Responsabilités. Il convient de s'assurer contractuellement que le sous-traitant mette en place les mesures adéquates en lien avec la LPrD pour le traitement des données transmises dans le cadre de la sous-traitance. Il doit également être prévu que le sous-traitant est également responsable pour les faits des sous-traitants en cascade qu'ils soient autorisés ou non. Une indemnisation pleine et entière pour l'ensemble des dommages directs et indirects subis par le responsable du traitement et causés par le sous-traitant ou un sous-traitant en cascade devrait être prévue.
12. Résiliation du contrat. Il convient de prévoir un droit de résilier le contrat par le responsable du traitement, moyennant le respect d'un préavis, sauf dans les cas où de justes motifs (à prévoir dans le contrat ; problèmes graves de sécurité par exemple) permettent de résilier immédiatement le contrat. Les conséquences de la résiliation du contrat doivent être prévues. Il s'agit notamment de l'obligation de restituer dans les plus brefs délais toutes les données au responsable du traitement et de détruire l'ensemble des copies de ces données. Le sous-traitant reste soumis aux règles de la LPrD dans ce cadre. Il est aussi utile de prévoir la transition vers un autre sous-traitant.
13. For et droit applicable. Le droit suisse est-il applicable et un for en Suisse<sup>5</sup> est-il prévu ?
  - a. Oui, le droit suisse s'applique et le for est en Suisse. Des données sensibles et des données soumises au secret de fonction peuvent être transmises si les autres conditions sont également remplies (cf. point 2). Il convient dans tous les cas de préférer le droit matériel suisse à un droit étranger.
  - b. Non, le droit suisse ne s'applique pas et/ou un for à l'étranger est prévu. Il convient dès lors de ne transmettre des données soumises au secret de fonction que de manière chiffrée selon les modalités du point 2.b. La décision doit être prise par le chef de service. Dans la mesure du possible on essayera d'avoir au moins un for alternatif (par exemple for du défendeur) et l'application du droit matériel suisse.

<sup>4</sup> A noter que le responsable de traitement dispose d'un délai (prévu par la loi) de 30 jours pour répondre aux demandes de droit d'accès qui lui sont adressées.

<sup>5</sup> For exclusif en Suisse romande de préférence.

---

**C. Étude d'opportunité pour un *cloud* souverain –  
document de cadrage, Conférence latine des directeurs  
du numérique**

**cldn:**  
conférence latine des  
directeurs du numérique  
fr · ge · ju · ne · ti · vd · vs

**Etude d'opportunité pour un *cloud* souverain**

**Document de cadrage**

*Document de cadrage rédigé par le Canton de Vaud (Catherine Pugin) et le  
Canton de Genève (Alexander Barclay), janvier 2022*

1

## 1. INTRODUCTION

Dans le cadre de la transition numérique de l'Etat de Vaud, la Direction générale du Numérique et des Systèmes d'Information (DGNSI), en charge de la coordination de la mise en œuvre de la Stratégie numérique du Canton de Vaud, s'interroge sur les enjeux, les impacts, l'opportunité et la faisabilité d'un cloud souverain et de manière plus globale sur le rôle de l'Etat dans ce contexte. Cette réflexion est également en cours dans d'autres cantons latins.

Ainsi, le Canton de Vaud, dans le cadre de la Conférence latine des directeurs du numérique (CLDN) et en collaboration avec d'autres cantons, souhaite mandater un prestataire externe pour la réalisation d'une étude d'opportunité sur ce thème.

L'objectif de cette étude est d'explorer la thématique du cloud souverain et des différentes variables qui le caractérisent. Les résultats de cette étude permettront de poser le cadre du développement futur en identifiant des pistes d'action (technologiques, réglementaires, politiques, de gouvernance, etc.) pour réaliser pleinement – ou dans la proportion la plus acceptable - un cloud souverain en Suisse.

Cette étude n'a pas vocation à explorer des domaines de politique publique particuliers (santé, éducation, etc.) mais ses résultats généraux devront être déclinables pour ces derniers si nécessaire.

## 2. CONTEXTE

La Confédération a mené une étude sur un cloud suisse qui conclut que la nécessité de disposer d'une telle infrastructure n'était pas avérée. Suite à cette étude, elle a attribué un mandat à plusieurs acteurs étrangers pour le développement de services cloud. Aucun acteur privé suisse n'a participé à l'appel d'offres.

Les cantons latins, dans le cadre d'une réflexion globale sur la souveraineté numérique mais également aux prises avec le développement de leur informatique respective, souhaitent aujourd'hui aborder cette question pour d'une part définir de manière plus précise la notion de souveraineté dans le cadre des technologies cloud et d'autre part évaluer différentes variantes de faisabilité. L'objectif est de donner à chaque canton la possibilité de poser le curseur politique par rapport à sa vision et son interprétation de la souveraineté numérique.

Au sein du Parlement fédéral, deux initiatives ont également été déposées par des parlementaires romands sur la question des infrastructures souveraines.

### 2.1 Contexte vaudois

La Stratégie numérique du Canton de Vaud, adoptée en novembre 2018 par le Conseil d'Etat, accompagne la transition numérique du Canton en définissant



une vision globale et cohérente de l'action de l'Etat. Elle est construite autour de cinq thématiques ou ancres (Donnée, Infrastructures et sécurité, Accompagnement des personnes, Accompagnement des entreprises, Gouvernance). Elle rappelle avant tout que le rôle de l'Etat ne change pas dans le contexte de la transition numérique.

L'ancre « Infrastructures et Sécurité » replace les enjeux de la transition numérique dans leur forme la plus concrète et la plus tangible en identifiant tout d'abord les infrastructures du numérique existantes : le réseau et les éléments techniques qui le composent (fibres optiques, câblage, antennes, relais, etc.) ainsi que les centres de données nécessaires au stockage des informations. Si le *cloud* peut parfois apparaître comme un élément lointain et immatériel, il reste cependant bien réel et concret, puisque pour supporter ce type de technologie, la mise en place d'infrastructures matérielles et tangibles est nécessaire. De plus, la relation de dépendance entre le fonctionnement de l'administration publique et ses outils informatiques soulève de nouveaux défis.

Les administrations publiques, à l'instar entreprises privées, sont de plus en plus contraintes de suivre l'innovation imposée par les éditeurs de solutions informatiques : en effet, ces éditeurs tendent à injecter toujours plus de technologie *cloud* dans leurs applications.

C'est dans ce contexte que le Canton de Vaud financera et pilotera cette étude, de manière coordonnée avec les autres cantons latins intéressés.

### 3. DIMENSIONS DU CLOUD SOUVERAIN

Le recours à une solution externalisée *cloud* soulève la question de la sécurité, de la localisation des données, de problématiques juridiques ainsi que de l'éventuelle dépendance à des acteurs privés. De plus, ces technologies sont significativement énergivores, ce qui implique une réflexion en termes de durabilité.

L'étude devra donc examiner les différentes variables du *cloud* sous l'angle de la souveraineté. Ces différentes dimensions sont, par exemple, les données, les logiciels, les accès, les infrastructures et leur durabilité, la maintenance, la dépendance, la réglementation, la contractualisation, les aspects transfrontières ou encore les enjeux géostratégiques.

#### 3.1 Cybersécurité

Le *cloud* n'est pas une réponse en soi aux problèmes de cybersécurité, en particulier les cyberattaques. Au contraire, il rajoute une couche de complexité supplémentaire en matière de sécurité.

Partant de ce constat, la mise en place d'un *cloud* souverain implique surtout la mise en place de mesures de sécurité techniques et organisationnelles de premier ordre, propres à garantir la sécurité des systèmes d'information.

Les acteurs majeurs du *cloud* actuels sont également la cible de cyberattaques. Certes, ces géants des technologies de l'information ont des moyens conséquents et adéquats pour y faire face. Cependant, leur sécurité *stricto sensu* n'empêche pas la survenance de risques majeurs pour le client. Ces

risques peuvent constituer en des atteintes à la confidentialité, intégrité et disponibilité des données. L'origine de ces risques peut être accidentelle, stratégique, géopolitique, malveillante et criminelle ou même d'erreur humaine, de par l'évidente dépendance du client envers son fournisseur.

### 3.2 Localisation des données

Il s'agit de rappeler ici la territorialité du numérique : loin d'être un nuage intangible et abstrait, il s'agit d'infrastructures physiques localisées sur un territoire, avec une possible multiplication des ordres juridiques impliqués. Par exemple, la stratégie poursuivie par la Confédération semble être de labelliser des *clouds* qui respecteraient le principe de souveraineté des données (également hors du territoire) plutôt que de développer une infrastructure dédiée sur le territoire suisse.

La création d'un *cloud* souverain pourrait-il permettre de garder la maîtrise sur le droit applicable (contractualisation et protection des données, etc.), et l'éventuelle ingérence d'Etat étrangers (par exemple par la coupure ces accès rendant impossible l'utilisation des données) ?

### 3.3 Services

Le recours au *cloud* permet, selon la solution retenue, d'avoir accès à des services apportant des bénéfices majeurs. Selon les pistes de *cloud* souverain envisagées, à quels types de services pourrions-nous accéder ? Quels opportunités et risques ? Quelles implications en terme de souveraineté ?

Lister ces services pourrait permettre de comprendre la différence entre les acteurs locaux en matière de *cloud* et les acteurs internationaux de type « hyperscaler ».

En termes de services, il est important d'identifier les différentes parties prenantes et leurs besoins spécifiques en matière de *cloud* : IT qui acquiert les services, le métier qui les utilise, les individus et les entreprises dont les données sont traitées au sein de cette infrastructure.

### 3.4 Aspects comptables

L'utilisation d'un *cloud* peut impliquer un changement de logique comptable dans les comptes publics, passant d'une logique de budget d'investissement à une logique de budget de fonctionnement (p.ex. location de service). La justification politique de ces budgets peut donc être amenée à évoluer.

### 3.5 Modèle économique

Le *cloud* souverain devra s'appuyer sur un modèle économique clairement formulé.

### 3.6 Dépendance et aspects juridiques

Le *cloud* souverain pose la question de la maîtrise et du contrôle sur les données. Un *cloud* souverain nécessite-t-il, pour permettre de répondre aux exigences légales et politiques, une localisation des données sur le territoire suisse ? Qu'en est-il de l'accès à distance aux données pour des raisons de maintenance et/ou de support des systèmes ?

S'agissant de la localisation sur le territoire suisse, la question des ambassades est particulièrement intéressante sachant qu'elles se trouvent sur le territoire national tout en étant dispersées sur les cinq continents (cf. projet estonien de « Data embassies »).

Le sujet du *cloud* est particulièrement sensible dès lors que des données personnelles sont concernées. En effet, tous les pays n'offrent pas de réglementations équivalentes en matière de respect de la sphère privée.

De plus, nonobstant un contrat soigneusement rédigé avec le fournisseur, il ne sera pas opposable aux autorités du lieu d'hébergement des données en cas de requête judiciaire ou officielle (*Patriot Act* ou *Cloud Act par ex.*). Dans tous les cas, il convient de rappeler que l'utilisation de la technologie *cloud* à l'étranger (fournisseur étranger) implique une perte de maîtrise au moins partielle sur les données traitées et sur notre capacité à exercer notre puissance publique puisqu'il s'agit d'une externalisation *de facto* et *de jure*.

Il convient de signaler, qu'en tant qu'administration publique, la problématique du secret de fonction s'ajoute aux problématiques susmentionnées. Il est envisageable de garantir ce secret en cas d'externalisation auprès d'un fournisseur suisse uniquement. En revanche, l'externalisation auprès d'un fournisseur à l'étranger ou un fournisseur étranger sis sur le territoire suisse ne permet vraisemblablement pas de garantir ce secret, et pourrait exposer la collectivité publique à des poursuites pénales pour violation de l'art. 320 du Code Pénal suisse (311.0 ; CP).

### 3.7 Souveraineté numérique

La réalisation d'un *cloud* souverain s'inscrit dans une certaine définition de la souveraineté, dont le concept est challengé à l'ère numérique. Un rapport analysant la souveraineté à l'ère numérique, tenant compte d'enjeux géostratégiques, techniques et politiques et dans une perspective prospective, sera confié à un groupe pluridisciplinaire de chercheurs (juridique, technique, sciences politiques, relations internationales). Il viendra compléter le reste de l'étude en contextualisant le cas du *cloud* dans une perspective critique de la souveraineté à l'ère numérique.

Dans ce contexte, il sera nécessaire de se poser la question du rôle de l'Etat en matière d'infrastructures numériques, en particulier en lien avec le secteur public, le secteur privé, voire la société civile.

#### 4. CADRE DE L'ETUDE

L'étude devra dans un premier temps identifier les acteurs locaux et faire une analyse de leur offre en matière de *cloud* en lien avec l'offre des acteurs internationaux, en particulier de type « hyperscaler ». Elle procédera également à un rapide tour d'horizon sur l'utilisation du *cloud* dans les différents cantons.

Dans un deuxième temps, l'étude devra identifier et analyser les enjeux liés à la création d'un *cloud* souverain, en lien avec les différentes dimensions décrites ci-dessus.

Dans un dernier temps, elle devra donner des pistes d'action et des variantes pour la réalisation d'un *cloud* souverain, éventuellement dans le cadre d'un partenariat public – privé, qui permette à l'Etat de jouer son rôle sous ses différentes casquettes (administration, service public, propriétaire d'infrastructure, ...) dans le cadre d'une société numérique en construction et qui bénéficie à l'ensemble des parties prenantes.

---

# Le Code de conduite CISPE des fournisseurs d'infrastructures Cloud relatif à la protection des données

AURÉLIEN ROCHER

Docteur en droit, Maître de conférences, Université Lumière Lyon 2  
(Equipe de recherches « Transversales »)

## Table des matières

<b>I. Introduction .....</b>	<b>201</b>
<b>II. Contenu du Code CISPE.....</b>	<b>204</b>
A. Champ d'application .....	204
B. Exigences .....	205
1. Les exigences générales de protection des données .....	205
2. Les exigences spéciales de transparence .....	210
C. Fonctionnement.....	210
1. Les modalités d'adhésion .....	210
2. La gouvernance du Code CISPE .....	211
D. Annexes.....	211
<b>III. Portée du Code de conduite au regard du RGPD .....</b>	<b>212</b>
A. L'approbation du Code de conduite CISPE .....	212
B. Les effets de l'approbation du Code de conduite CISPE.....	213
<b>IV. Perspectives pour les utilisateurs en Suisse .....</b>	<b>214</b>
<b>V. Conclusion.....</b>	<b>216</b>
<b>VI. Bibliographie .....</b>	<b>217</b>
A. Doctrine.....	217
B. Textes officiels.....	218

## I. Introduction

Le recours croissant aux solutions d'informatique en nuage (*cloud*) provoque de nombreux défis en matière de conformité aux règles de droit de la protection des données, et tout particulièrement au regard du Règlement (UE)

2016/679 du Parlement européen et du Conseil du 27 avril 2016 (« RGPD »)<sup>1</sup> et de la loi fédérale sur la protection des données (LPD ; RS 235.1). L'usage de ces infrastructures informatiques externalisées combine effectivement un grand nombre de sujets (recours à des intermédiaires, sécurité des activités de traitement, gouvernance des processus, transferts de données à l'étranger, *etc.*) qui peuvent mettre à mal le respect du principe cardinal de responsabilité ('*accountability*') au sens de l'article 5 par. 2 du RGPD. Dans ce contexte, la nouvelle de la publication par l'association à but non lucratif de droit belge *Cloud Infrastructure Services Providers in Europe* (« CISPE ») d'un code de conduite approuvé au sens de l'article 40 du RGPD (le « Code CISPE » ou le « Code ») a été accueillie très favorablement par les nombreux acheteurs et utilisateurs de ces solutions. Pour mémoire, CISPE regroupe un grand nombre de prestataires de solutions *cloud*<sup>2</sup> et se positionne comme la voix des fournisseurs d'infrastructures *cloud* en Europe, en accord avec ses objectifs visés à l'article 4.2 de ses statuts<sup>3</sup>. L'une des activités principales de l'association correspond au développement, à la gestion et à l'actualisation du Code CISPE mais ses actions ne s'arrêtent pas là. Elles incluent notamment une participation au projet GAIA-X<sup>4</sup> ainsi qu'au groupe de travail multipartite SWIPO (*Switching Cloud Providers and Porting Data*) mis en place par la Commission européenne et ayant abouti à la rédaction de deux codes de conduite, au sens de l'article 6 du Règlement (UE) 2018/1807 du parlement européen et du conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne<sup>5</sup>. Tant pour le premier (qui concerne les fournisseurs d'infrastructures *cloud – IaaS*)<sup>6</sup> que pour le second (qui est consacré aux services *cloud - SaaS*)<sup>7</sup>, l'objectif est de faciliter le changement de fournisseurs de services et la portabilité des données. C'est

---

<sup>1</sup> V. pour une étude d'ensemble : KUNER/BYGRAVE/DOCKSEY.

<sup>2</sup> Au 3 octobre 2022, 25 membres, essentiellement européens mais incluant aussi des prestataires globaux comme AWS : <<https://cispe.cloud/members/>> (consulté le 3 octobre 2022).

<sup>3</sup> Article 4.2 des statuts de l'association sans but lucratif de droit belge CISPE.

<sup>4</sup> Initiative portée par la France et l'Allemagne visant à créer un cloud souverain européen répondant à la législation et aux valeurs de l'Union européenne, conduite sous la forme d'une association internationale sans but lucratif de droit belge : Gaia-X European Association for Data and Cloud AISBL. V., à ce sujet : BERTRAND, p. 139.

<sup>5</sup> Ce Règlement européen est le pendant du RGPD pour les données non personnelles et fixe en son article 4 un principe de libre circulation de ces données en interdisant les exigences de localisation « *sauf si elles sont justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité* ». Ce faisant, ce texte érige une 5<sup>e</sup> liberté communautaire, se rajoutant aux quatre libertés du marché unique (liberté de circulation des personnes, des biens, des services et des capitaux).

<sup>6</sup> SWIPO AISBL, Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services, v. 3.0., 27 May 2020.

<sup>7</sup> SWIPO AISBL, Code of Conduct Switching and Portability of data related to Software as a Service (SaaS), 8 July 2020.

donc un acteur majeur du *cloud* en Europe, rompu à l'exercice d'autorégulation encouragé par les réglementations européennes (RGPD et règlement de libre flux des données non personnelles), qui a établi un outil de gestion de la conformité RGPD non négligeable pour tous les utilisateurs de solutions *cloud*.

Sur le plan du droit des sources, le recours au dispositif du code de conduite est intéressant, puisqu'il est traditionnellement perçu comme une norme hybride<sup>8</sup>. À l'image du Dieu antique Janus, le code de conduite présente un double visage, empruntant pour partie à la *hard law*, pour partie à la *soft law*. Il se retrouve fréquemment dans les domaines relevant du droit de la *compliance*<sup>9</sup>, notamment sur des matières liées à la protection de l'environnement<sup>10</sup> ou la lutte contre la corruption<sup>11</sup>. Dans le contexte du RGPD, le code de conduite renvoie à un ensemble de règles « destinées à contribuer à la bonne application du règlement »<sup>12</sup>, élaboré par des associations professionnelles selon une procédure volontaire et régie par une section spécifique du RGPD. Un dispositif similaire est prévu par la nouvelle loi fédérale sur la protection des données (nLPD)<sup>13</sup> en son article 11. Dans les deux cas, le code de conduite s'apparente à une norme, au sens de la conception kelsénienne la définissant comme « la signification d'un acte par lequel une conduite est ou prescrite ou permise et en particulier habilitée »<sup>14</sup>. L'origine de cette norme est toutefois complexe mêlant une source légale (RGPD ou nLPD), une initiative privée (l'association professionnelle) et un contrôle par un organe public (autorité nationale de protection des données d'un État membre de l'Union européenne ou préposé fédéral à la protection des données). Les sanctions d'éventuels manquements aux prescriptions de ces normes hybrides sont donc variables et nécessitent des développements particuliers.

La présente contribution ambitionne de synthétiser les apports du Code CISPE pour les prestataires de services d'infrastructures *cloud* en précisant son champ d'application et son contenu (II.), sa portée au regard du RGPD (III.) et les perspectives qu'il offre aux utilisateurs de ces services en Suisse (IV.).

---

<sup>8</sup> LAROUER.

<sup>9</sup> FRISON-ROCHE, Tracer les cercles du Droit de la Compliance.

<sup>10</sup> RACINE, p. 409-424.

<sup>11</sup> FRISON-ROCHE, Régulation, Supervision, Compliance.

<sup>12</sup> Art. 40, par. 1, RGPD.

<sup>13</sup> V., pour un commentaire extensif : MÉTILLE.

<sup>14</sup> KELSEN.

## II. Contenu du Code CISPE

La structure du Code CISPE précise successivement son champ d'application (A.), ses exigences (B.), son fonctionnement (C.) et fournit un grand nombre de détails techniques dans ses sept annexes (D.).

### A. Champ d'application

Sur le plan matériel, le champ d'application du Code CISPE comporte deux limites. D'une part, il « *se concentre sur les fournisseurs Infrastructure-as-a-Service* »<sup>15</sup>, désignés dans le document comme *Cloud Infrastructure Services Providers* (« *CISPs* ») et entendus comme ceux fournissant « *uniquement du matériel informatique ou une infrastructure informatique virtualisée* » par opposition aux prestataires *Software-as-a-Service*, lesquels « *proposent en principe une application logicielle spécifiquement conçue pour traiter des données à caractère personnel* »<sup>16</sup>. Sont donc visés ici uniquement les fournisseurs d'infrastructures informatiques en nuage et non les prestataires *SaaS* lesquels ne mettent pas à disposition de leurs clients ces infrastructures mais uniquement des applications immédiatement opérationnelles. D'autre part, il se limite aux *CISPs* agissant en qualité de sous-traitants au sens de l'article 4 par. 8 du RGPD. Il résulte de cette double limitation matérielle que l'ensemble des prestataires *SaaS* ne sont pas couverts par les mécanismes prévus par ce Code, de même que les activités réalisées par les fournisseurs *IaaS* en qualité de responsable du traitement tel que défini à l'article 4 par. 7 du RGPD.

Sur le plan territorial, son champ d'application est transnational. Il est certes annoncé que le territoire cible est celui de tous les États membres de l'Espace Économique Européen (EEE) mais, prenant en compte le caractère volontaire de l'adhésion au Code, « *les CISPs qui ne sont pas soumis aux dispositions du RGPD peuvent également décider, de leur plein gré, de se soumettre [à ses] dispositions* »<sup>17</sup>. L'articulation de ces deux précisions permet de distinguer entre (i) les *CISPs* établis sur le territoire national d'un État membre de l'Espace Économique Européen (EEE) et entrant dans le champ d'application – territorial ou extraterritorial – du RGPD de ceux qui (ii) sont établis au sein de l'EEE mais n'entrent pas dans le champ d'application du RGPD. Pour les *CISPs* établis hors EEE, qui sont donc hors champ du Code CISPE, il y a, encore une fois, lieu de distinguer entre ceux qui (i) sont pleinement soumis au RGPD de ceux (ii) qui ne le sont pas. Le critère le plus pertinent, au-delà du

---

<sup>15</sup> Code CISPE, Introduction, p. 5.

<sup>16</sup> *Ibid.*

<sup>17</sup> Code CISPE, 3, p. 12.



lieu d'établissement, est donc celui de l'application du RGPD car c'est l'objet même du Code CISPE que d'« *aider les CISPs à s'assurer du respect des dispositions du RGPD* »<sup>18</sup>. Indépendamment de leur lieu d'établissement, les opérateurs soumis au champ d'application territorial ou extraterritorial du RGPD<sup>19</sup> ont donc un intérêt direct à se soumettre au Code CISPE qui leur permettra de faciliter la démonstration de leur conformité au RGPD. Pour ceux qui ne seraient pas soumis au RGPD mais qui peuvent sur une base volontaire adhérer au Code CISPE, l'intérêt se situe ailleurs, sur le plan commercial, en pouvant jouir de la marque associée à ce code de conduite et séduire davantage de clients.

## B. Exigences

Le Code détaille ses exigences en deux catégories, la première déclinant toutes les exigences générales découlant strictement de l'application de l'ensemble du RGPD (1), la seconde requérant des mesures spéciales de transparence (2).

### 1. Les exigences générales de protection des données

Sans surprise, l'essentiel du contenu de cet « *instrument démontrant la conformité* »<sup>20</sup> au RGPD détaille les exigences attendues de tous ses adhérents quant à la protection des données personnelles, ce qui correspond à la définition légale du code de conduite, lequel doit « *préciser les modalités d'application du présent règlement* »<sup>21</sup>. Pour rappel, le RGPD fournit une liste, non-exhaustive, de ces dernières qui recouvrent notamment :

- a) le traitement loyal et transparent ;
- b) les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques ;
- c) la collecte des données à caractère personnel ;
- d) la pseudonymisation des données à caractère personnel ;
- e) les informations communiquées au public et aux personnes concernées ;
- f) l'exercice des droits des personnes concernées ;
- g) les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l'enfant ;

---

<sup>18</sup> Code CISPE, Introduction, p. 5.

<sup>19</sup> MÉTILLE/ACKERMANN.

<sup>20</sup> DOUVILLE, p. 240.

<sup>21</sup> Art. 40 par. 1 RGPD.

- h) les mesures et les procédures visées aux articles 24 et 25 et les mesures visant à assurer la sécurité du traitement visées à l'article 32 ;
- i) la notification aux autorités de contrôle des violations de données à caractère personnel et la communication de ces violations aux personnes concernées ;
- j) le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales ; ou
- k) les procédures extrajudiciaires et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement<sup>22</sup>.

Pour les adhérents non soumis au RGPD, le respect du Code CISPE peut être accompagné d'une déclaration publique affichant la volonté d'élever leurs exigences en matière de protection des données au niveau des standards de références posés par le RGPD, tout en soulignant que cette adhésion n'entraîne pas présomption d'applicabilité du RGPD, pour éviter toute ambiguïté potentiellement préjudiciable.

La méthodologie suivie par les rédacteurs du Code a consisté à reprendre toutes les exigences listées dans des dispositions du RGPD applicables à un sous-traitant et, pour chacune d'elles, de préciser l'obligation afférente pour le CISP tout en expliquant les raisons correspondantes. Dix points du RGPD sont couverts et explicités, à savoir successivement (i) le contrat avec le CISP, (ii) la sécurité, (iii) le transfert des données personnelles vers des pays tiers, (iv) la sous-traitance, (v) la démonstration du respect du RGPD, (vi) les droits des personnes concernées, (vii) le personnel du CISP, (viii) la violation des données, (ix) la suppression ou restitution de données personnelles et (x) les registres des activités de traitement. Pour tous ces sujets, des obligations précises sont mises à la charge du CISP agissant comme sous-traitant mais ce mouvement n'est pas qu'à sens unique. À diverses reprises, le Code rappelle effectivement les éléments relevant de la responsabilité du client du CISP agissant comme responsable de traitement. Il en va ainsi de la détermination de la licéité du traitement de données personnelles dont le responsable du traitement doit s'assurer<sup>23</sup> tandis que le sous-traitant doit simplement traiter ces dernières « *sur instruction documentée du responsable du traitement* »<sup>24</sup>. Relevons à cet égard que le client du CISP n'est évidemment pas adhérent du Code CISPE et donc non soumis aux règles que ce dernier édicte. Pour autant, les CISPs soumis audit code de conduite auront toujours la latitude de reprendre les clés de répartition proposées par les rédacteurs du Code CISPE et de les appliquer, contractuellement, à leurs clients. Ils peuvent d'autant plus procéder de la sorte que le Code CISPE est

---

<sup>22</sup> Art. 40 par. 2 RGPD.

<sup>23</sup> Art. 5 par. 1 RGPD.

<sup>24</sup> Art. 283 par. 3 let. a et art. 29 RGPD.

auréolé de son approbation par la CNIL. Les rédacteurs du Code apportent d'utiles clarifications sur chacun des points précités mais ce sont surtout les développements sur la sécurité et sur les notifications de violations de sécurité, les seuls à bénéficier d'une annexe dédiée, qui fournissent de nombreux enseignements.

En pratique, les professionnels en charge d'un projet *cloud* savent que la clé de la conformité RGPD se situe dans la juste combinaison des mesures contractuelles, techniques et organisationnelles. Toute la question reste alors de savoir où placer le curseur, étant noté que les autorités européennes ont déjà précisé que les mesures techniques étaient les plus sûres, davantage que celles contenues dans un contrat qui, par hypothèse, pourraient être écartées par les dispositions d'une loi étrangère impérative<sup>25</sup>. Pour la sécurité, la grande *summa divisio* est celle qui distingue la sécurité de l'infrastructure, d'une part, et des données traitées, d'autre part. Pour la première, la responsabilité de la sécurité est à la charge du CISP, ce qui recouvre « *le matériel informatique, le logiciel d'exploitation hôte (si celui-ci s'applique au service proposé), la mise en réseau et les installations qui permettent d'exécuter les services d'infrastructure cloud* »<sup>26</sup>, ainsi qu'un mécanisme de filtrage des flux de données, comme un pare-feu. Pour les secondes, la responsabilité du client du CISP correspond à « *la gestion du système d'exploitation invité (y compris les mises à jour et patchs de sécurité), de tout logiciel applicatif ou tous équipements qu'il a installés pour ce service, ainsi que la configuration du pare-feu fourni par le CISP pour chaque instance, [...] la sécurité des données en transit et de ses identifiants de connexion, et la gestion des autorisations qu'il accorde aux membres de son personnel qui utilisent le service* »<sup>27</sup>. Par ailleurs, le CISP a l'obligation « *d'établir un programme sur la sécurité de l'information [et de] procéder à des examens réguliers de la sécurité du réseau du CISP et de l'adéquation de son programme sur la sécurité de l'information* »<sup>28</sup>.

En matière de notification de violation de sécurité, le Code précise que le CISP doit établir une politique de gestion des incidents qui décrit les procédures d'identification et de réponses aux violations de données à caractère personnel et fournit également un modèle de notification à utiliser pour dûment informer les clients impactés par la violation. Ces obligations ne se substituent pas à

---

<sup>25</sup> CEPD, Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, version 2.0, n. 69.

<sup>26</sup> Code CISPE, 4.3, p. 19.

<sup>27</sup> *Ibid.*

<sup>28</sup> Code CISPE, 4.3, p. 20.

celles énoncées par le RGPD et prévoyant, le cas échéant, une communication aux autorités de contrôle compétentes et aux personnes concernées<sup>29</sup>.

Sans dresser un inventaire à la Prévert des autres dispositions instructives du Code, mentionnons tout de même les clarifications apportées sur les sujets du contrat liant le CISPE et son client, les transferts de données personnelles vers les États tiers et la documentation de la conformité RGPD. Pour le premier, le Code retient une approche souple et pragmatique en exigeant un contrat écrit (ce qui inclut la forme électronique), ayant force obligatoire pour les parties et dont le contenu, en accord avec l'article 28 par. 3 du RGPD, doit faire référence aux sections pertinentes du Code, tout en précisant que sa forme est indifférente (contrat unique, simples conditions générales ou ensemble contractuel complexe).

Pour le deuxième, les rédacteurs commencent par rappeler que ce document « *n'a pas vocation à servir de garantie pour les transferts transfrontaliers de données à caractère personnel* »<sup>30</sup>, lesquels doivent répondre aux conditions posées par le droit européen en la matière (à savoir essentiellement les dispositifs visés à l'article 46 du RGPD : notamment recours aux clauses contractuelles types ou encore aux règles d'entreprise contraignantes). Ils précisent également que le CISPE doit aider les clients, en tant qu'exportateurs, à se conformer à leurs obligations en la matière. Cela recouvre notamment la fourniture « *d'informations appropriées, notamment sur le lieu du traitement concerné, afin de permettre au client de vérifier au cas par cas, avant tout transfert, si la législation ou la pratique du pays tiers concerné assure le niveau de protection des données requis dans l'EEE, de manière à déterminer si les garanties fournies par les garanties appropriées choisies peuvent être en pratique respectées* ». Bien plus, le Code spécifie que le fournisseur *IaaS* doit vérifier au cas par cas, en cas de demande étatique étrangère de divulgation de données personnelles « *si le jugement ou la décision correspondante peut être reconnu ou exécuté sur la base d'un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, afin de garantir la légalité de ce transfert ou de cette divulgation* »<sup>31</sup>. À défaut, il est expressément prévu qu'il mette en œuvre les mesures nécessaires garantissant le refus d'une telle demande. Ce dernier point est tout particulièrement intéressant dans le contexte du *Clarifying Lawful Overseas Use of Data (CLOUD) Act*<sup>32</sup>, promulgué le 25 mars 2018, lequel amende le *Stored Communications Act* de 1986<sup>33</sup> afin d'étendre la possibilité pour le juge américain d'enjoindre aux

---

<sup>29</sup> Art. 33 et 34 RGPD.

<sup>30</sup> Code CISPE, 4.4, p. 24.

<sup>31</sup> Code CISPE, 4.4., p. 22.

<sup>32</sup> Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 1213 (2018) (codified in scattered sections of 18 U.S.C.).

<sup>33</sup> Stored Communications Act, 18 U.S.C. Chapter 2701, et seq., as amended by the Cloud Act, Pub. L. 115-141.

opérateurs de solutions *cloud* relevant de la compétence des États-Unis de transmettre les informations nécessaires à la poursuite d'une investigation pénale, où qu'elles se trouvent<sup>34</sup>. Le caractère extraterritorial de cette réglementation a été caractérisé par la doctrine<sup>35</sup>, les autorités européennes<sup>36</sup> et certaines juridictions d'États membres de l'Union européenne<sup>37</sup>, comme problématique au regard de la nécessaire protection équivalente des réglementations étrangères par rapport aux attentes édictées par le RGPD. Cette position retenue dans le Code par CISPE correspond donc à une garantie importante conférée par ses adhérents envers leurs clients puisqu'ils devraient alors s'opposer à une demande formulée en application du *US CLOUD Act*, puisque ce dernier ne correspond pas à un accord international entre les États-Unis et l'Union européenne ou l'un de ses États membres. Naturellement, cette garantie donnée par l'adhérent au Code CISPE est à combiner avec les autres mesures permettant la réalisation de ce transfert transfrontalier de données personnelles.

Pour le troisième, la documentation de l'état de conformité RGPD du fournisseur *IaaS* est facilitée par l'obligation de ce dernier de communiquer au client les informations et la documentation appropriées et de soumettre ses installations de traitement des données à des audits réalisés par un tiers indépendant. Le client est alors plus à même d'exercer ses droits en vertu de l'article 28 par. 3 let. h du RGPD, puisque le Code précise la nature des informations que le CISP doit fournir et la méthode de communication. Le recours à des accords de confidentialité est encouragé pour certaines informations sensibles, afin que le CISP soit assuré que ces dernières ne soient pas partagées avec des tiers, à l'exception de l'autorité de contrôle dont relève le client. Une liste illustrative est également insérée dans le Code CISPE pour expliciter les éléments de sécurité hautement sensibles que le fournisseur *IaaS* est légitime à ne pas communiquer et qu'il peut alors remplacer par un exposé de situation (p. ex : l'identité et la localisation du personnel en charge des opérations de sécurité ; les résultats détaillés des tests d'intrusion réalisés en interne, etc.).

---

<sup>34</sup> Cloud Act, sect. 3 : « *A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States* » (codifié sous 18 U.S.C., § 2713).

<sup>35</sup> BISMUTH, n° 80 ; SCHWARZ, p. 193 ; JACOB, p. 665.

<sup>36</sup> EDPB, "Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and negotiations of an EU-US Agreement on cross-border access to electronic evidence." (July 10, 2019).

<sup>37</sup> V. le mémoire en observations de la Présidente de la CNIL en date du 8 oct. 2020 dans le cadre du contentieux *Health Data Hub* : CE, ord., 13 oct. 2020, n° 444937, Association Le Conseil national du logiciel libre.

## 2. *Les exigences spéciales de transparence*

Ces obligations générales liées au RGPD sont complétées par d'autres exigences spéciales de transparence propres au statut de CISP pour l'ensemble des services déclarés conformes au Code. Ces éléments comprennent une déclaration d'ensemble sur les objectifs de sécurité et les normes applicables au service ainsi que des informations concernant la conception et la gestion du service, les processus de gestion du risque et des critères du CISP, les mesures de sécurité mises en place par le CISP pour le service, le fonctionnement du service pour répondre aux demandes d'exercice des droits des personnes concernées et de suppression ou récupération des données. L'accent est une nouvelle fois mis sur la sécurité de l'infrastructure et se distingue des obligations liées à la protection des données par le fait qu'il s'agit surtout ici d'assurer une transparence élevée quant à la conformité non pas avec le RGPD mais avec les dispositions du Code CISPE lui-même.

## C. **Fonctionnement**

Le fonctionnement du Code repose sur des modalités d'adhésion (1) et une gouvernance (2) bien définies.

### 1. *Les modalités d'adhésion*

Deux procédures d'adhésion au Code sont possibles à savoir l'auto-évaluation et l'adhésion contrôlée<sup>38</sup>. Dans la première, le candidat fournit au secrétariat du Code une déclaration d'adhésion, accompagnée d'une liste de contrôle de la conformité complète sur le modèle de celle fournie en annexe. Le secrétariat vérifie alors si la documentation remise est complète et si tel est le cas il procède alors à la consignation de la déclaration d'adhésion dans le registre public CISPE dans un délai de 10 jours ouvrés après avoir signifié son acceptation au CISP. Le registre public CISPE<sup>39</sup> doit indiquer clairement que le service concerné n'a pas encore été évalué et le présenter comme un service « candidat » jusqu'à son approbation par un organisme de contrôle accrédité. Une fois que le secrétariat CISPE reçoit cette confirmation écrite de conformité validée par l'organisme de contrôle, il actualise la mention portée au registre public pour attester de cette validation, ce qui permet au CISP considéré de jouir de la marque de conformité CISPE. La seconde procédure, dite d'adhésion

---

<sup>38</sup> Code CISPE, 6, p. 39.

<sup>39</sup> Accessible sur le site internet de l'association : <<https://www.codeofconduct.cloud/public-register/>> (consulté le 3 octobre 2022).

contrôlée, consiste en une inscription unique au registre public CISPE, en lieu et place de l'inscription en deux temps de l'auto-évaluation, car fondée sur la déclaration d'adhésion, la liste de contrôle de la conformité complète ainsi que la confirmation écrite délivrée par l'organisme de contrôle. Dans les deux cas, l'organisme de contrôle procède à un examen annuel de la conformité du CISP par rapport au Code et réalise un audit tous les trois ans dont le rapport est communiqué à CISPE.

## 2. *La gouvernance du Code CISPE*

Le Code requiert une gouvernance solide, à même de garantir des interactions efficaces entre les fournisseurs *IaaS* adhérents et candidats, organismes de contrôle, autorités de contrôle et autres parties prenantes. L'Association des fournisseurs européens d'infrastructures Cloud (CISPE) est responsable de la gouvernance du Code et divers organes sont instaurés à cette fin, mobilisant l'assemblée générale, le comité exécutif, la *task force* du Code de conduite (CCTF), le comité de surveillance indépendant du Code, le secrétariat et les observateurs. En dehors de cette constellation des organes internes au CISPE, les organismes et autorités de contrôle sont en charge des missions qui leur sont attribuées en application des articles 40 et 41 du RGPD. L'ensemble de ces organes et organismes permet ainsi d'assurer un suivi efficace du Code, de son application et de ses éventuelles modifications en fonction des changements réglementaires, d'instruire les réclamations et de prononcer ou superviser des mesures d'exécution.

## D. **Annexes**

Le Code comprend également sept annexes sur plus de 80 pages, dont la moitié est consacrée à la liste de contrôle de la conformité (annexe B). Celle-ci s'appréhende comme une matrice des rôles et responsabilités des CISPs eu égard aux exigences édictées par le Code. La seconde annexe bénéficiant du plus grand nombre de développements correspond à l'annexe A listant les pratiques techniques et organisationnelles en matière de sécurité et obligations en matière de sécurité. Elle explicite les exigences minimales portant sur la sécurité des informations, des ressources humaines, de la gestion de l'accès des utilisateurs, de la sécurité physique et environnementale, de la gestion de la protection contre les logiciels malveillants, de la gestion des vulnérabilités, de la journalisation et du monitoring et des équipements en fin de vie. Pour chacun de ces points, l'annexe distingue les mesures relevant de la responsabilité du CISP de celles à la charge du client et fournit également

des tableaux explicatifs citant des mesures envisageables pour les CISP. En termes de certifications, la norme ISO/IEC 27002 est recommandée comme document d'orientation pour mettre en œuvre les contrôles de sécurité de l'information généralement admis et les CISP qui sont accrédités ISO/IEC 27001, ISO/IEC 27018, ISO/IEC 27017, ou tout standard de référence équivalent, sont réputés respecter les exigences de sécurité du Code<sup>40</sup>.

### III. Portée du Code de conduite au regard du RGPD

Ayant reçu l'aval des autorités européennes (A.), le Code de conduite CISPE permet à ses adhérents de documenter et démontrer plus aisément leur niveau de conformité au RGPD (B.).

#### A. L'approbation du Code de conduite CISPE

Conformément aux prescriptions des lignes directrices relatives aux codes de conduite<sup>41</sup>, le Code CISPE a été examiné par la CNIL en tant qu'autorité de contrôle compétente, qui a ensuite soumis son projet de décision pour avis au comité européen de la protection des données (CEPD) le 29 février 2021. Dans son avis en date du 19 mai 2021<sup>42</sup>, le CEPD conclut à sa conformité avec le RGPD car ledit code de conduite (i) répond aux besoins du secteur, (ii) facilite l'application effective du RGPD et (iii) propose des mécanismes efficaces pour le contrôle de son respect. Par une délibération en date du 3 juin 2021<sup>43</sup>, la CNIL procède donc à l'approbation du Code. Fondée sur l'avis favorable du CEPD, elle relève que le Code répond aux exigences de forme prévues par l'article 40.2 du RGPD, précise son champ d'application matériel comme territorial ainsi que les modalités d'application du RGPD tout en prenant en compte les besoins des professionnels du secteur de l'informatique en nuage. Constatant également que le Code fournit à ses adhérents une matrice des exigences à respecter, juridiquement contraignantes du fait de leur adhésion au Code, la CNIL a considéré qu'il « *apporte ainsi une réelle valeur ajoutée aux futurs adhérents dans leur démarche de redevabilité* ». Cette décision a été

---

<sup>40</sup> Code CISPE, annexe A, p. 59.

<sup>41</sup> Lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du règlement 2016/679, adoptées par le comité européen de la protection des données le 4 juin 2019.

<sup>42</sup> CEPD, Avis 17/2021 sur le projet de décision de l'autorité de contrôle française concernant le code de conduite européen soumis par les prestataires de services d'infrastructure en nuage (CISPE), 29 mai 2021.

<sup>43</sup> CNIL, Délibération n° 2021-065 du 3 juin 2021 portant approbation du code de conduite européen porté par Cloud Infrastructure Service Providers Europe (CISPE).



suivie par plusieurs délibérations portant agrément des organismes de contrôle<sup>44</sup>, constatant que les organisations candidates se conforment bien au référentiel adopté à cet effet par la CNIL<sup>45</sup>. Dans ce dernier, la CNIL avait édicté les qualités attendues de l'organisme pour être en mesure de lui délivrer l'agrément, notamment sur l'expertise de son personnel, la gestion des conflits d'intérêts, l'indépendance fonctionnelle par rapport à la gouvernance du porteur du code de conduite mais aussi par rapport à l'ensemble des adhérents. Si ces conditions sont remplies, il appartient aux organismes agréés de réaliser les missions de contrôle et d'instruction prévus pour eux par le code de conduite, ce qui contribue à l'opérationnalisation de ce dernier<sup>46</sup>.

## **B. Les effets de l'approbation du Code de conduite CISPE**

L'approbation du Code CISPE permet, pour ses adhérents comme pour leurs clients, de bénéficier de certains avantages prévus par le RGPD. Tout d'abord, se référer à un code de conduite approuvé doit permettre de réduire les coûts de conformité dès lors que les processus sont davantage standardisés<sup>47</sup>. Ensuite, l'application d'un code de conduite approuvé est un élément permettant de démontrer la conformité avec les dispositions du RGPD sur la sécurité des traitements de données personnelles<sup>48</sup>. C'est notamment un critère pris en compte, en cas de manquement, pour le prononcé et la quantification d'éventuelles amendes administratives<sup>49</sup>. Enfin, il a pour effet de permettre à un responsable de traitement, faisant intervenir des sous-traitants appliquant un tel

---

<sup>44</sup> CNIL, Délibération n° 2021-076 du 17 juin 2021 portant agrément de EY CERTIFY-POINT B.V. en tant qu'organisme de contrôle du code de conduite européen porté par CISPE (Cloud Infrastructure Service Providers Europe) ; Délibération n° 2021-112 du 23 septembre 2021 portant agrément du Laboratoire national de métrologie et d'essai (LNE) en tant qu'organisme de contrôle du code de conduite européen porté par CISPE (Cloud Infrastructure Service Providers Europe) ; Délibération n° 2021-117 du 7 octobre 2021 portant agrément de Bureau Veritas Italia Spa en tant qu'organisme de contrôle du code de conduite européen porté par CISPE (Cloud Infrastructure Service Providers Europe).

<sup>45</sup> CNIL, Délibération n° 2020-050 du 30 avril 2020 portant adoption d'un référentiel relatif à l'agrément des organismes chargés de contrôler le respect des codes de conduite.

<sup>46</sup> À ce jour, trois organismes ont été agréés : Laboratoire national de métrologie et d'essai (LNE), Bureau Veritas Italia Spa, EY Certifypoint. <<https://www.cnil.fr/fr/organismes-agrees-controle-code-de-conduite>> (consulté le 3 octobre 2022).

<sup>47</sup> Lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du règlement 2016/679, adoptées par le comité européen de la protection des données le 4 juin 2019, spéc. n° 11.

<sup>48</sup> Art. 32 par. 3 RGPD.

<sup>49</sup> Art. 83 par. 2, let. j RGPD.

code de conduite, de démontrer qu'il a respecté ses obligations<sup>50</sup>. Plus largement et au-delà des dispositions du RGPD, un code de conduite approuvé a pour effet de contribuer à l'instauration d'un climat de confiance, notamment à l'égard des personnes concernées<sup>51</sup>, ce que précise expressément le Code CISPE dans son introduction<sup>52</sup>.

Le Code CISPE implique également la possibilité, sous conditions, de faire usage d'une marque de conformité définie en son article 6.4 comme « *un symbole, face au public, de l'adhésion d'un service aux exigences du Code* ». Différentes règles sont prévues pour régir l'usage de cette marque, avec deux symboles différents pour différencier les candidats (modalité d'adhésion par auto-évaluation tant que la candidature n'est pas entérinée) des adhérents validés. Pour maintenir la confiance des utilisateurs, les adhérents doivent s'assurer qu'ils utilisent cette marque pour les seuls services en conformité avec le Code, dès lors qu'ils peuvent choisir de ne pas soumettre l'ensemble des services de leurs catalogues aux dispositions du Code<sup>53</sup>. Il est toutefois à noter que cette marque ne s'analyse pas comme une marque au sens de l'article 46 du RGPD<sup>54</sup>. Cette restriction est conforme à la limitation générale applicable à l'ensemble du Code, lequel ne peut pas être utilisé comme un instrument de conformité à l'égard des transferts de données vers les États tiers<sup>55</sup>.

#### IV. Perspectives pour les utilisateurs en Suisse

Le Code CISPE reste une référence directement mobilisable en Suisse dès lors que les opérateurs nationaux sont soumis au respect des dispositions du RGPD, dont le caractère extraterritorial du champ d'application est bien

---

<sup>50</sup> Cons. 81 et art. 24 par. 3 RGPD : « *L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.* »

<sup>51</sup> DOUVILLE, p. 243.

<sup>52</sup> Code CISPE, introduction, p. 5.

<sup>53</sup> CISPE, Lignes directrices pour l'utilisation des marques.

<sup>54</sup> Code CISPE, 6.4, p. 46 : « *Pour lever toute ambiguïté, l'affichage de la Marque de Conformité ne se substitue pas au respect du RGPD et ne présume pas du respect des dispositions d'un code de conduite assorti d'engagements juridiquement contraignants et exécutoires en application de l'Art. 46 du RGPD.* »

<sup>55</sup> RGPD, art. 46 par. 2 let. j) : « *Les garanties appropriées visées au paragraphe 1 [pour justifier des transferts vers des pays tiers ou des organisations internationales] peuvent être fournies, sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle, par: [...] un code de conduite approuvé conformément à l'article 40, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.* »

connu<sup>56</sup>. Le Code rappelle également que son champ d'application territorial est « transnational » et que des fournisseurs *IaaS* non soumis au RGPD peuvent faire le choix de l'appliquer. Recourir à une solution *cloud* fournie par un opérateur adhérent au Code et bénéficiant de la marque correspondante contribue ainsi à démontrer un état minimum de conformité au RGPD. De même, les différentes mesures de conformité qu'il recommande ou impose à ses adhérents sont autant de pistes de réflexions et d'argumentaires potentiels pour aider les clients de solutions *IaaS* dans la négociation avec leurs fournisseurs *IaaS*, même non adhérents au Code. Dès lors qu'il s'agit du seul et premier document de ce type dans le secteur du *cloud*, il jouit d'une aura qui rayonne au-delà du périmètre de ses membres et peut être utilisé comme un utile catalogue de mesures envisageables à définir isolément au sein de l'entreprise ou conjointement avec le fournisseur *IaaS* considéré.

Le Code CISPE répond donc aux exigences de l'article 40 du RGPD et a une utilité certaine pour tous les opérateurs en Suisse soumis à cette réglementation européenne. Sous l'angle de la loi fédérale sur la protection des données (LPD), le Code CISPE ne bénéficie pas de reconnaissance automatique ce qui s'explique, d'une part, par la relative étanchéité des législations suisse et européennes<sup>57</sup> et, d'autre part, par la nature juridique particulière du code de conduite. En l'occurrence, le Code CISPE emprunte bien à la *soft law* (norme privée et volontaire) et à la *hard law*, mais celle-ci, au cas particulier, est européenne (article 40 du RGPD) et non pas suisse. Mobiliser cet outil est d'autant plus intéressant dans le contexte du droit suisse que la nouvelle loi fédérale sur la protection des données (nLPD)<sup>58</sup> prévoit aussi, en son article 11, cet instrument d'autorégulation pour simplifier la démonstration de la conformité au texte<sup>59</sup>. La logique est similaire, il s'agit de suivre une approche sectorielle et de permettre à un organisme fédérateur du secteur de préciser dans un code volontaire à portée obligatoire la manière dont la législation suisse de protection des données personnelles peut s'appliquer. C'est ensuite le Préposé fédéral à la protection des données et à la transparence (PFPDT) qui est invité à prendre position publiquement sur ce texte. Le PFPDT a d'ailleurs publié un

<sup>56</sup> V., à ce sujet : MÉTILLE/ACKERMANN.

<sup>57</sup> Pour une illustration, voir l'argumentation du préposé fédéral à la protection des données dans sa prise de position sur la transmission de données personnelles vers les États-Unis en date du 8 septembre 2020 qui rappelle que « l'arrêt précité de la CJUE [Schrems II] n'a pas d'effet contraignant pour la Suisse, puisque cette dernière n'est pas membre de l'UE » mais conclut tout de même que les États-Unis ne peuvent plus être considérés comme intégrés à la liste des États offrant une protection adéquate.

<sup>58</sup> V., pour un commentaire extensif : MÉTILLE.

<sup>59</sup> Art. 11 nLPD : « Les associations professionnelles, sectorielles et économiques, lorsqu'elles sont autorisées de par leurs statuts à défendre les intérêts économiques de leurs membres, de même que les organes fédéraux, peuvent soumettre leur code de conduite au PFPDT. Le PFPDT prend position sur les codes de conduite et publie ses prises de position. »

point de vue sur la nLPD dans lequel il a rappelé les bénéfiques à attendre d'un tel dispositif, notamment sur le fait qu'« *un avis positif du PFPDT [sur le code de conduite] justifiera la présomption légale que le comportement défini dans le code est conforme à la protection des données* »<sup>60</sup>. Le potentiel de cet outil normatif original a été souligné par la doctrine<sup>61</sup>, dans un contexte où les législations nationales se veulent agnostiques sur le plan technologique pour limiter le risque d'obsolescence des réglementations. Le corollaire de cette neutralité du législateur, et des dispositions générales qu'il édicte, réside dans le manque de détails concrets sur les moyens disponibles pour les mettre en œuvre. Ce vide législatif peut alors être partiellement comblé par ces codes de conduite, explicitant dans leurs secteurs d'activité les mesures nécessaires. Relevons tout de même que la *ratio legis* du législateur européen diffère sensiblement de celle retenue par son homologue helvétique. Parmi les différences notables, la procédure édictée par le RGPD et les lignes directrices publiées par le CEPD est complexe et requiert l'approbation obligatoire de l'autorité de contrôle compétente ainsi qu'un mécanisme de suivi par des organismes de contrôle devant être agréés par l'autorité en charge là où la soumission au PFDPT, bien que souhaitée par ce dernier<sup>62</sup>, n'est que facultative. L'ampleur des effets du recours au code de conduite est également amoindrie, essentiellement limitée à une dispense d'analyse d'impact relative à la protection des données (AIPD) dans certains cas<sup>63</sup> là où la soumission à un code de conduite au sens du RGPD a des effets plus larges, permettant de démontrer la conformité aux exigences en matière de sécurité des données<sup>64</sup> ou aux exigences attendues des responsables du traitement<sup>65</sup>.

## V. Conclusion

Le Code CISPE est un document qui fera date dans l'histoire de la protection des données personnelles. Premier code de conduite au sens du RGPD, il a pour objet le secteur des fournisseurs d'infrastructure *cloud*, qui

---

<sup>60</sup> PFDPT, *Nouvelle loi fédérale sur la protection des données : le point de vue du PFPDT*, 9 fév. 2021, p. 5, n° 8.

<sup>61</sup> COSSALI SAUVAIN/DUBOIS.

<sup>62</sup> Message LPD 2017, FF 2017 p. 6654.

<sup>63</sup> ROSENTHAL/STUDER/LOMBARD (pour la traduction), spéc. n° 175 et s.

<sup>64</sup> Art. 32 par. 3 RGPD : « *L'application d'un code de conduite approuvé comme le prévoit l'article 40 [...] peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article [c'est-à-dire les exigences en matière de sécurité].* »

<sup>65</sup> Art. 24 par. 3 RGPD : « *L'application d'un code de conduite approuvé comme le prévoit l'article 40 [...] peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.* »

est l'un des sujets phares de tout processus de digitalisation d'entreprise ou d'administration publique. La prestation *IaaS* s'analysant en une externalisation de l'infrastructure informatique et constituant le fondement de la myriade d'applications *SaaS* qui déferlent sur le marché, ce document constitue un outil non négligeable pour les utilisateurs de ces solutions. Souvent confrontés à des questions délicates lors du déploiement de projets *cloud*, ils peuvent trouver dans ce document à la nature normative singulière, combinant le caractère volontaire de son adhésion et le caractère obligatoire de son application pour les adhérents, de multiples arguments et critères pour décider des mesures contractuelles, techniques et organisationnelles à mettre en œuvre pour assurer la protection des données personnelles amenées à transiter par le *cloud*. À bien des égards, le Code CISPE implique que ces adhérents fournissent des garanties supplémentaires à celles prévues par le RGPD, du fait de l'interprétation extensive de ses concepts, comme illustré par l'engagement des adhérents au CISPE à refuser toute demande d'un pays tiers à l'Union européenne « *si le jugement ou la décision correspondante [ne peut pas] être reconnu ou exécuté sur la base d'un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, afin de garantir la légalité de ce transfert ou de cette divulgation* »<sup>66</sup>. Plus généralement, le Code permet au client de CISP, en sa qualité de responsable du traitement, de faciliter la preuve de sa propre conformité au RGPD en excipant tant de l'approbation du Code CISPE par la CNIL que des mesures importantes de suivi et d'audit de ses adhérents par des organismes habilités indépendants. Cette expérience normative européenne inédite doit donc contribuer, sur le plan théorique, à nourrir la réflexion sur la force juridique de ces instruments d'un genre nouveau, notamment dans le contexte futur de la nLPD et, sur le plan pratique, à équiper les clients de solutions d'infrastructures *cloud* avec une boîte à outils riche et innovante.

## VI. Bibliographie

### A. Doctrine

**Brunessen BERTRAND**, La souveraineté technologique européenne, *RTD Eur.* 2021, p. 139 ; **Régis BISMUTH**, *Every Cloud Has a Silver Lining. Une analyse contextualisée de l'extraterritorialité du Cloud Act*, JCP E 2018, n° 80 ; **Monique COSSALI SAUVAIN/Camille DUBOIS**, Les codes de conduite dans le projet de révision de la loi fédérale sur la protection des données, *in : LeGes* 29 (2018) 3 ; **Thibault DOUVILLE**, Droit des données à caractère personnel, Gualino, 2021 ; **Marie-Anne FRISON-ROCHE**, Tracer les cercles du Droit de la Compliance, 2017 (cité : FRISON-ROCHE, Tracer les cercles du Droit de la Compliance) ;

---

<sup>66</sup> Code CISPE, 4.4, p. 22.

**Marie-Anne FRISON-ROCHE**, Régulation, Supervision, Compliance, Paris, Dunod, 2017 (cité : FRISON-ROCHE, Régulation, Supervision, Compliance) ; **Patrick JACOB**, La compétence des États à l'égard des données numériques : du nuage au brouillard... en attendant l'éclaircie ?, RCDIP 2019, p. 665 ; **Hans KELSEN**, Théorie pure du droit, 2<sup>e</sup> éd., 1960, trad. Eisenmann, Dalloz, 1962 ; **Christopher KUNER/Lee A BYGRAVE/Christopher DOCKSEY**, *The EU General Data Protection Regulation (GDPR) : A commentary*, Oxford 2019 ; **Marion LAROUER**, Les codes de conduite, sources du droit, Dalloz, coll. Nouvelle Bibliothèque de Thèses, Dalloz, 2018 ; **Sylvain MÉTILLE**, Le traitement de données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données du 25 septembre 2020, SJ 2021 II 1 ; **Sylvain MÉTILLE/Annelise ACKERMANN**, RGPD : application territoriale et extraterritoriale, in : Astrid EPINEY/Sophia ROVELLI (éds), *Datenschutzgrundverordnung (DSGVO) : Tragweite und erste Erfahrungen /Le règlement général sur la protection des données (RGPD) : portée et premières expériences*, Schulthess, 2020 ; **Jean-Baptiste RACINE**, La valeur juridique des codes de conduite privés dans le domaine de l'environnement, Revue juridique de l'Environnement, 1996, pp. 409-424 ; **David ROSENTHAL/Samira STUDER (Alexandre LOMBARD pour la traduction)**, La nouvelle loi sur la protection des données, in : *Jusletter* 16 novembre 2020 ; **Martina SCHWARZ**, *Der US-CLOUD Act*, EF 4/20, S. 193.

## B. Textes officiels

**CEPD**, Lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du règlement 2016/679, adoptées par le comité européen de la protection des données le 4 juin 2019 ; **CEPD**, Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, version 2.0 ; **CEPD**, Avis 17/2021 sur le projet de décision de l'autorité de contrôle française concernant le code de conduite européen soumis par les prestataires de services d'infrastructure en nuage (CISPE), 29 mai 2021 ; **CISPE**, Code de Conduite des Fournisseurs d'Infrastructures Cloud relatif à la Protection des Données, 9 février 2021 ; **Conseil fédéral**, Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017 (cité : Message LPD 2017), FF 2017 p. 6654 ; **PFDP**, Nouvelle loi fédérale sur la protection des données : le point de vue du PFPDT, 9 février 2021.

---

# Le dossier électronique du patient : révolution ou désillusion ?

FRÉDÉRIC ERARD

Dr iur., avocat, CIPP/E, Reponsable du département légal et du transfert de technologie au SIB Institut Suisse de Bioinformatique

## Table des matières

<b>I. Introduction .....</b>	<b>219</b>
<b>II. Caractéristiques et fonctionnement du DEP .....</b>	<b>221</b>
A. Système secondaire et décentralisé .....	221
B. Communautés.....	222
C. Caractère facultatif.....	223
1. Pour les patients.....	223
2. Pour les professionnels de la santé.....	225
D. Données saisies dans le DEP .....	225
1. Par les professionnels de la santé.....	225
2. Par le patient.....	227
E. Gestion du DEP et des droits d'accès .....	228
1. Droits d'accès .....	228
2. Suppression des données et suppression du DEP.....	230
<b>III. Questions choisies.....</b>	<b>231</b>
A. Secret professionnel .....	231
B. Partage des compétences entre Confédération et cantons.....	233
C. Statut des communautés sous l'angle de la protection des données	235
D. Utilisation secondaire des données à des fins de recherche.....	238
<b>IV. Conclusion.....</b>	<b>240</b>
<b>V. Bibliographie .....</b>	<b>241</b>
A. Littérature.....	241
B. Documents officiels .....	242

## I. Introduction

Le dossier électronique du patient (DEP) est un instrument nouveau qui permet à un patient et aux professionnels de la santé qu'il aurait autorisés à accéder en tout temps et à distance à certaines informations issues de son dossier

médical. Le DEP est construit sur un système qui implique notamment la décentralisation d'une partie de l'infrastructure de gestion du DEP ainsi qu'une externalisation éventuelle du stockage de certaines données de santé des patients. Le DEP présente ainsi certaines caractéristiques liées aux technologies de type *cloud*.

Le DEP a été conçu dans un contexte où les nouvelles technologies de l'information et de la communication ont un impact croissant sur le secteur des soins. Or, ce secteur fait lui-même l'objet d'évolutions rapides puisqu'il doit répondre à de nombreux défis actuels, à l'image des nouveaux besoins créés par une population toujours plus âgée (augmentation des maladies chroniques), de l'augmentation du nombre de fournisseurs de soins (spécialisation des professions), du mouvement d'*empowerment* des patients ou encore des pressions croissantes sur les coûts de la santé.

Dans ce contexte pour le moins mouvant, le Conseil fédéral a fait de la transformation technologique et numérique le premier des quatre objectifs de sa politique de santé pour la période 2020-2030<sup>1</sup>. Cela requiert non seulement des fournisseurs de soins qu'ils puissent bénéficier d'infrastructures coordonnées, mais aussi que les patients voient leurs compétences renforcées du fait d'un meilleur accès à leurs données de santé et à l'information médicale.

La coordination des efforts en matière de santé numérique n'est pas complètement nouvelle en Suisse. La première Stratégie Cybersanté Suisse a été adoptée par le Conseil fédéral et les cantons en 2007 avec l'objectif de permettre à tout individu d'autoriser les soignants de son choix à accéder « *à tout moment et en tout lieu* » à des informations sur sa personne, ainsi qu'à assurer la mise en réseau des acteurs du système de santé grâce aux technologies de l'information et de la communication<sup>2</sup>. L'adoption en 2015 de la LDEP<sup>3</sup> – une loi dont l'objectif ne consiste pas à régler l'ensemble des détails du DEP, mais plutôt ses conditions-cadre – constitue un des jalons majeurs de cette stratégie. En 2018, la Stratégie Cybersanté Suisse a été remplacée par une nouvelle Stratégie Cybersanté Suisse 2.0 adoptée en mars 2018, dont le but principal est d'accompagner la diffusion du dossier électronique du patient (DEP)<sup>4</sup> et qui arrivera à échéance au cours de l'année 2022.

En dépit du fait que la LDEP a été adoptée en 2015, le déploiement du DEP a subi des retards non négligeables. Le premier DEP n'a été ouvert qu'en décembre 2020 et le nombre de DEP ouverts reste relativement faible à l'heure où ces lignes sont écrites. Les retards s'expliquent certes par des délais de mise en

---

<sup>1</sup> Conseil fédéral, Stratégie 2030, p. 12 ss.

<sup>2</sup> Office fédéral de la santé publique, Stratégie Cybersanté (eHealth) Suisse, 27 juin 2007, p. 3.

<sup>3</sup> Loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP), RS 816.1.

<sup>4</sup> Confédération suisse/CDS, Stratégie Cybersanté Suisse 2.0, 14 décembre 2018, p. 3.



œuvre différés prévus par le législateur, mais aussi par des difficultés liées aux certifications des communautés du DEP et plus généralement par des incertitudes en lien avec le partage des compétences entre Confédération et cantons. Face à des débuts plutôt modestes, voire décevants, le Conseil fédéral a annoncé par un communiqué de presse du 27 avril 2022 son intention de lancer une révision complète de la LDEP. Cette révision, dont les éléments clés ont été succinctement énumérés par le Conseil fédéral, a pour objectif annoncé de garantir le succès de l'introduction et de la diffusion du DEP<sup>5</sup>.

La présente contribution offre une présentation générale et non exhaustive des principales règles juridiques applicables au DEP, puis aborde brièvement plusieurs thématiques sélectionnées pour leur pertinence juridique ou pratique.

## **II. Caractéristiques et fonctionnement du DEP**

### **A. Système secondaire et décentralisé**

L'art. 2 let. a LDEP définit le DEP comme un « *dossier virtuel permettant de rendre accessibles en ligne, en cas de traitement concret, des données pertinentes pour ce traitement qui sont tirées du dossier médical d'un patient et enregistrées de manière décentralisée ou des données saisies par le patient lui-même* ».

Le DEP ne doit pas être confondu avec le dossier médical classique ou ordinaire tenu par un professionnel de la santé ou une institution, qui peut d'ailleurs être informatisé ou non (système primaire). Ce dernier n'est aucunement affecté par la mise en œuvre du DEP et sa tenue continue d'être réglée par les règles ordinaires applicables aux professionnels de la santé en matière de documentation<sup>6</sup>. Pour sa part, le DEP constitue un « *second* » dossier médical (système secondaire), virtuel, qui contient seulement des liens vers les lieux d'hébergement de certaines informations tirées du ou des dossier(s) primaire(s). Le patient a également la possibilité d'enregistrer lui-même des informations dans son DEP. En tant que système secondaire, le DEP ne remplace donc pas le dossier médical ordinaire<sup>7</sup>.

---

<sup>5</sup> Conseil fédéral, Le Conseil fédéral veut développer davantage le dossier électronique du patient, communiqué de presse du 27 avril 2022. Pour un commentaire de l'annonce du Conseil fédéral : ERARD, Conseil fédéral.

<sup>6</sup> P. ex. art. 87 Loi cantonale vaudoise du 29 mai 1985 sur la santé publique, BLV 800.01. Au sujet des exigences posées par les différentes lois et jurisprudences relatives au contenu du dossier médical : DONZALLAZ, N 5974 ss ; FELLMANN/ODERMATT, N 13 ss.

<sup>7</sup> DONZALLAZ, N 5930.

Conformément à la définition de l'art. 2 let. a LDEP, le DEP repose de surcroît sur une architecture décentralisée, qui a notamment pour conséquence que les données médicales déposées dans les DEP ne sont pas réunies, puis hébergées auprès d'un acteur central qui aurait pour tâche de les rendre accessibles. Outre qu'il est typiquement helvétique, le choix du législateur de faire reposer l'ensemble du DEP sur un système décentralisé a notamment été opéré pour mieux surmonter les difficultés liées aux partages de compétences délicats entre Confédération et cantons en matière de protection des données et de santé ou encore pour éviter de construire un système trop rigide dont l'échec menacerait le DEP dans son ensemble<sup>8</sup>.

## B. Communautés

Le fonctionnement du DEP repose dans une bonne mesure sur les « communautés », que l'art. 2 let. d LDEP définit laconiquement comme des unités organisationnelles de professionnels de la santé et de leurs institutions. Le LDEP distingue deux types de communautés. Les communautés dites « simples » doivent au moins s'assurer que les données inscrites dans le DEP sont accessibles par le biais du DEP et consigner dans un historique chaque traitement de données<sup>9</sup>. Cela signifie que les communautés doivent entre autres tenir un registre de documents constitué des liens (métadonnées) vers l'ensemble des lieux de stockage des documents mis à disposition du DEP par les membres affiliés à cette communauté<sup>10</sup>. Les communautés dites « de référence » assument les mêmes tâches que les communautés simples, mais doivent en plus gérer les consentements des patients liés à l'ouverture d'un DEP et assurer que les patients puissent exercer leurs droits en lien avec le DEP (p. ex. gérer les accès ou accéder à leurs propres données)<sup>11</sup>. Chaque patient, professionnel de la santé ou institution utilisant le DEP doit s'affilier auprès d'une communauté (pour les patients, nécessairement une communauté de référence)<sup>12</sup>. Les art. 9 à 12 ODEP<sup>13</sup> définissent plus précisément les tâches des communautés, notamment en matière de tenue et transfert de données.

Le législateur a volontairement laissé une marge de manœuvre importante pour la forme des communautés : si elles doivent nécessairement disposer de la personnalité juridique, leur forme juridique reste quant à elle libre<sup>14</sup>. Sept communautés

---

<sup>8</sup> Message LDEP 2013, FF 2013 4747, p. 4757 s.

<sup>9</sup> Art. 10 al. 1 LDEP.

<sup>10</sup> Message LDEP 2013, FF 2013 4747, p. 4763 ; SPRECHER/HOFER, p. 53.

<sup>11</sup> Art. 10 al. 2 LDEP.

<sup>12</sup> SPRECHER/HOFER, p. 55.

<sup>13</sup> Ordonnance du 27 mars 2017 sur le dossier électronique du patient (ODEP), RS 816.11.

<sup>14</sup> WIDMER, Das elektronische Patientendossier, p. 769 ; SPRECHER/HOFER, p. 55.

de références ont été certifiées à l'heure où ces lignes sont écrites. En Suisse romande, les cantons de Fribourg, Genève, Jura, Valais et Vaud ont créé une association intercantonale en vue d'établir la communauté de référence (CARA)<sup>15</sup>. Le canton de Neuchâtel fait quant à lui cavalier seul avec la communauté de référence du Dossier Électronique du Patient Neuchâtel.

La LDEP n'établit pas directement le lieu d'hébergement des données versées dans le DEP, de telle sorte que les professionnels de la santé et les institutions disposent théoriquement d'une certaine marge de manœuvre en la matière<sup>16</sup>. À la lumière de la loi, rien n'empêche en effet un cabinet médical d'exploiter lui-même un système secondaire (*cf. supra* II.A.) pour mettre les données du DEP à disposition des autres professionnels de la santé. Dans les faits, les exigences strictes posées par la loi en matière de sécurité des données ainsi que la nécessité d'assurer la disponibilité des données en tout temps va conduire les professionnels de la santé ou les petites entités (p. ex. cabinets médicaux, pharmacies) à choisir de faire héberger les données du DEP auprès des communautés, des communautés de référence ou de prestataires privés en raison des coûts induits<sup>17</sup>.

## **C. Caractère facultatif**

### *1. Pour les patients*

L'ouverture d'un DEP requiert le consentement du patient et est donc purement facultative<sup>18</sup>. Au cours de la procédure d'ouverture d'un DEP, la communauté de référence doit informer le patient sur le but du DEP, le traitement des données, les conséquences du consentement et l'attribution des droits d'accès à son DEP<sup>19</sup>.

---

<sup>15</sup> Les cantons « CARA » ont par ailleurs initié des travaux préparatoires pour l'adoption d'une convention intercantonale en matière de santé numérique (le texte de l'avant-projet est consultable ici : <<https://www.fr.ch/dsas/ssp/actualites/convention-intercantonale-en-matiere-de-sante-numerique-0>> (*consulté le 7 mai 2022*). L'avant-projet prévoit notamment que les cantons contractants créent en commun une organisation dont le but est la gestion d'une communauté de référence (art. 9 al. 1). Il prévoit également que les prestataires de soins établis sur leur territoire et qui sont au bénéfice d'une inscription dans la planification cantonale au sens de la LAMal ou au bénéfice d'un mandat de prestations de la part des cantons contractants sont tenus de s'affilier à la communauté de référence commune (art. 9 al. 4).

<sup>16</sup> WIDMER, Das elektronische Patientendossier, p. 770.

<sup>17</sup> WIDMER, Das elektronische Patientendossier, p. 769 ; SPRECHER/HOFER, p. 59 ; ERARD, Le secret médical, N 169.

<sup>18</sup> Art. 3 al. 1 LDEP.

<sup>19</sup> Art. 3 al. 1 LDEP, art. 15 ODEP.

L'ouverture, la gestion et la révocation du DEP relèvent des droits strictement personnels au sens de l'art. 19c CC. Ces actes peuvent ainsi être valablement opérés par un mineur agissant seul à la condition qu'il soit capable de discernement<sup>20</sup>. Dans la mesure où les actes liés au DEP relèvent de droits strictement personnels sujets à représentation, ils peuvent également être valablement effectués par un représentant. La représentation peut être volontaire (art. 32 ss CO) et une simple procuration suffit alors pour désigner une ou plusieurs personnes chargées de l'ouverture, de la gestion ou de la fermeture du DEP<sup>21</sup>. La représentation volontaire peut également trouver sa source dans des directives anticipées (dans la mesure nécessaire pour déterminer les soins médicaux à administrer ; art. 370 ss CC) ou un mandat pour cause d'incapacité (art. 360 ss CC) et prend alors effet lorsque les conditions légales sont réunies (p. ex. incapacité de discernement pour les directives anticipées)<sup>22</sup>. Quant aux personnes incapables de discernement qui n'auraient pas pris de mesures préalables pour se faire représenter, elles peuvent bénéficier de plusieurs types de représentation légale. Les adultes incapables de discernement peuvent être représentés par un curateur qui s'est vu confier le pouvoir de représenter la personne dans le domaine médical (curatelle de représentation portant sur les affaires médicales ou curatelle de portée générale). Contrairement à ce qu'indiquent les directives de *eHealth Suisse*<sup>23</sup>, l'art. 378 CC qui prévoit la représentation d'une personne incapable de discernement par les proches parents dans le domaine médical semble quant à lui constituer une base légale limitée pour la gestion du DEP. Cette disposition se contente en effet d'octroyer un pouvoir de représentation limité au consentement à des soins médicaux et seules les actions dans le DEP liées à l'acte médical concerné pourraient donc faire l'objet d'une représentation<sup>24</sup>. L'art. 378 CC ne permet donc pas à un proche de fermer un DEP par exemple. Enfin, les mineurs incapables de discernement peuvent se voir ouvrir un DEP si leurs représentants légaux (généralement les parents) en décident ainsi, de telle sorte qu'un DEP peut être ouvert pour un enfant dès sa naissance.

Le caractère strictement facultatif du DEP pour les patients fera toutefois bientôt l'objet de débats. Dans son annonce de projet de révision totale de la LDEP, le Conseil fédéral a en effet affiché sa volonté de mettre en consultation une variante dans laquelle le libre choix du patient serait remplacé par un système d'*opt-out*. En d'autres termes, la modification mise en consultation devrait

---

<sup>20</sup> eHealth Suisse, Représentation dans le cadre du DEP, p. 11.

<sup>21</sup> Conformément à l'art. 35 al. 1 CO, ce type de représentation cesse cependant de produire des effets lorsque la personne représentée devient incapable de discernement, sauf si la procuration mentionne explicitement ce cas de figure.

<sup>22</sup> eHealth Suisse, Représentation dans le cadre du DEP, p. 22 s.

<sup>23</sup> eHealth Suisse, Représentation dans le cadre du DEP, p. 24 s.

<sup>24</sup> Pour une analyse détaillée de cette question, cf. MEIER.

prévoir l'ouverture automatique d'un DEP pour chaque patient, à moins que ce dernier n'en décide autrement<sup>25</sup>.

## 2. *Pour les professionnels de la santé*

Afin d'atteindre un plafond d'adoption suffisant, la LDEP a d'emblée obligé les fournisseurs de prestations au sens des art. 39 et 49a al. 4 LAMal (soit les hôpitaux, maisons de naissance et EMS) à proposer le DEP tout en leur octroyant des délais transitoires et différenciés de mise en œuvre selon le type d'établissements<sup>26</sup>.

Le libre choix des autres professionnels de la santé d'offrir ou non le DEP s'est toutefois rapidement amenuisé avec l'entrée en vigueur, le 1<sup>er</sup> janvier 2022, d'un nouvel art. 37 al. 3 LAMal obligeant les médecins qui obtiennent leur admission à pratiquer à charge de l'assurance obligatoire des soins à partir de cette date à s'affilier à une communauté ou une communauté de référence.

Dans son annonce de révision totale de la LDEP, le Conseil fédéral a affiché sa volonté de continuer sur la lancée puisqu'un des éléments clés de la révision vise à étendre l'obligation d'affiliation à l'ensemble des professionnels de la santé exerçant dans le domaine ambulatoire, y compris ceux qui auraient obtenu une autorisation de pratiquer à charge de l'assurance obligatoire de soins avant le 1<sup>er</sup> janvier 2022. Dans cette hypothèse, le libre choix de s'affilier ou non à une communauté ne s'étendrait plus qu'aux rares professionnels qui n'exercent ni dans un hôpital, un EMS ou une maison de naissance ni à charge de l'assurance obligatoire de soins.

## D. **Données saisies dans le DEP**

### 1. *Par les professionnels de la santé*

Comme cela a été mentionné (*cf. supra* II.A.), le DEP ne constitue pas une copie parfaite du dossier médical primaire, mais contient seulement certaines informations tirées de celui-ci. Conformément à la définition légale du DEP, les professionnels de la santé doivent ainsi y saisir les données pertinentes pour le traitement<sup>27</sup>. Or, sans autre forme de précision légale, la

---

<sup>25</sup> Conseil fédéral, Le Conseil fédéral veut développer davantage le dossier électronique du patient, communiqué de presse du 27 avril 2022.

<sup>26</sup> Pour une analyse des situations où une institution médico-hospitalière faillit à respecter son obligation d'affiliation sous l'angle de la LAMal, *cf.* STÖCKLI.

<sup>27</sup> Art. 2 let. a LDEP.

détermination de ce qui constitue ou non une donnée pertinente pour le traitement fait l'objet d'une marge d'interprétation importante. Dans son message relatif à la LDEP, le Conseil fédéral s'est contenté d'affirmer qu'il s'agissait d'informations importantes pour que d'autres professionnels de la santé puissent poursuivre le traitement<sup>28</sup>. Pour parer aux incertitudes soulevées, *eHealth Suisse* a publié des lignes directrices spécifiquement dédiées à la notion d'informations pertinentes pour le traitement. Selon la définition retenue, les documents sont pertinents pour le traitement « *lorsqu'ils contiennent des informations qui, au moment de la prise en charge du patient, sont valables et décisives pour définir un traitement. Il s'agit tout particulièrement d'informations qui contribuent à accroître l'efficacité de différents processus dans le système de santé et qui, lorsqu'elles sont disponibles, facilitent ces processus (p. ex. liste complète des diagnostics, anamnèse familiale)* »<sup>29</sup>. Les lignes directrices contiennent également un schéma d'aide à la décision pour établir si des informations sont pertinentes ou non pour le traitement<sup>30</sup>. De manière plus générale, la mise à disposition des données dans le DEP doit se faire en conformité avec le principe général de proportionnalité, c'est-à-dire que seules les informations qui sont nécessaires, pertinentes et non excessives pour la poursuite du traitement devraient être saisies dans le DEP<sup>31</sup>. En fin de compte, la décision de déterminer ce qui constitue ou non une donnée pertinente pour le traitement repose sur les épaules des professionnels de la santé<sup>32</sup>, même si les établissements médicaux devraient adopter des directives institutionnelles à cet égard<sup>33</sup>.

L'art. 3 al. 2 LDEP institue une présomption légale selon laquelle le patient ouvre un DEP consent à ce que les professionnels de la santé y saisissent des données en cas de traitement médical. Le patient n'est donc pas tenu de donner son consentement pour l'inscription de chaque nouvelle donnée dans son DEP<sup>34</sup>. Lors des débats d'adoption de la LDEP, le législateur a tenu à compléter l'art. 3 al. 2 LDEP en précisant que cette présomption s'appliquait également aux professionnels de la santé travaillant pour des institutions de droit public ou pour des institutions qui assument une tâche publique qui leur a été confiée par un canton ou une commune. Cet ajout visait à assurer que la saisie de nouvelles données dans le DEP ne serait pas contrecarrée par des impératifs liés au partage de compétences entre Confédération et cantons, les traitements de données effectués par les organes publics cantonaux (de surcroît dans le domaine de la santé) étant par principe soumis au droit cantonal de la protection des

---

<sup>28</sup> Message LDEP 2013, p. 4797.

<sup>29</sup> *eHealth Suisse, Informations pertinentes*, p. 7.

<sup>30</sup> *eHealth Suisse, Informations pertinentes*, p. 10.

<sup>31</sup> DONZALLAZ, N 6531 ss.

<sup>32</sup> FELLMANN/ODERMATT, N 10.

<sup>33</sup> FELLMANN/ODERMATT, N 11.

<sup>34</sup> Message LDEP 2013, p. 4800 ; WIDMER, *ePatientdossier*, p. 162.

données. Alors même que cette disposition de droit fédéral empiète sur les compétences fédérales, l'Assemblée fédérale a jugé qu'il était bon de l'adopter par souci de « *simplification* »<sup>35</sup>.

Le droit octroyé aux professionnels de la santé d'entrer des informations dans le DEP de leurs patients ne doit pas être confondu avec le droit d'accéder aux données du DEP. L'accès aux informations contenues dans un DEP repose en effet sur les droits d'accès octroyés par le patient (*cf. infra* E.1.).

Si la LDEP présume que le patient accepte que les professionnels de la santé puissent saisir des données dans le DEP, elle n'indique rien sur une éventuelle obligation de le faire. Sur ce point, un avis de droit demandé par la FMH arrive à la conclusion qu'une telle obligation ne peut en effet pas être déduite directement de la LDEP<sup>36</sup>. Que le professionnel de la santé soit légalement tenu ou non de s'affilier à une communauté (p. ex. un médecin qui obtient son autorisation de pratiquer à charge de l'assurance obligatoire des soins après le 1<sup>er</sup> janvier 2022) ne change rien à cette conclusion. Néanmoins, une telle obligation de saisie peut être imposée aux professionnels de la santé qui sont affiliés à une communauté sur la base de leur obligation contractuelle ou légale de documentation<sup>37</sup>. En d'autres termes, un patient qui possède un DEP peut s'attendre à ce que son médecin y saisisse des informations. Le médecin qui s'abstient complètement d'y saisir des données alors qu'il en a la possibilité pourrait, selon les circonstances, faillir à son devoir de diligence<sup>38</sup>.

## 2. Par le patient

Le patient peut quant à lui saisir lui-même des données dans son DEP, à l'instar de directives anticipées ou d'un consentement au don d'organe<sup>39</sup>. Il peut par exemple numériser des documents puis les verser dans son DEP (comme on le ferait avec un outil d'hébergement de données *cloud* de type *Dropbox*). L'organe *eHealth Suisse* mène cependant des travaux pour déterminer dans quelles conditions le DEP pourrait être directement et automatiquement

---

<sup>35</sup> V. en particulier l'intervention du rapporteur de la Commission du Conseil national Ignazio Cassis, BO (CN) 2015, p. 437.

<sup>36</sup> SCHINDLER/TSCHUMI, N 24.

<sup>37</sup> SCHINDLER/TSCHUMI, N 25.

<sup>38</sup> FELLMANN/ODERMATT, N 23 ss. Selon les mêmes auteurs, un professionnel de la santé est aussi susceptible d'engager sa responsabilité civile s'il saisit des données erronées dans le DEP et qu'un dommage est causé par un autre professionnel de la santé qui s'appuie sur les données erronées. Sur la question de la responsabilité en lien avec le DEP, voir aussi : SCHINDLER/TSCHUMI, N 40 ss ; *eHealth Suisse*, Responsabilité.

<sup>39</sup> Art. 2 let. a LDEP.

alimenté par des applications mobiles de santé (*mHealth*)<sup>40</sup>. Un avis de droit rendu dans ce cadre a souligné la nécessité d'assurer le respect d'exigences minimales de protection et de sécurité des données, ainsi que de recueillir le consentement général du patient pour fonder un transfert automatique de données de l'application mobile vers le DEP<sup>41</sup>. En l'état, un tel transfert automatique de données semble néanmoins contraire à la LDEP, notamment parce que toute forme d'accès au DEP nécessite une procédure de double authentification<sup>42</sup>.

## E. Gestion du DEP et des droits d'accès

### 1. Droits d'accès

Toute personne qui accède à un DEP doit nécessairement bénéficier d'une identité électronique sécurisée<sup>43</sup>. Or, seuls les patients et les professionnels de la santé peuvent obtenir une identité électronique sécurisée au sens de la LDEP, de telle sorte que l'accès au DEP est par effet réflexe limité à ces deux seules catégories de personnes. Notons au passage que la LDEP est la première loi qui définit le « *professionnel de la santé* » à l'échelon fédéral, soit en l'occurrence tout « *professionnel du domaine de la santé reconnu par le droit fédéral ou cantonal qui applique ou prescrit des traitements médicaux ou qui remet des produits thérapeutiques ou d'autres produits dans le cadre d'un traitement médical* »<sup>44</sup>. Cette définition exclut les gestionnaires de cas des assurances, les médecins-conseils ou les experts assurance-invalidité, qui ne peuvent donc en aucun cas accéder au DEP d'un patient<sup>45</sup>.

Du point de vue du patient, le principe est simple : celui-ci peut accéder sans restriction et en tout temps aux données médicales saisies dans son DEP<sup>46</sup>. Le débiteur du droit du patient d'accéder aux données de son DEP est la communauté de référence à laquelle le patient est affilié<sup>47</sup>. Le droit d'accès direct du patient à ses informations médicales est en phase avec l'art. 25 al. 3 de la LPD

---

<sup>40</sup> Pour une vue générale des travaux menés : <[www.e-health-suisse.ch/fr/mise-en-oeuvre-communautes/activites-ehealth/mhealth.html](http://www.e-health-suisse.ch/fr/mise-en-oeuvre-communautes/activites-ehealth/mhealth.html)> (consulté le 7 mai 2022).

<sup>41</sup> ISLER, N 143.

<sup>42</sup> Art. 23 let. c ODEP.

<sup>43</sup> Art. 7 al. 1 LDEP.

<sup>44</sup> Art. 2 let. b LDEP. Au sujet de la notion de professionnel de la santé au sens de la LDEP : ERARD, Secret médical, N 144 ss ; DONZALLAZ, N 6534 ss.

<sup>45</sup> DONZALLAZ, N 6540.

<sup>46</sup> Art. 8 al. 1 LDEP.

<sup>47</sup> Art. 10 al. 2 let. B ch. 2 LDEP.



révisée (nLPD)<sup>48</sup> qui prévoit que des données sur la santé d'une personne peuvent lui être communiquées par l'intermédiaire d'un professionnel de la santé, à condition toutefois que la personne concernée y consente. À l'inverse, dans le régime qui prévaut jusqu'à l'entrée en vigueur de la LPD révisée, l'art. 8 al. 3 LPD<sup>49</sup> énonce que le maître du fichier est en droit de décider unilatéralement de communiquer des données sur la santé d'une personne par l'intermédiaire d'un médecin s'il l'estime nécessaire. Cette disposition, dont le but est de protéger le patient contre une prise de connaissance d'informations qui pourrait lui être néfaste relève d'un paternalisme aujourd'hui dépassé. Dans le contexte du DEP, l'éthique médicale – en particulier le respect des principes de bienfaisance ou de non-malfaisance – conduiront néanmoins les professionnels de la santé à prendre les précautions nécessaires pour délivrer l'information au patient dans les meilleures conditions possibles et conformément aux règles de l'art. Ainsi, lorsqu'un professionnel de la santé est amené à annoncer un diagnostic grave à un patient par exemple, il devrait en principe veiller à ce que les informations concernées soient « poussées » dans le DEP après l'annonce au patient, de telle sorte à éviter que le patient ne découvre lui-même l'information brute sans autre forme d'explication.

De son côté, le professionnel de la santé peut uniquement accéder aux données d'un DEP s'il y a été autorisé par le patient<sup>50</sup>, lequel ne peut en aucun cas être contraint de rendre ses données accessibles<sup>51</sup>. Le patient peut décider d'octroyer un droit d'accès à un professionnel de la santé en particulier ou, pour des considérations d'ordre pratique, à un groupe de professionnels de la santé<sup>52</sup>. La loi ne définit pas ce qu'il faut entendre par groupes de professionnels de la santé. Il peut s'agir des professionnels d'un même établissement médical, d'un département d'hôpital ou d'un groupe d'experts interdisciplinaires par exemple<sup>53</sup>. Le droit d'accès octroyé à un professionnel de la santé en particulier (qui ne doit pas être confondu avec le droit d'accès des personnes concernées à accéder à leurs propres données, au sens de la LPD) continue de déployer ses effets jusqu'à sa révocation. La durée du droit d'accès donné à un groupe de professionnels de la santé doit quant à elle être définie à l'avance par le patient<sup>54</sup>. Ce dernier peut toutefois prolonger la durée d'accès s'il le souhaite.

Les auxiliaires n'ont pas besoin d'être spécifiquement autorisés par le patient et peuvent accéder au DEP dans la même mesure que le professionnel de la

---

<sup>48</sup> Loi fédérale sur la protection des données du 25 septembre 2020, FF 2020, p. 7397, dont l'entrée en vigueur est annoncée pour septembre 2023.

<sup>49</sup> Loi fédérale sur la protection des données du 19 juin 1992 (LPD), RS 235.1.

<sup>50</sup> Art. 9 al. 1 LDEP.

<sup>51</sup> Art. 3 al. 4 LDEP.

<sup>52</sup> Art. 2 al. 1 ODEP.

<sup>53</sup> ERARD, Secret médical, N 175.

<sup>54</sup> Art. 3 ODEP.

santé pour le compte duquel ils exercent leur activité. Ils doivent cependant s'affilier à une communauté et s'identifier avec leur propre identité électronique, de telle sorte que tout accès au DEP par un auxiliaire est journalisé sous son propre nom<sup>55</sup>.

Le patient peut attribuer différents niveaux de confidentialité aux documents de son DEP (normal, restreint ou secret)<sup>56</sup>. Par défaut, les données saisies dans le DEP ont un niveau de confidentialité « normal », sauf si le soignant en décide autrement<sup>57</sup>. Seuls les professionnels de la santé qui ont reçu un droit d'accès « étendu » peuvent consulter les données classées par le patient avec un niveau « restreint »<sup>58</sup>. Les données auxquelles le patient attribue un niveau de confidentialité « secret » sont uniquement accessibles par le patient<sup>59</sup>.

En cas d'urgence, les professionnels de la santé peuvent accéder aux données du DEP de niveau « normal », même sans autorisation du patient<sup>60</sup>. Le patient a néanmoins la possibilité d'interdire tout accès en cas d'urgence ou, au contraire, d'étendre les possibilités d'accès aux données de niveau « restreint » dans de telles circonstances<sup>61</sup>. Le patient doit en être informé dans un délai approprié après un accès en cas d'urgence par un professionnel de la santé<sup>62</sup>.

Lorsqu'un professionnel de la santé bénéficie d'un droit d'accès à un DEP, il peut non seulement consulter les documents, mais aussi les télécharger sur son système primaire<sup>63</sup>. Les documents concernés sortent alors du champ de contrôle des règles applicables au DEP<sup>64</sup>.

## 2. *Suppression des données et suppression du DEP*

Les données saisies par le professionnel de la santé dans le DEP sont effacées à l'issue d'un délai de vingt ans, même si le patient peut décider que les données seront conservées pour une plus longue période<sup>65</sup>. Les données enregistrées par le patient lui-même sont quant à elles conservées sans limite

---

<sup>55</sup> § 1.6 Annexe 2 de l'Ordonnance du DFI du 22 mars 2017 sur le dossier électronique du patient (ODEP-DFI), RS 816.111.

<sup>56</sup> Art. 1 al. 1 ODEP.

<sup>57</sup> Pour une opinion selon laquelle le classement par défaut des données en niveau « normal » est contraire au principe de *privacy by default* : WIDMER, ePatientdossier, p. 166.

<sup>58</sup> Office fédéral de la santé publique, Rapport explicatif ODEP, p. 10.

<sup>59</sup> Office fédéral de la santé publique, Rapport explicatif ODEP, p. 10.

<sup>60</sup> Art. 9 al. 5 LDEP ; art. 2 al. 2 ODEP.

<sup>61</sup> Art. 4 let. e ODEP.

<sup>62</sup> Art. 9 al. 5 LDEP ; art. 2 al. 2 ODEP.

<sup>63</sup> WIDMER, Das elektronische Patientendossier, p. 772.

<sup>64</sup> ERARD, Secret médical, N 183.

<sup>65</sup> Art. 10 al. 1 let. d ODEP.

de temps. Dans tous les cas, le patient peut décider de supprimer tout ou partie des données enregistrées dans son DEP, sans égard au fait que les données ont été saisies par lui-même ou par un professionnel de la santé.

Le patient peut choisir de révoquer en tout temps son consentement à la constitution d'un DEP<sup>66</sup>. La révocation n'est soumise à aucune forme et n'a pas à être motivée<sup>67</sup>. Dans ce cas, le DEP doit être détruit et la situation qui prévalait avant le DEP doit être rétablie. La destruction du DEP n'a toutefois pas d'impact sur les documents enregistrés dans les systèmes primaires (aussi bien pour les documents *uploadés* vers le DEP ou *downloadés* depuis le DEP)<sup>68</sup>. La déclaration de révocation du consentement est gérée par la communauté de référence auprès de laquelle le patient est affilié<sup>69</sup>.

Lorsque le patient décède, la communauté de référence concernée doit supprimer son DEP. La destruction du DEP doit intervenir au plus tôt deux ans après le décès<sup>70</sup>.

### **III. Questions choisies**

La mise en œuvre du DEP est récente et soulève de nombreuses interrogations pratiques, mais aussi juridiques. L'annonce du Conseil fédéral de réviser en profondeur la LDEP, alors que les premiers DEP ont été ouverts il y a peu, renforce de surcroît les incertitudes qui planent sur l'application des règles en vigueur. Les lignes qui suivent traitent, sans intention d'exhaustivité aucune, de quelques problématiques juridiques choisies liées au DEP.

#### **A. Secret professionnel**

La grande majorité des professionnels de la santé qui exercent leur activité en Suisse sont aujourd'hui soumis au secret professionnel imposé par l'art. 321 CP<sup>71</sup>. Cette disposition impose aux professionnels visés ainsi qu'à leurs auxiliaires un devoir personnel de garder le silence sur les secrets qui leur ont été confiés en vertu de leur profession ou dont ils ont eu connaissance dans l'exercice de celle-ci. De prime abord, la mise en œuvre du DEP ne semble pas juridiquement neutre pour le secret professionnel puisqu'elle implique une

---

<sup>66</sup> Art. 3 al. 3 LDEP ; art. 21 al. 1 ODEP.

<sup>67</sup> Message LDEP 2013, FF 2013 4747, p. 4800.

<sup>68</sup> Message LDEP 2013, FF 2013 4747, p. 4800.

<sup>69</sup> Message LDEP 2013, FF 2013 4747, p. 4801.

<sup>70</sup> Art. 21 al. 2 ODEP.

<sup>71</sup> Code pénal suisse du 21 décembre 1937 (CP), RS 311.0.

augmentation sensible des communications ainsi qu'une externalisation potentielle de données couvertes par le secret professionnel.

Dans les faits, la thématique du secret professionnel a été largement écartée des travaux préparatoires de la LDEP, le Conseil fédéral se contentant d'affirmer dans son message que la LDEP n'apporterait aucun changement aux règles relatives au secret professionnel<sup>72</sup>. Il est vrai que le DEP – du moins dans sa forme actuelle – fait reposer toute la justification de l'outil sur le consentement de la personne concernée, que ce soit pour l'ouverture du DEP ou pour la détermination des droits d'accès par exemple<sup>73</sup>.

Il n'en reste pas moins que la préservation du secret professionnel peut être mise à mal par le DEP dans certaines situations. On pense notamment aux DEP ouverts pour des enfants, dont le passage à l'adolescence entraîne en principe l'acquisition de la capacité de discernement permettant de se déterminer seul sur la levée du secret professionnel et, par conséquent, sur la gestion du DEP (droit strictement personnel ; cf. *supra* II.C.1.)<sup>74</sup>. Or, jusqu'à ce point temporel qui diffère pour chacun selon sa capacité de comprendre et de se déterminer sur son DEP, ce sont les représentants légaux (en principe les parents) qui représentent l'enfant et disposent de ce fait des droits d'accès au DEP. Si le maintien de l'accès par les parents peut se justifier durant une période « transitoire », il est nécessaire de prendre les mesures nécessaires pour permettre à l'adolescent de se déterminer activement quant à son souhait de continuer ou non à autoriser ses parents à accéder à son DEP. Cette problématique a été identifiée par *eHealth Suisse*, qui recommande aux communautés de référence d'informer une fois par année tous les enfants de plus de 12 ans quant à leurs droits en matière de DEP<sup>75</sup>.

Sous l'angle du respect du secret professionnel, il conviendra par ailleurs d'être vigilant lors de la révision annoncée de la LDEP. Si l'ouverture du DEP devient automatique en l'absence de volonté contraire du patient (système d'*opt-out*, cf. *supra* II.C.1.), le patient pourrait avoir une conscience moins aiguë de l'existence de son DEP et des données qui y sont saisies sur la base de la présomption légale de l'art. 3 al. 2 LDEP (même si le texte actuel présume que le patient accepte que les professionnels de la santé saisissent des données dans le DEP lorsqu'ils ont donné leur « *consentement* » à l'ouverture de ce dernier, ce qui ne serait plus tout à fait le cas en cas d'*opt-out*). Si la proposition aboutit, le patient devrait néanmoins garder le droit de décider à qui il entend octroyer des droits d'accès.

---

<sup>72</sup> Message LDEP 2013, FF 2013 4747, p. 4796.

<sup>73</sup> WIDMER, ePatientdossier, p. 162.

<sup>74</sup> ERARD, Secret médical, N 875.

<sup>75</sup> eHealth Suisse, Représentation dans le cadre du DEP, p. 17.

## **B. Partage des compétences entre Confédération et cantons**

Comme déjà mentionné, le partage complexe des compétences législatives entre la Confédération et les cantons dans les domaines de la santé et de la protection des données compte parmi les raisons qui ont motivé l'adoption d'un système décentralisé pour le DEP<sup>76</sup>. Sous réserve des règles imposées par la LDEP et ses ordonnances (règles spéciales de droit fédéral), les différents acteurs impliqués dans la mise en œuvre du DEP restent soumis au droit qui leur est applicable en situation normale, qu'il s'agisse des professionnels de la santé, des institutions, des communautés ou de tout autre intervenant. En matière de protection des données, les acteurs du DEP sont ainsi soumis alternativement à la LPD (traitements de données par un organe public fédéral ou une personne privée) ou aux législations cantonales sur la protection des données (traitements de données par un organe public cantonal). De la même manière, la surveillance en matière de protection des données est exercée alternativement par le Préposé fédéral à la protection des données ou par les préposés cantonaux à la protection des données<sup>77</sup>. Comme les communautés doivent également faire l'objet d'une certification<sup>78</sup>, l'organisme de certification accrédité exerce aussi une surveillance sur les critères techniques et organisationnels applicables aux communautés, dont bon nombre sont en rapport direct avec la protection des données personnelles<sup>79</sup>.

En plus du caractère décentralisé du DEP et de l'application du cadre réglementaire hétérogène qu'il implique, il faut aussi prendre en compte que la LDEP a été conçue comme une loi-cadre. En d'autres termes, la LDEP limite significativement la marge de manœuvre de la Confédération pour développer le DEP et laisse planer bon nombre d'incertitudes sur le partage des responsabilités entre Confédération et cantons. Un rapport du Conseil fédéral de 2018 a identifié ces différentes conclusions comme des « défis » (ce par quoi il faut probablement entendre « déficits ») ayant des impacts négatifs aussi bien sous l'angle du financement du DEP que de la conduite générale du projet par exemple<sup>80</sup>.

Un regard attentif sur la LDEP montre que la Confédération a déduit ses compétences législatives des articles 95 al. 1 Cst. (activités économiques lucratives

---

<sup>76</sup> Sur le partage délicat des compétences en matière de santé numérique, v. en particulier : SCHWEIZER, p. 205.

<sup>77</sup> eHealth Suisse, *Datenschutzrechtliche Zuständigkeit*, p. 1. Le document contient également un tableau récapitulatif des différents acteurs potentiellement impliqués dans la mise en œuvre du DEP avec l'indication de l'organe de surveillance compétent en matière de protection des données et les bases légales applicables, p. 2-4.

<sup>78</sup> Art. 11 ss LDEP.

<sup>79</sup> Art. 2 al. 1 et Annexe 2 ODEP-DFI.

<sup>80</sup> Conseil fédéral, *Rapport Wehrli*, notamment p. 44 s.

privées) et 122 al. 1 Cst. (droit civil). Le lien entre ces deux domaines de compétences et le DEP ne coule évidemment pas de source. Dans son message, le Conseil fédéral a expliqué que les règles imposant à un professionnel de la santé de mettre à disposition des données dans le DEP sous certaines formes ou sous certains formats techniques touchaient à la manière dont sa profession devait être exercée. Si la profession était exercée à titre privé, la compétence législative de la Confédération pouvait être déduite de l'art. 95 al. 1 Cst. Quant aux institutions de droit public comme les hôpitaux cantonaux, elles aussi susceptibles de mettre des données dans le DEP (un système réglé selon le droit privé), il faudrait selon le Conseil fédéral qu'elles « *agissent comme des organes privés et qu'elles se fassent certifier en tant que communautés, communautés de référence ou membres d'une communauté ou communauté de référence* »<sup>81</sup>.

La motivation du Conseil fédéral manque de solidité, même si tout le monde s'accordera à dire que le rattachement du DEP aux compétences législatives fédérales relève d'un exercice particulièrement délicat. En fin de compte, cette situation constitutionnelle pour le moins flottante a certainement joué un rôle important dans l'adoption d'un texte qui laisse finalement peu de place à la Confédération et qui, aujourd'hui, se traduit par des retards de mise en œuvre ainsi que bon nombre d'incertitudes juridiques et pratiques.

Le Conseil fédéral n'a pas pour autant dit son dernier mot. Dans son communiqué annonçant une révision complète de la LDEP, il a évoqué son intention d'assimiler le DEP à un instrument de l'assurance obligatoire des soins<sup>82</sup>. Ce repositionnement stratégique devrait permettre à la Confédération de s'accaparer des compétences beaucoup plus larges pour légiférer sur le DEP, en s'appuyant sur l'art. 117 Cst. (assurance-maladie et assurance-accidents). Le Conseil fédéral s'est justifié en expliquant que le DEP contribuera à atteindre les objectifs de l'assurance obligatoire des soins en matière « *d'amélioration de la qualité des traitements et du rapport coût-efficacité* »<sup>83</sup>. Cette explication ne manque pas de susciter quelques interrogations puisqu'il a toujours été clair que le DEP n'avait pas de composante liée aux assurances. Le Conseil fédéral a tout de même tenu à préciser que les assureurs n'auraient pas accès au DEP.

La stratégie du Conseil fédéral de faire basculer le DEP dans le giron réglementaire fédéral des assurances sociales est-elle un coup de maître ou un coup dans l'eau ? Seul l'avenir pourra le dire. Ce débat a néanmoins le mérite de mettre en lumière une problématique récurrente dans le domaine de la santé et

---

<sup>81</sup> Message LDEP 2013, FF 2013 4747, p. 4769.

<sup>82</sup> Conseil fédéral, Le Conseil fédéral veut développer davantage le dossier électronique du patient, communiqué de presse du 27 avril 2022.

<sup>83</sup> Conseil fédéral, Le Conseil fédéral veut développer davantage le dossier électronique du patient, communiqué de presse du 27 avril 2022.

de la protection des données : dans le contexte constitutionnel helvétique actuel, la mise en œuvre d'une initiative nationale en matière de santé numérique est un exercice d'équilibrisme particulièrement périlleux.

### C. Statut des communautés sous l'angle de la protection des données

Si la LDEP et ses ordonnances d'application laissent une grande liberté aux communautés pour se constituer juridiquement comme elles l'entendent (cf. *supra* II.B.), elles leur imposent néanmoins bon nombre d'obligations en lien avec la gestion des données saisies dans le DEP. Les communautés doivent par exemple s'assurer que les données du DEP sont accessibles et consigner un historique de chaque traitement de données<sup>84</sup>. De plus, les communautés de référence doivent gérer les consentements d'ouverture des DEP ou donner la possibilité aux patients d'octroyer des droits d'accès aux professionnels de la santé ou leur permettre d'accéder à leurs propres données. Elles doivent également fournir une information au patient sur le but du DEP, sur le traitement de données ou encore sur les conséquences du consentement<sup>85</sup>.

En parallèle, les communautés sont régies par les législations générales sur la protection des données qui leur sont applicables, ce qui implique de définir le « rôle » ou « statut » de ces communautés à la lumière du droit de la protection des données. En effet, l'assignation d'un rôle ou d'un autre a un impact sur les obligations en matière de protection des données. Les deux rôles traditionnels sont ceux de « responsable du traitement » (ou « maître du fichier » sous l'angle de la LPD actuelle) et de « sous-traitant ».

Le responsable du traitement est celui qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens d'un traitement de données personnelles<sup>86</sup>. La détermination du but et des moyens d'un traitement de données peut concrètement être exercée par plusieurs entités distinctes, qualifiées alors de responsables conjoints du traitement. Dans un tel cas, les responsables conjoints du traitement répondent ensemble du respect des règles de protection des données vis-à-vis des tiers (y compris les personnes concernées), étant entendu qu'ils peuvent et devraient régler à l'interne leurs obligations mutuelles<sup>87</sup>. Pour être

---

<sup>84</sup> Art. 10 al. 1 LDEP.

<sup>85</sup> Art. 15 al. 1 ODEP.

<sup>86</sup> P. ex. art. 5 let. j nLPD.

<sup>87</sup> ROSENTHAL, p. 67. Il s'agit d'une obligation en droit européen : art. 26 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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 (RGPD).

qualifié comme tel, un responsable conjoint du traitement ne doit pas nécessairement disposer d'un accès aux données<sup>88</sup>. La reconnaissance de ce statut se limite toutefois aux données pour lesquelles la personne ou l'entité détermine effectivement les finalités et moyens du traitement de données.

Quant au sous-traitant, il s'agit de la personne ou de l'entité qui traite des données personnelles pour le compte du responsable du traitement. En principe, la sous-traitance des données personnelles est soumise à certaines conditions légales. L'art. 10a LPD exige par exemple que la sous-traitance repose sur une base légale ou un contrat et que le mandant ne sous-traite que les traitements de données qu'il est lui-même en droit d'effectuer. Au surplus, l'acte de sous-traitance ne doit pas être interdit par une obligation légale ou contractuelle de garder le secret et le mandant doit notamment s'assurer que le tiers garantit la sécurité des données. La qualité de sous-traitant au sens du droit de la protection des données est reconnue si trois conditions sont réunies : (i.) le sous-traitant doit être une entité juridique distincte du responsable du traitement, (ii.) le sous-traitant doit effectivement traiter des données personnelles, c'est-à-dire qu'un simple service ne suffit pas encore à admettre un cas de sous-traitance et (iii.) le sous-traitant doit agir pour le compte – c'est-à-dire selon les instructions – du responsable du traitement<sup>89</sup>. Cette dernière condition s'examine à la lumière du degré d'indépendance concret de l'entité et non du libellé d'un éventuel contrat par exemple.

La qualification du rôle des communautés LDEP n'est pas évidente. Pour rappel (*cf. supra* II.B.), la LDEP n'interdit pas aux institutions médico-hospitalières ou aux cabinets médicaux de gérer eux-mêmes un système secondaire et de maintenir l'hébergement des données « DEP » à l'interne. Comme les données doivent néanmoins rester constamment disponibles et qu'elles doivent être hébergées dans un environnement soumis à des normes de sécurité sévères, la solution « *in house* » peut se révéler coûteuse et difficile à mettre en œuvre, surtout pour les petites structures. Ces dernières peuvent ainsi faire héberger les données de leurs patients mises à disposition du DEP auprès des communautés, des communautés de référence ou de prestataires de services privés<sup>90</sup>. Pour certains auteurs, l'hébergement des données DEP par une communauté lui confère le rôle de sous-traitant, de telle sorte que la relation qui lie ces deux protagonistes devrait être réglée par un contrat de sous-traitance au sens de

---

<sup>88</sup> JOTTERAND/ERARD, N 82. En droit européen, se référer notamment aux arrêts de la Cour de justice de l'Union européenne « *Wirtschaftsakademie* » (CJUE, Aff. C-210/16 du 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388, par. 38) et « *Fashion ID* » (Aff. C-40/17 du 29 septembre 2019, *Fashion ID GmbH & Co.KG contre Verbraucherzentrale NRW eV*, ECLI:EU:C:2019:629, par. 82).

<sup>89</sup> JOTTERAND/ERARD, N 83.

<sup>90</sup> WIDMER, *Das elektronische Patientendossier*, p. 770 ; SPRECHER/HOFER, p. 59.



l'art. 10a LPD (pour autant que la LPD s'applique à la personne ou l'entité qui externalise le traitement de données)<sup>91</sup>. Dans cette configuration, les professionnels de la santé, cabinets ou institutions médico-hospitalières endosseraient quant à eux le rôle de responsable du traitement.

Qualifier les communautés de « simples » sous-traitants suscite néanmoins des interrogations. À la lumière des conditions énoncées ci-dessus, les communautés sont effectivement des entités juridiques distinctes qui traitent des données personnelles, mais on peut se demander si elles le font véritablement selon les instructions de l'institution médicale ou du cabinet concerné. La LDEP et ses ordonnances d'exécution imposent en effet un cadre si rigide quant à la manière de traiter les données qu'elles laissent au final bien peu de latitude pour les instructions du mandant une fois que les données sont hébergées auprès d'une communauté (si ce n'est, comme cela peut arriver, les instructions de retirer les données pour les héberger ailleurs). Par exemple, les données versées dans le DEP ne peuvent être rendues accessibles qu'aux conditions posées par la loi. Le degré de précision des exigences de certification des communautés<sup>92</sup> renforce de surcroît ce sentiment.

Dans le même sens, l'adoption d'une perspective différente conduit à se demander si les communautés (à tout le moins les communautés de référence) ne revêtent pas plutôt un rôle de responsable conjoint du traitement, même dans les cas où elles n'hébergeraient pas directement de données de patients. En effet, à la lumière des tâches que leur confie la loi, les communautés de référence assument *de lege* certaines tâches traditionnelles d'un responsable du traitement. Il leur appartient par exemple de fournir une information suffisante aux personnes concernées sur les traitements de données effectués dans le cadre du DEP ou de déterminer à qui les données des patients peuvent être rendues accessibles ou non. Comme le rôle de responsable conjoint du traitement n'implique pas nécessairement un accès direct aux données, il n'apparaît donc pas dénué de sens de reconnaître un tel statut aux communautés, ou à tout le moins aux communautés de référence.

Dogmatiquement, il serait certainement plus exact de reconnaître aux communautés de référence un double statut de responsable conjoint du traitement pour certaines activités (p. ex. gestion du DEP) et de sous-traitant pour d'autres (hébergement des données pour le compte des professionnels de la santé). Pour des raisons pratiques, il est néanmoins préférable de considérer que le rôle de responsable conjoint du traitement englobe celui de sous-traitant, de telle manière à retenir le seul statut de responsable conjoint du traitement. Les institutions médico-hospitalières ou les cabinets médicaux faisant héberger leurs données auprès d'une communauté ont néanmoins tout intérêt à régler ce

---

<sup>91</sup> WIDMER, *Das elektronische Patientendossier*, p. 770 ; SPRECHER/HOFER, p. 59.

<sup>92</sup> Annexe 2 ODEP-DFI.

type de rapports dans un contrat, même en dépit d'une marge de manœuvre somme toute réduite laissée par la LDEP et ses ordonnances.

Il y a encore lieu de préciser que les communautés peuvent elles-mêmes recourir à des sous-traitants pour faire héberger les données des patients. Les critères de certification des communautés établissent d'ailleurs expressément les conditions à satisfaire lorsque les communautés recourent aux services d'un sous-traitant<sup>93</sup>.

En synthèse, l'analyse qui précède montre que les rôles traditionnels du droit de la protection des données (responsable du traitement, sous-traitant) deviennent difficiles à définir dans un système non seulement marqué par la décentralisation, mais aussi et surtout par une forte densité normative. À cet égard, on peut regretter que le législateur ait adopté un système qui s'écarte des concepts traditionnels du droit de la protection des données tout en évitant d'aborder les questions ainsi suscitées. La détermination des rôles dans le DEP pourrait néanmoins faire l'objet de réflexions nouvelles si le Conseil fédéral parvient à concrétiser ses objectifs de révision de la LDEP. Il a en effet affiché sa volonté d'imposer des lieux de stockage centralisés pour les données « dynamiques »<sup>94</sup>. Si l'on se rapporte au rapport WEHRLI<sup>95</sup>, duquel a vraisemblablement été tiré directement cet objectif, l'idée de centralisation vise à remédier aux problèmes causés par le caractère statique des informations qui figurent aujourd'hui dans le DEP (en particulier les fichiers PDF). Dans sa forme décentralisée actuelle, le DEP ne permet en effet pas d'échanger des données dynamiques. Le projet de révision de la LDEP proposera (ou imposera) probablement d'enregistrer des données dynamiques (p. ex. un plan de médication) dans un lieu de stockage centralisé d'une communauté de référence sélectionnée<sup>96</sup>. Si ce projet aboutit, la détermination du rôle d'une telle communauté au sens du droit de la protection des données devra faire l'objet d'une analyse détaillée, à la lumière des nouvelles règles adoptées.

## **D. Utilisation secondaire des données à des fins de recherche**

Le DEP a été conçu principalement, voire exclusivement, comme un outil de soins. Cette idée se déduit implicitement du texte de la LDEP qui limite l'octroi des identités électroniques nécessaires pour accéder au DEP aux seuls patients et professionnels de la santé<sup>97</sup>. Les travaux préparatoires de la LDEP

---

<sup>93</sup> § 4.9 Annexe 2 ODEP-DFI.

<sup>94</sup> Conseil fédéral, Le Conseil fédéral veut développer davantage le dossier électronique du patient, communiqué de presse du 27 avril 2022.

<sup>95</sup> Rapport WEHRLI, p. 5.

<sup>96</sup> Rapport WEHRLI, p. 5.

<sup>97</sup> Art. 7 ss LDEP.

confirment par ailleurs que cette loi est volontairement dénuée de bases légales qui permettraient l'utilisation des données du DEP « *en vue de développer des registres de maladies ou de qualité, à des fins de statistiques ou de recherche ou dans le but d'optimiser des processus administratifs. Si de telles dispositions devaient voir le jour, il faudrait les introduire dans la législation spéciale* »<sup>98</sup>.

Les données de santé saisies dans le DEP suscitent néanmoins certaines convoitises. Au regard de leur nature, ces données pourraient par exemple être exploitées à des fins de recherche sur l'être humain ou de surveillance épidémiologique. Se pose alors la question de savoir si le droit actuellement en vigueur autorise ou non leur accès dans un tel but. La question de l'accès à des fins de recherche a fait l'objet d'une interpellation en 2019 à l'Assemblée fédérale<sup>99</sup>. Dans sa réponse, le Conseil fédéral a exposé qu'il convenait d'appliquer les prescriptions de la LRH<sup>100</sup> relative à la réutilisation des données à des fins de recherche sur l'être humain (art. 16 et art. 32 à 34) et a rappelé les différents types de consentement qui peuvent entrer en ligne de compte selon la nature (génétique ou non génétique) ou la forme (codées ou non codées) des données personnelles en jeu. Il a de surcroît tenu à préciser qu'il serait nécessaire de définir les procédures et les démarches concrètes qui permettraient d'utiliser les données du DEP tout en soulignant les faiblesses de ces données pour la recherche. En effet, ces données ne sont pas structurées et surtout incomplètes puisqu'elles ne concernent que les données pertinentes pour la suite du traitement (*cf. supra* D.1.) et que le patient peut décider en tout temps d'en détruire tout ou partie, alternativement de les rendre secrètes.

Comme la LDEP limite aujourd'hui implicitement l'accès aux données du DEP aux seuls patients et professionnels de la santé, on peut légitimement se demander si la réponse du Conseil fédéral qui reconnaît la possibilité d'accès par des chercheurs est compatible avec la LDEP. Par ailleurs, le renvoi aux dispositions régissant la réutilisation des données à des fins de recherche soulève une nouvelle question. Alors que le DEP a été construit sur un modèle qui repose essentiellement sur le consentement du patient (ouverture du DEP, niveaux de confidentialité modulables, autorisation d'accès), le renvoi en bloc aux dispositions de la LRH ouvre possiblement la voie à des réutilisations de données sans consentement, même si celles-ci ne devraient être admises que de manière exceptionnelle (art. 34 LRH). Une telle réutilisation est néanmoins seulement admissible si le recueil du consentement est impossible ou pose des difficultés disproportionnées, de telle sorte que son application semble peu probable en présence d'un outil comme le DEP. En effet, ce dernier a été conçu comme un

---

<sup>98</sup> Message LDEP 2013, FF 2013 4747, p. 4796.

<sup>99</sup> Interpellation de Edith GRAF-LITSCHER du 25 septembre 2019, Le dossier électronique du patient peut-il être utilisé à des fins de recherche scientifique ?, objet n° 19.4136.

<sup>100</sup> Loi fédérale du 30 septembre 2011 relative à la recherche sur l'être humain (LRH), RS 810.30.

outil qui doit précisément permettre au patient d'accorder facilement ou non des accès à ses données de santé.

Comme c'est le cas pour les autres questions choisies de cette contribution, l'accès aux données du DEP à des fins de recherche devrait bientôt être débattu. Dans son communiqué relatif à la révision de la LDEP, le Conseil fédéral a en effet annoncé son intention d'assurer que les milieux de la recherche puissent accéder aux données du DEP si les patients y consentent<sup>101</sup>.

## IV. Conclusion

En dépit de son caractère non exhaustif, la présente contribution a permis de mettre en lumière quelques caractéristiques juridiques essentielles du DEP ainsi que certaines problématiques ouvertes. Parmi les conclusions notables, on retiendra en particulier les difficultés posées par le droit constitutionnel suisse pour la mise en œuvre d'une initiative d'envergure nationale dans le domaine de la santé numérique. Les partages complexes de compétences entre la Confédération et les cantons en matière de santé et de protection des données ont par exemple conduit à l'adoption d'une loi-cadre qui devait initialement se limiter à poser des principes, mais qui s'est en réalité traduite par une législation d'application particulièrement dense et peu flexible. Dans un sens similaire, les bases constitutionnelles peu solides de la LDEP ainsi que les hésitations apparentes du Conseil fédéral ont débouché sur une loi qui fait la part belle à la décentralisation, tout en créant des lacunes importantes en matière de gouvernance. Ces dernières se distinguent particulièrement sous l'angle du *leadership* et du financement du DEP.

En annonçant son intention de réviser totalement la LDEP, notamment en modifiant son rattachement constitutionnel pour offrir un plus grand pouvoir décisionnel à la Confédération, le Conseil fédéral a montré qu'il avait identifié une partie au moins des défauts de la LDEP. L'examen des objectifs annoncés pour cette révision laisse ainsi entrevoir une forme générale de « *recentralisation* » du DEP, non seulement sur le plan de la gouvernance, mais aussi sur celui des traitements de données (projet de centraliser les données dynamiques auprès d'une communauté de référence). Or, une « *centralisation* » entraîne nécessairement une « *externalisation* ». Cette externalisation existe déjà dans une certaine mesure avec l'hébergement de données par les communautés ou tout simplement au travers des services assumés par ces dernières pour assurer la mise à disposition des données aux autres professionnels de la santé. Selon

---

<sup>101</sup> Conseil fédéral, Le Conseil fédéral veut développer davantage le dossier électronique du patient, communiqué de presse du 27 avril 2022.

la forme et l'ampleur qu'il prendra dans le futur, ce phénomène d'externalisation suscitera des questions techniques et juridiques similaires à celles posées par les technologies *cloud* et il conviendra d'examiner celles-ci de près lorsqu'elles seront discutées et mises en œuvre.

À ce jour, les réflexions liées au DEP se sont principalement concentrées sur son utilisation à l'échelon helvétique uniquement. Un bref regard vers nos voisins européens montre cependant une forte activité en matière de gestion électronique des données médicales des patients. Au début du mois de mai 2022, la Commission européenne a officiellement lancé son projet d'espace européen des données de santé (ou *European Health Data Space*, EHDS)<sup>102</sup>. La mise en œuvre de l'EHDS doit notamment permettre aux citoyens d'avoir un accès facilité et immédiat à leurs données de santé et leur donner les moyens de partager facilement leurs données avec d'autres professionnels de la santé, y compris au sein de l'Union européenne. L'EHDS doit également améliorer les conditions d'accès aux données de santé à des fins de recherche, d'innovation et d'élaboration de politiques grâce à un nouveau cadre juridique qui autorisera l'accès à ces données sous certaines conditions strictes, en particulier liées à la protection des données et à la garantie de l'anonymat des personnes concernées. Comme le DEP se trouve aujourd'hui encore dans une phase de développement propice à la malléabilité, il y aurait tout intérêt à intégrer aussi tôt que possible les aspects juridiques d'interopérabilité avec des systèmes étrangers similaires et plus particulièrement avec les outils qui seront développés dans le contexte de l'EHDS.

Au final et au regard du faible taux d'adoption actuel, le DEP n'a pas créé la révolution qu'on aurait pu attendre de lui. Il est néanmoins trop tôt pour évoquer une désillusion. Le DEP est encore naissant et les révisions légales qui doivent le conduire à maturité devront faire l'objet d'une attention particulière.

## V. Bibliographie

### A. Littérature

**Yves DONZALLAZ**, Traité de droit médical. Volume II – Le médecin et les soignants, Berne 2021 ; **Frédéric ERARD**, Le secret médical. Étude des obligations de confidentialité des soignants en droit suisse, Zurich 2021 (cité : ERARD, Le secret médical ; <[https://suigeneris-verlag.ch/img/uploads/pdf/oa\\_pdf-015-1621189059.pdf](https://suigeneris-verlag.ch/img/uploads/pdf/oa_pdf-015-1621189059.pdf)> (consulté le 7 mai 2022) ; **Frédéric ERARD**, Le Conseil fédéral veut faire avancer le dossier électronique du patient,

---

<sup>102</sup> Commission européenne, Union européenne de la santé : Un espace européen des données de santé pour les personnes et pour la science, communiqué de presse du 3 mai 2022, <[https://ec.europa.eu/commission/presscorner/detail/fr/ip\\_22\\_2711](https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_2711)> (consulté le 7 mai 2022).

Swissprivacy.law 3 mai 2022 <<https://swissprivacy.law/142/>> (consulté le 7 mai 2022) (cité : ERARD, Conseil fédéral) ; **Walter FELLMANN/Michèle ODERMATT**, Haftpflichtrechtliche Fragen beim elektronischen Patientendossier, Jusletter 27 avril 2020 ; **Michael ISLER**, Datenschutz und Informationssicherheit im Bereich « mobile health » (mHealth), avis de droit, 19 janvier 2018, <<https://www.e-health-suisse.ch/fr/mise-en-oeuvre-communautes/activites-ehealth/mhealth.html>> (consulté le 7 mai 2022) ; **Alexandre JOTTERAND/Frédéric ERARD**, Recherche sur l'être humain et données personnelles. Gestion des échanges et répartition des responsabilités, Jusletter 30 août 2021 ; **Philippe MEIER**, Le proche représentant en matière médicale peut-il délier le médecin de son secret professionnel ?, RMA 2018, p. 455 ss ; **David ROSENTHAL**, Controller oder Processor : Die datenschutzrechtliche Gretchenfrage, Jusletter 17 juin 2019 ; **Benjamin SCHINDLER/Tobias TSCHUMI**, Kurzgutachten zu Fragen im Zusammenhang mit dem elektronischen Patientendossier (EPD), avis de droit, 28 février 2018, <<https://www.fmh.ch/files/pdf25/gutachten-zu-fragen-im-zusammenhang-mit-dem-elektronischen-patientendossier-v1.pdf>> (consulté le 7 mai 2022) ; **Rainer J. SCHWEIZER**, Digitalisierung im Gesundheitswesen, digma 2020, p. 204 ss ; **Franziska SPRECHER/Aline HOFER**, Das elektronische Patientendossier, Datenschutzaspekte, in Astrid EPINEY/Déborah SANGSUE (éds), Protection des données et droit de la santé. Forum Europarecht : Vol. 40, Zürich 2019, p. 43 ss ; **Andreas STÖCKLI**, Elektronisches Patientendossier und Krankenversicherungsrecht, AJP/PJA 2019, p. 1156 ss ; **Barbara WIDMER**, Das elektronische Patientendossier – ein Mammutprojekt wird Realität, AJP 2017, p. 765 ss (cité : WIDMER, Das elektronische Patientendossier) ; **Barbara WIDMER**, ePatientendossier und Datenschutz, digma 2017, p. 160 ss (cité : WIDMER, ePatientendossier).

## B. Documents officiels

**Confédération suisse**, Stratégie Cybersanté Suisse 2.0, 14 décembre 2018 ; **Conseil fédéral**, Message concernant la loi fédérale sur le dossier électronique du patient (LDEP) du 29 mai 2013, FF 2013 p. 4747 ss (cité : Message LDEP 2013) ; **Conseil fédéral**, Politique de la santé : stratégie du Conseil fédéral 2020-2030, décembre 2019 (cité : Stratégie 2030) ; **Conseil fédéral**, Dossier électronique du patient. Que faire encore pour qu'il soit pleinement utilisé ? Rapport du Conseil fédéral donnant suite au postulat 18.4328 Wehrli, 14 décembre 2018 (cité : Rapport WEHRLI) ; **Conseil fédéral**, Le Conseil fédéral veut développer davantage le dossier électronique du patient, communiqué de presse du 27 avril 2022, <<https://www.admin.ch/gov/fr/accueil/documentation/communiqués.msg-id-88245.html>> (consulté le 7 mai 2022) ; **eHealth Suisse**, Responsabilité lors de l'utilisation du DEP, factsheet, mars 2021 (cité : eHealth Suisse, Responsabilité) ; **eHealth Suisse**, Représentation dans le cadre du DEP. Aide à la mise en œuvre pour les communautés de référence, mars 2019 (cité : eHealth Suisse, Représentation dans le cadre du DEP) ; **eHealth Suisse**, Informations pertinentes pour le traitement. Aide à la mise en œuvre pour les communautés de référence, septembre 2019 (cité : eHealth Suisse, Informations pertinentes) ; **eHealth Suisse**, Das elektronische Patientendossier und die datenschutzrechtliche Zuständigkeit, 20 novembre 2018 (cité : eHealth Suisse, Datenschutzrechtliche Zuständigkeit) ; **Office fédéral de la santé publique**, Stratégie Cybersanté (eHealth) Suisse, 27 juin 2007 ; **Office fédéral de la santé publique**, Rapport explicatif concernant l'ordonnance sur le dossier électronique du patient (ODEP) et l'ordonnance du DFI sur le dossier électronique du patient (ODEP-DFI), 22 mars 2017 (cité : Office fédéral de la santé publique, Rapport explicatif ODEP).

---

# Cloud et territoire

SUZANNE VERGNOLLE

Docteure en droit, Maître de conférences au Conservatoire national des arts et métiers (Cnam)

## Table des matières

<b>I. Introduction .....</b>	<b>244</b>
A. Observations générales .....	244
B. Le « <i>Cloud</i> » : brèves observations conceptuelles .....	244
C. Le territoire : fondement de la souveraineté de l'État .....	245
D. Le <i>cloud</i> et le territoire : quelles interactions ? .....	246
<b>II. Le <i>cloud</i> dans le territoire .....</b>	<b>247</b>
A. Observations introductives.....	247
B. L'aspiration à une « souveraineté numérique » .....	248
1. Observations introductives .....	248
2. Une aspiration générale .....	248
3. Des aspirations ciblées.....	249
C. Les tentatives de <i>Cloud</i> souverain .....	250
D. Les lois imposant la localisation des données sur leur territoire....	252
<b>III. Le <i>Cloud</i> au-delà du territoire .....</b>	<b>253</b>
A. Observations introductives.....	253
B. Les règles encadrant les transferts de données au-delà du territoire.....	254
C. Les règles octroyant des accès aux données au-delà du territoire ( <i>CLOUD Act, e-evidence</i> ).....	256
<b>IV. Observations conclusives.....</b>	<b>259</b>
<b>V. Bibliographie .....</b>	<b>260</b>
A. Littérature.....	260
B. Documents officiels .....	261

## I. Introduction

### A. Observations générales

« *N'oublie pas que chaque nuage, si noir soit-il, a toujours une face ensoleillée, tournée vers le ciel.* » Cette incitation à la réflexion proposée par Friedrich Wilhelm Weber nous rappelle que toute perception est une question de point de vue. En fonction de la perspective, chacun y voit ce qu'il veut y voir, ignorant parfois qu'une autre position, donc une autre perspective, est possible.

Les nuages informatiques sont-ils si différents des nuages météorologiques ? Après tout, ils présentent bel et bien certaines caractéristiques communes : ils peuvent être larges ou petits, attendus ou redoutés, proches ou lointains. Parfois, ils entraînent la foudre et lorsqu'elle frappe, par son électricité ou par une cyberattaque, les humains sont souvent dévastés !

En droit, l'apparente volatilité du nuage informatique a parfois généré quelques doutes ou incompréhensions sur les enjeux territoriaux liés à cette technologie. Fort heureusement, les informaticiens n'ont pas manqué de rappeler aux juristes que : « *there is no cloud, it's just someone else's computer* », soulignant ainsi le principe de matérialité et de territorialité de l'infrastructure technique existante derrière le *cloud*.

### B. Le « *Cloud* » : brèves observations conceptuelles

L'informatique en nuage, équivalent français de *cloud* ou *cloud computing*, fait référence à « *l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau* »<sup>1</sup>. En d'autres termes, le *cloud* est une infrastructure informatique virtualisée fournissant des services que les utilisateurs peuvent exploiter depuis n'importe quel lieu du monde. Le *cloud* repose donc fondamentalement sur une délocalisation des traitements ainsi que sur une externalisation des compétences<sup>2</sup>. En confiant leurs données ou leurs infrastructures à des entreprises plus compétentes et expertes qu'elles, les clients peuvent alors mieux se concentrer sur leurs propres services. C'est ce qui explique la variété des offres de *cloud computing* parmi lesquelles figurent trois modèles de services (SaaS<sup>3</sup>, PaaS<sup>4</sup>,

---

<sup>1</sup> CNIL, site Internet, page « Définition de Cloud Computing ».

<sup>2</sup> MONTAVON, p. 459.

<sup>3</sup> *Software as a Service*, pouvant être traduit par « logiciel à la demande ».

<sup>4</sup> *Platform as a Service*, pouvant être traduit par « plateforme-service ».



IaaS<sup>5</sup>) et trois modèles de déploiement (public, privé, hybride)<sup>6</sup>. Le choix du modèle dépend des besoins du client, notamment en termes d'architecture informatique, de gouvernance, et de gestion des risques.

En pratique, le *cloud* présente de nombreux avantages. D'abord, il offre une meilleure utilisation des ressources, particulièrement avec le déploiement des *clusters*, lesquels adaptent l'infrastructure utilisée en fonction des besoins du client. Cette meilleure utilisation des ressources techniques se transforme souvent en économies financières : non seulement des économies d'échelle sont réalisées mais surtout, seuls les services utilisés par le client sont facturés. Ensuite, les infrastructures de *cloud* de bonne qualité présentent souvent un meilleur niveau de sécurité que celui existant dans les infrastructures autonomes. En externalisant leurs besoins à des fournisseurs de confiance, les petites et moyennes entreprises bénéficient de technologies de meilleur niveau que celles qu'elles pourraient développer en interne. De plus, les organisations se déchargent des tâches de maintenance et de mise à jour des systèmes informatiques, et bénéficient des certifications réglementaires détenues par leurs fournisseurs. Enfin, le *cloud* offre également une plus grande mobilité pour le client puisque les données sont accessibles depuis n'importe quelle machine connectée au réseau.

Ces avantages ne doivent pas cacher les risques liés à l'usage de cette technologie, tels que la perte de contrôle ou de données, le manque d'isolation entre les données, les pannes du système et du réseau...<sup>7</sup> Surtout, dès lors que l'usage est délocalisé, il n'est pas certain que les serveurs du fournisseur de *cloud* se situent sur le même territoire que leurs clients. Des problèmes d'application territoriale du droit peuvent alors surgir. Le territoire et le droit entretiennent en effet des liens profonds et anciens.

### C. Le territoire : fondement de la souveraineté de l'État

La notion de « territoire » de l'État s'est progressivement séparée de l'idée de « possession du sol » par le seigneur qui a longtemps prévalu pendant le Moyen Âge<sup>8</sup>. À partir du XVI<sup>e</sup> siècle, le territoire va apparaître comme l'un des fondements essentiels de l'État, notamment avec les Traités de Westphalie signés en 1648. La notion de territoire devient alors la pierre angulaire du droit international.

<sup>5</sup> *Infrastructure as a Service*, pouvant être traduit par « infrastructure à la demande ».

<sup>6</sup> GREVET, p. 10 s.

<sup>7</sup> PFPDT, Explications.

<sup>8</sup> CARREAU/MARRELLA, p. 52.

Le territoire marque les limites géographiques où s'exerce exclusivement l'autorité, c'est-à-dire la compétence de l'État. En dehors de ces limites, l'État n'a pas de compétence et il ne peut donc pas légitimement intervenir. Ce principe est rappelé par de nombreuses règles, notamment l'article 3 alinéa 1 du Code pénal suisse, lequel limite son applicabilité « à quiconque commet un crime ou un délit en Suisse ». Bien sûr, des exceptions existent afin de garantir la cohérence et l'utilité de ce principe, mais les frontières du territoire caractérisent bel et bien la compétence étatique de principe<sup>9</sup>.

La notion de territoire est souvent rapprochée de celle de souveraineté. Cette dernière est classiquement définie comme la capacité des États à imposer des règles sur leur territoire et à interagir avec leurs pairs. Cela signifie non seulement que la compétence de l'État sur son territoire est pleine et exclusive, mais aussi qu'il n'existe pas de subordination d'un État par rapport aux autres<sup>10</sup>. Les limites de la souveraineté d'un État ainsi que sa capacité à édicter des règles juridiques, sont donc largement liées aux démarcations territoriales. Les caractéristiques du *cloud* rendent parfois complexe l'appréhension de la compétence territoriale ainsi que son application.

#### **D. Le *cloud* et le territoire : quelles interactions ?**

Puisque le *cloud* est un outil reposant principalement sur Internet, il n'est pas inutile de rappeler la caractéristique principale de ce dernier : il s'agit d'un ensemble de réseaux sans délimitation territoriale<sup>11</sup>. En étant accessible partout dans le monde, Internet a largement contribué à redéfinir l'application territoriale des règles juridiques ainsi que la compétence juridictionnelle.

Pourtant, en dépit de son apparente volatilité et de son absence de rattachement territorial, Internet repose bel et bien sur des infrastructures techniques et matérielles. Les menaces pesant sur la rupture des câbles sous-marins ainsi que les enjeux écologiques liés aux fermes de serveurs en sont des témoins. Il en va de même pour le *cloud*. Les interruptions de services de l'entreprise *Amazon Web Services* (AWS) en 2017 avaient en effet entraîné de fortes perturbations sur de nombreux services et sites marchands et mis en évidence la réalité matérielle existante derrière le *cloud*.

De nombreux enjeux de compétences découlent de l'utilisation du *cloud*. Par exemple, comment déterminer le droit applicable aux données d'une entreprise suisse, dont l'informatique est gérée depuis la France, avec des serveurs *cloud* situés en Belgique, disposant d'une infrastructure de secours aux États-Unis ?

---

<sup>9</sup> MÜLLER, p. 307.

<sup>10</sup> KRANZ, p. 413 ss.

<sup>11</sup> GOLDSMITH, p. 475 ; SCHERRER, p. 474.

Est-ce uniquement le droit suisse ? Probablement pas. Seulement un autre des droits des États impliqués ? Non plus. En réalité, le droit applicable à ces données est certainement un assemblage des différentes règles juridiques des pays offrant un rattachement plus ou moins direct avec les différents acteurs. Le juriste doit alors effectuer une vérification minutieuse de la compatibilité de ces règles entre elles afin de s'assurer de leur cohérence ainsi que de la conformité de son organisation aux règles nationales. La question de la conformité est d'autant plus importante lorsque les données envoyées et conservées dans le *cloud* sont des données personnelles<sup>12</sup>. Dans ce cas, aux principes juridiques d'ores et déjà applicables au *cloud* tels que ceux relatifs aux obligations liées à la coopération pénale s'ajoute également la réglementation spéciale du droit des données personnelles, menant à des vérifications techniques et juridiques ainsi qu'à l'insertion de dispositions contractuelles impératives<sup>13</sup>.

L'objectif de la présente contribution n'est pas de proposer une réponse juridique exhaustive en lien avec une situation particulière. Il est plutôt d'ébaucher quelques-unes des principales problématiques en lien avec le *cloud* et le territoire. À cet effet, il sera proposé d'étudier les interactions entre ces deux thèmes, mais aussi d'élargir les perspectives à d'autres sujets liés, tels que ceux de souveraineté ou d'extraterritorialité. Pour ce faire, il s'agit, dans un premier temps, de s'intéresser aux enjeux liés au *cloud* dans le territoire (II.) pour ensuite voir, dans un second temps, les enjeux liés au *cloud* au-delà du territoire (III.).

## II. Le *cloud* dans le territoire

### A. Observations introductives

L'espoir d'un développement numérique ouvert et décentralisé offrant un renouvellement des modes de gouvernance et de répartition des pouvoirs s'étirole progressivement pour laisser place à une centralisation croissante des services en ligne. Quelques multinationales américaines et chinoises se partagent aujourd'hui la majorité du « gâteau » numérique. Les enjeux de gouvernance liés à cette centralisation ne sont pas uniquement théoriques mais bel et bien politiques et géostratégiques. Depuis plusieurs années, la tendance actuelle des registres décentralisés (souvent dénommés « Web 3 ») cherche à prendre le contre-pied de cette centralisation. Par ailleurs, un nombre croissant d'États développent des stratégies favorables à une souveraineté dans l'environnement numérique (B). Certains États européens, dont la France et la Suisse, tentent

---

<sup>12</sup> Sur les exigences de la protection des données, voir la contribution de FISCHER/PITTET dans cet ouvrage ; BOURGEOIS/MOINE.

<sup>13</sup> ANCELLE/FERDJANI, p. 140.

ainsi de développer des *cloud* souverains (C), alors que d'autres États, tels que la Chine ou la Russie, ont imposé l'hébergement des données sur leur territoire aux opérateurs actifs dans leur juridiction (D).

## **B. L'aspiration à une « souveraineté numérique »**

### *1. Observations introductives*

L'expression « souveraineté numérique » renvoie à l'application des principes de souveraineté au domaine des technologies de l'information et de la communication. L'aspiration à une souveraineté numérique suppose de s'intéresser aux différents acteurs impliqués dans l'outil numérique : de la construction des composants électroniques, à la localisation des machines, en passant par les logiciels exécutés sur celles-ci, chacune de ces étapes génèrent des enjeux de souveraineté<sup>14</sup>. L'aspiration à une souveraineté numérique peut donc être générale (2) ou ciblée (3).

### *2. Une aspiration générale*

Comme le remarquait le mathématicien et député français Cédric VILLANI dans un rapport sur l'intelligence artificielle, « rien qu'en France, 80 % des visites vers les 25 sites les plus populaires sur un mois sont captés par les grandes plateformes américaines »<sup>15</sup>. Affinant ce constat, des sénateurs français relevaient que la situation géopolitique actuelle place l'Europe dans une situation délicate face à la prédominance des acteurs américains, parfois concurrencés par certains acteurs chinois<sup>16</sup>. Les sénateurs remarquaient d'ailleurs que le continent européen avait, jusqu'à présent, adopté une attitude plutôt défensive à l'égard de ces grands services en ciblant la défense de certaines valeurs, telles que la protection des données personnelles<sup>17</sup>.

Face à ce constat, des voix s'élèvent de plus en plus fort pour encourager une vision plus ambitieuse de la souveraineté numérique et pour mettre en place des infrastructures numériques garantissant une véritable autonomie européenne<sup>18</sup>. D'autres voix n'hésitent pas à rappeler que les subventions publiques ne suffiront pas à poser les bases d'une souveraineté et que les causes du retard se trouvent dans des facteurs plus fondamentaux, tels que les visions sociales

---

<sup>14</sup> FITZJEAN Ó COBHTHAIGH, p. 16.

<sup>15</sup> VILLANI, p. 27.

<sup>16</sup> MONTAUGE/LONGUET, p. 16.

<sup>17</sup> *Ibid.*

<sup>18</sup> Voir par exemple GHERNAOUTI/AGHROUM, p. 81.

et culturelles de la technologie et du numérique. Conciliant ces deux approches, le rapport sénatorial français<sup>19</sup> considère qu'une politique ambitieuse de souveraineté doit s'inscrire dans trois directions :

- *celle des infrastructures*, à savoir le déploiement sur le territoire européen ou national d'infrastructures numériques ;
- *celle politique*, c'est-à-dire le développement d'une politique industrielle identifiant les secteurs technologiques essentiels dans lesquels investir ; et enfin
- *celle des écosystèmes*, à savoir la mise en place de moyens humains et financiers favorisant l'émergence de virtuoses numériques européens.

Des stratégies générales et ambitieuses sont donc proposées par les États européens afin de stimuler le développement d'un modèle alternatif et souverain<sup>20</sup>. À ces stratégies générales s'ajoutent également certaines aspirations ciblées.

### 3. Des aspirations ciblées

Pour l'actuelle Présidente de la Commission européenne Ursula VON DER LEYEN, « *il est peut-être trop tard pour reproduire des géants du numérique, mais il n'est pas trop tard pour atteindre la souveraineté technologique dans certains secteurs technologiques critiques* »<sup>21</sup>. Ainsi, plutôt que de tenter d'imiter les succès passés, il faudrait faire des choix stratégiques pour garantir un futur technologique ambitieux et respectueux des valeurs européennes.

Selon cette approche, certains secteurs clés doivent être privilégiés, au rang desquels figurent les technologies liées à la « *blockchain, au calcul informatique de pointe, à l'informatique quantique, ainsi qu'aux algorithmes et aux outils permettant l'usage et le partage des données* »<sup>22</sup>. Il est assez clair que certaines de ces technologies entretiennent un lien avec le *cloud*.

Constatant que l'informatique en nuage se produit actuellement principalement dans certains grands centres de données, la Commission européenne compte sur une inversion de cette tendance d'ici 2025. Selon l'institution, 80 % des données devraient être traitées par des appareils intelligents plus proches de l'utilisateur, une tendance connue sous le nom de « *edge computing* ». Une telle

<sup>19</sup> MONTAUGE/LONGUET, p. 119.

<sup>20</sup> Ces stratégies incluent notamment le développement d'infrastructures souveraines telles que le *cloud* souverain ou de politiques publiques favorables aux nouveaux entrants sur le marché numérique telles que celles proposées dans le *Digital Markets Act*.

<sup>21</sup> VON DER LEYEN, p. 13.

<sup>22</sup> VON DER LEYEN, p. 13.

inversion offrirait des perspectives intéressantes en termes de souveraineté et permettrait sans doute des investissements stratégiques pour préparer l'avenir.

Ces stratégies technologiques sont complétées par une politique réglementaire effervescente. Des textes en lien avec le *cloud* tels que ceux liés à la circulation des données<sup>23</sup> ou à la cybersécurité<sup>24</sup> ont été rapidement adoptés, et de nombreux autres textes sont en cours de négociation.

La stratégie européenne est encore plus précise et ambitieuse en matière de *cloud* « souverain ».

### C. Les tentatives de *Cloud* souverain

En tant qu'infrastructure, le *cloud* se révèle un outil essentiel de toute stratégie de souveraineté numérique. C'est pourquoi plusieurs pays tels que la France, la Suisse ou l'Allemagne ont pour ambition de développer des *cloud* dits souverains. Le *cloud* souverain est défini comme un modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur des données par un service de *cloud* sont physiquement réalisés dans les limites du territoire national par une entité de droit national et en application des lois et normes nationales<sup>25</sup>. Une telle définition surprend puisqu'il est désormais reconnu que le droit national s'applique non seulement aux entités de droit national mais aussi aux entités étrangères ayant un rattachement avec le territoire national. Par exemple, la loi fédérale sur les cartels prévoit explicitement qu'elle « est applicable aux états de fait qui déploient leurs effets en Suisse, même s'ils se sont produits à l'étranger »<sup>26</sup>. L'article 3 al. 1 de la nouvelle Loi fédérale de protection des données (nLPD<sup>27</sup>) reprend ce principe de l'effet, en tant que concrétisation particulière du principe de territorialité<sup>28</sup>. Même si l'objectif de *cloud* souverain va bien au-delà d'une réponse purement juridique, il est regrettable de voir une mauvaise identification de l'un de ses enjeux principaux.

---

<sup>23</sup> Règlement 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, JO L 303 du 28 novembre 2018, p. 59.

<sup>24</sup> Règlement 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications, JO L 151 du 7 juin 2019, p. 15.

<sup>25</sup> Ministères français de l'intérieur et de la culture, Note d'information du 5 avril 2016.

<sup>26</sup> Article 2 de la loi fédérale du 6 octobre 1995 sur les cartels (LCart), RO 1996 546.

<sup>27</sup> Loi fédérale du 25 septembre 2020 sur la protection des données (nLPD), FF 2020 7397.

<sup>28</sup> ROSENTHAL/STUDER, p. 37.

D'autant que les acteurs nationaux, dès qu'ils ont un rayonnement à l'international, seront également soumis à des droits étrangers<sup>29</sup>.

Plusieurs initiatives de *cloud* souverain essaient en Europe. Elles sont les témoins de la volonté politique d'améliorer la souveraineté nationale en matière de données et de réduire au minimum la dépendance des pays aux prestataires internationaux de services en nuage publics<sup>30</sup>. Dès janvier 2010, le Premier ministre français regrettait que les entreprises nord-américaines « *dominent ce marché, qui constitue pourtant un enjeu absolument majeur [...] pour la souveraineté de nos pays* »<sup>31</sup>. Son souhait était alors de développer « *un partenariat public-privé grâce aux fonds du programme pour les investissements d'avenir* ». Deux ans plus tard, l'État français investissait 150 millions d'euros dans deux projets de *cloud* (*Numergy* et *Cloudwatt*) qui ont peiné à atteindre leurs objectifs et à trouver leur public. Face à ces difficultés, *Numergy* fut placé en redressement judiciaire, puis fut racheté par *SFR* en 2016, et *Cloudwatt* a fermé ses portes en janvier 2020. Cet échec cuisant n'a pas découragé les représentants politiques qui ont continué d'insister sur la nécessité d'un *cloud* français ou européen en février 2020<sup>32</sup>, lequel s'est matérialisé avec le projet *GAIA-X*. Initialement lancé autour de 22 entreprises françaises et allemandes, il associe, depuis novembre 2020, plus de 180 entreprises, notamment les grandes figures (étrangères) du *cloud*, telles *Alibaba*, *Amazon*, *Google*, *Microsoft*, et du logiciel, comme *Oracle*, *Palantir* ou *Salesforce*. D'importants problèmes de gouvernance au sein du projet ont été dénoncés par la société civile. D'ailleurs, en novembre 2021, l'entreprise française *Scaleway*, un des membres fondateurs de l'initiative, a annoncé son retrait en raison de la présence jugée trop importante des acteurs étrangers.

Si *GAIA-X* s'est récemment orienté vers un rassemblement des acteurs du *cloud* sous une même initiative, le rêve d'un *cloud* souverain persiste. La Conférence « *Construire la souveraineté numérique de l'Europe* » de février 2022 en est une preuve supplémentaire. Douze États membres de l'Union y ont manifesté leur volonté de contribuer au « *projet important d'intérêt européen commun (PIIEC), afin de renforcer nos investissements et notre autonomie stratégique en matière de cloud et d'edge computing* », avec un financement à hauteur de 7 milliards d'euros<sup>33</sup>. L'articulation entre *GAIA-X* et ce nouveau projet

<sup>29</sup> Voir développements III, C.

<sup>30</sup> Conseil fédéral, Communiqué du 16 avril 2020.

<sup>31</sup> Premier ministre français, Discours du 18 janvier 2010.

<sup>32</sup> Ministre de l'économie et Commissaire européen au marché intérieur, Déclarations du 7 février 2020.

<sup>33</sup> Ministère français de l'Europe et des affaires étrangères, Ministère français de l'économie et Secrétariat d'État français chargé de la transition numérique, Communiqué conjoint du 7 février 2022.

n'apparaît pas très claire et des doutes subsistent quant à la bonne allocation des fonds publics dans ce domaine.

De son côté, le Conseil fédéral avait décidé de faire examiner, en avril 2020, « *la nécessité, la conception, l'utilité et la faisabilité d'un nuage informatique suisse (« Swiss Cloud »)* »<sup>34</sup>. Publié en décembre 2020, le rapport d'évaluation concluait que « *la nécessité d'un « Swiss Cloud » sous forme d'infrastructure de droit public et comme clé du succès de la place économique suisse n'est pas démontrée* », mais que « *la demande est forte concernant un label « Swiss Cloud » proposant un cadre adapté et des lignes directrices pour une utilisation compétente et sécurisée des services en nuage* »<sup>35</sup>. Sans plus attendre, la Confédération a publié quelques semaines plus tard un appel d'offres pour des services d'informatique en nuage d'une valeur de 110 millions de francs, lequel a fait l'objet d'importantes critiques de certains acteurs locaux l'ayant qualifié de contre-productif et excluant les firmes suisses<sup>36</sup>. Sans grande surprise, l'appel d'offres fut remporté par cinq géants du *cloud*, quatre américains (*Amazon, IBM, Microsoft et Oracle*) et un chinois (*Alibaba*). Toutefois, et de manière surprenante, *Google* ne faisait pas partie des acteurs américains sélectionnés. L'entreprise écartée avait intenté un recours qui fut rejeté par le Tribunal administratif fédéral<sup>37</sup>. Plusieurs concurrents suisses ont réitéré leurs critiques sur le choix de la Confédération et ont dénoncé le renforcement de la dépendance à l'égard des grands fournisseurs de *cloud* étrangers.

À ces projets de *cloud* souverains s'ajoutent également d'autres initiatives telles que celles liées aux lois imposant la localisation des données.

## **D. Les lois imposant la localisation des données sur leur territoire**

Depuis le début des années 2010, plusieurs pays ont adopté des lois exigeant que certaines données (personnelles, commerciales, ou financières) soient collectées, traitées ou conservées sur leur territoire. Les mesures vont d'une simple obligation de conserver physiquement les données dans le pays d'origine à une restriction, voire à une prohibition, de les transférer vers des pays tiers. Parmi les États ayant adopté de telles lois figurent notamment la Chine, l'Inde, l'Indonésie, la Russie ou encore le Vietnam<sup>38</sup>. Les arguments

---

<sup>34</sup> Conseil fédéral, Communiqué du 16 avril 2020.

<sup>35</sup> Rapport « Swiss Cloud », décembre 2020, p. 30.

<sup>36</sup> Office fédéral des constructions et de la logistique, Appel d'offre du 7 décembre 2020, n° 1136861.

<sup>37</sup> TAF, arrêt B-3238/2021 du 18 octobre 2021.

<sup>38</sup> CORY/DASCOLI, p. 27 s. ; CHANDER/LÉ, p. 682 s.



justifiant de telles obligations diffèrent en fonction des pays, mais se résument souvent à une prétendue meilleure sécurité ou protection des données, à une sauvegarde de la souveraineté nationale, ainsi qu'aux besoins d'accès par les enquêteurs dans le cadre d'enquêtes<sup>39</sup>. Si ces arguments sont parfaitement recevables et sont de nature à justifier une politique juridique imposant certaines limites en matière de circulation des données, ils peuvent aussi se révéler comme un miroir distordant d'objectifs politiques distincts. Certains de ces pays utilisent en effet ces lois pour permettre une surveillance de leurs citoyens et affaiblir les opinions politiques dissidentes.

Du fait de sa structure technique, le *cloud* se prête, en principe, plutôt mal aux obligations de localisation des données. En effet, les *clouds* sont accessibles depuis n'importe quel lieu et les serveurs peuvent être localisés dans le monde entier. Certaines obligations, telles que celles liées à la résilience, encouragent d'ailleurs les fournisseurs de *cloud* à effectuer des copies des données dans des serveurs situés sur plusieurs territoires. Pourtant, et en dépit de ces difficultés, les fournisseurs de *cloud* ont diversifié leurs offres afin d'offrir des services localisés dans certaines régions identifiées dans le contrat de *cloud*<sup>40</sup>. Les fournisseurs ouvrent des *data centers* (centres de données) dans de nombreuses régions du monde, non seulement en réponse aux obligations liées à la localisation des données, mais aussi pour être territorialement proches de leurs clients (et ainsi garantir des temps d'accès aux données réduits).

Dans tous les cas, il semble que ces obligations légales de localisation se diffusent de plus en plus largement, sans toutefois que leurs effets réels soient toujours convaincants pour la protection des personnes et de leurs données.

Pour autant, il reste fréquent que le *cloud* se trouve au-delà du territoire du client. Dans ce cas, d'autres difficultés juridiques peuvent alors survenir.

### III. Le *Cloud* au-delà du territoire

#### A. Observations introductives

Il est courant de penser que ce qui est hors de notre portée est difficile à contrôler. Pour mieux connaître et contrôler les risques liés aux choix technologiques effectués par les entreprises, les autorités nationales ont imposé des règles encadrant les transferts de certaines données en dehors de leurs frontières (B). Il arrive aussi que des États adoptent des règles afin de se réserver

<sup>39</sup> PANDAY/MALCOLM, p. 515 s.

<sup>40</sup> Par exemple, *Amazon* (AWS), *Cloudflare*, *Google*, *Microsoft* (*Azure*) offrent la possibilité de choisir spécifiquement les régions dans lesquelles les clients souhaitent que leurs données soient conservées.

des accès aux données, et cela quel que soit le territoire sur lequel les données se trouvent (C).

## **B. Les règles encadrant les transferts de données au-delà du territoire**

La plupart des lois réglementant les traitements de données personnelles ont encadré les transferts de données en dehors de leurs territoires. Par exemple, la loi française relative à l'informatique et aux libertés de 1978<sup>41</sup>, la Convention 108 du Conseil de l'Europe de 1981<sup>42</sup> ou la LPD de 1992<sup>43</sup> reconnaissaient déjà de tels principes. La directive européenne de 1995 sur la protection des données avait, quant à elle, dédié un chapitre entier aux transferts des données en dehors des frontières de l'Union. Le principe consacré était celui de la confiance entre les États membres, matérialisé par la libre circulation des données sur le territoire européen, et celui de la défiance pour les États tiers, matérialisé par des restrictions juridiques interdisant en principe les transferts en dehors des frontières européennes. Ces transferts n'étaient permis que dans des cas clairement définis, notamment si « *le pays tiers en question assure un niveau de protection adéquat* » ou si le responsable du traitement, situé dans le pays tiers, « *offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes* »<sup>44</sup>. Ces principes ont été repris par le Règlement européen sur la protection des données<sup>45</sup> et se retrouvent aussi dans d'autres lois nationales de protection des données, telles que la LPD<sup>46</sup>. Ces règles ont un impact important pour les acteurs du *cloud* qui devront faire des choix informés avant de décider de l'ouverture de nouveaux serveurs sur d'autres territoires.

---

<sup>41</sup> Art. 24 de la loi 78-17 relative à l'informatique, aux fichiers et aux libertés (France) du 6 janvier 1978.

<sup>42</sup> Chapitre III de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Conseil de l'Europe) du 28 janvier 1981.

<sup>43</sup> Art. 6 de la Loi fédérale du 19 juin 1992 sur la protection des données (LPD), FF 1988 II 421.

<sup>44</sup> Art. 25 s. de la Directive 95/46 du Parlement européen et du Conseil du 25 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, JO L 281 du 23 novembre 1995, p. 31.

<sup>45</sup> Art. 44 s. du Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, JO L 119 du 4 mai 2016, p. 1.

<sup>46</sup> Art. 6 LPD.

D'apparence assez stricte, la mise en œuvre de ces règles s'est révélée plutôt favorable aux traitements transfrontaliers<sup>47</sup>. Dès 2000, la Commission européenne a ainsi reconnu les États-Unis comme un territoire présentant un niveau de protection adéquat<sup>48</sup> permettant ainsi d'effectuer des transferts vers ce pays. Les experts en protection des données savent que cette décision d'adéquation (*Safe Harbor*), ainsi que celle qui l'a remplacée (*Privacy Shield*), ont été successivement annulées par la Cour de justice de l'Union européenne en 2015<sup>49</sup> et en 2020<sup>50</sup>, générant une grande insécurité juridique pour les entreprises américaines se fondant sur ce mécanisme juridique de transfert. Les accords suisses avec les États-Unis (*Safe Harbor* et *Privacy Shield*) ont subi un sort similaire.

En mars 2022, la Commission européenne et les États-Unis ont toutefois annoncé avoir trouvé un nouvel accord de principe pour justifier les flux de données vers les États-Unis sur le fondement d'une nouvelle décision d'adéquation (*Trans-Atlantic Data Privacy Framework*). Bien que le texte juridique n'ait pas été rendu public à ce jour, la principale nouveauté du cadre juridique proposé est liée à la reconnaissance d'une voie de recours sur le territoire américain<sup>51</sup>. L'annonce de cet accord a été accueillie très favorablement par les grands acteurs américains du *cloud*, particulièrement *Google* et *Microsoft*. Ces instruments juridiques sont importants puisqu'ils témoignent d'une relation de confiance entre les pays et contribuent à une meilleure sécurité juridique pour les acteurs internationaux. Pour autant, l'indulgence européenne ne doit pas se transformer en complaisance, et il sera essentiel que la Commission européenne s'assure non seulement du respect des principes par les entreprises situées aux États-Unis, mais aussi de la mise en place de mécanismes de contrôle stricts sur le territoire américain<sup>52</sup>.

En sus de ces obligations liées aux données personnelles, d'autres secteurs d'activité posent également certaines contraintes en cas de transferts internationaux. Par exemple, le secteur bancaire est strictement régulé en Suisse, et des règles spécifiques sont applicables aux banques et aux sociétés d'assurance lorsqu'elles utilisent des prestataires externes. Dans une circulaire de 2018<sup>53</sup>, l'Autorité fédérale de surveillance des marchés financiers (FINMA) a introduit

<sup>47</sup> Pour certains textes, telle que la Convention 108, leur objet était précisément d'organiser la circulation des données entre les territoires offrant des protections adéquates.

<sup>48</sup> Commission européenne, décision 2000/520 du 26 juillet 2000.

<sup>49</sup> CJUE, affaire C-362/14, du 6 octobre 2015, *Maximilian Schrems contre Data Protection Commissioner*, ECLI:EU:C:2015:650.

<sup>50</sup> CJUE, affaire C-311/18, du 16 juillet 2020, *Data Protection Commissioner contre Facebook Ireland Ltd et Maximilian Schrems*, ECLI:EU:C:2020:559.

<sup>51</sup> Commission européenne, *Trans-Atlantic Data Privacy Framework*, 15 mars 2022.

<sup>52</sup> Voir dans ce sens, EDPB, *Statement 01/2022*, 6 avril 2022.

<sup>53</sup> FINMA, *Circulaire 2018/3 remplaçant FINMA, Circulaire 2008/7*.

des recommandations en cas d'externalisation. Selon cette circulaire, les transferts de données à l'étranger ne sont autorisés que si l'entreprise (le client) peut « *expressément garantir qu'elle-même, sa société d'audit ainsi que la FINMA peuvent exercer et faire appliquer leurs droits de regard et d'examen* ». Cela passe notamment par le fait de garantir, à tout moment, un accès aux informations nécessaires depuis la Suisse. Cela ne devrait pas poser de problème particulier puisqu'un tel accès délocalisé est justement l'une des particularités des services de *cloud*. Pour autant, certains commentateurs pourraient qualifier ces accès comme une forme d'application extraterritoriale du droit suisse. Il arrive ainsi que les autorités de certains pays s'arrogent un pouvoir d'accès aux données situées en dehors de leur territoire.

### **C. Les règles octroyant des accès aux données au-delà du territoire (*CLOUD Act, e-evidence*)**

La mondialisation des échanges et la normalisation des transferts de biens et de personnes ont engendré d'importantes évolutions dans le domaine juridique. En principe, comme nous l'avons vu, le critère utilisé pour déterminer la compétence législative et juridictionnelle est celui de la localisation matérielle. Cette localisation peut notamment être celle du sujet de droit, celle du client utilisateur ou celle du fournisseur de *cloud*. Chaque situation pouvant présenter des particularités, il faudra donc être attentif à la compétence territoriale et à l'application des dispositions impératives de chaque territoire.

Dans le domaine pénal, l'articulation entre les différents droits nationaux applicables s'est rapidement révélée complexe. La massification des flux internationaux de données a en effet créé de nouvelles difficultés pour les enquêteurs. Ces derniers souhaitent souvent accéder à des preuves localisées à l'étranger et dispersées à travers plusieurs États, ce qui rend particulièrement difficile leur reconstitution. Il est effectivement de plus en plus fréquent que les enquêteurs aient besoin d'accéder à des preuves situées sur d'autres territoires, comme les informations liées à un compte d'utilisateur ou les courriels d'une personne. Afin de permettre de tels accès, un nombre croissant de pays ont signé, à partir des années 1970, des traités bilatéraux et multinationaux d'entraide judiciaire (les *Mutual Legal Assistance Treaties*, MLAT). Ces traités fournissent un cadre juridique en matière d'accès et d'utilisation des preuves situées sur un autre territoire. Bien que nécessaires, ces traités se sont révélés trop complexes dans leur mise en œuvre et souvent inadaptés à l'ère numérique<sup>54</sup>. L'utilisation généralisée du *cloud* dont la caractéristique est de proposer des services transfrontières a augmenté la frustration des autorités d'enquête qui doivent, le plus

---

<sup>54</sup> SWIRE/HEMMINGS/VERGNOLLE, p. 324 s.

souvent, passer par des procédures juridiques longues et complexes alors même qu'un accès à distance est possible.

Par ailleurs, les fournisseurs de services se sont parfois retrouvés dans des situations juridiques inextricables. D'un côté, le droit de l'État dans lequel leur client se trouve empêchait la divulgation de données à un État tiers, sans passer par les mécanismes de la coopération judiciaire. De l'autre, le droit de l'État de leur siège social leur imposait de collaborer avec les autorités d'enquête nationale, en dehors des règles de la coopération judiciaire. Plusieurs affaires, notamment liées à *Yahoo!*<sup>55</sup> ou *Microsoft*<sup>56</sup>, ont illustré l'étendue de ces difficultés. Dans les deux cas, les autorités nationales (belges et américaines) avaient respectivement requis *Yahoo!* et *Microsoft* de leur communiquer des informations stockées sur des serveurs basés à l'étranger (respectivement aux États-Unis et en Irlande). Les deux entreprises avaient contesté ces réquisitions en demandant aux autorités nationales de passer par les mécanismes de l'entraide judiciaire<sup>57</sup>. *Yahoo!* avait été condamné à une amende d'un montant de 44'000 euros en Belgique pour ne pas avoir communiqué les informations aux autorités belges. Quant à l'affaire *Microsoft*, elle a conduit le Congrès américain à adopter le *Clarifying Lawful Overseas Use of Data Act* (également connu sous l'acronyme *CLOUD Act*) en mars 2018<sup>58</sup>.

Le *CLOUD Act* a eu deux apports principaux. D'abord, il a ouvert la possibilité pour les États d'adopter des procédures simplifiées de coopération judiciaire internationale, plus adaptées au monde numérique<sup>59</sup>. Ensuite, il a reconnu explicitement la compétence des autorités américaines, dans le cadre d'enquêtes pénales ou administratives diligentées pour des infractions graves, d'accéder à des données, et ce quel que soit le lieu où celles-ci sont conservées (sur ou en dehors du territoire américain)<sup>60</sup>. Les demandes d'accès peuvent être adressées aux personnes soumises à la compétence américaine. Selon une jurisprudence constante, les juridictions américaines interprètent cette notion de compétence selon deux niveaux :

- une compétence générale, typiquement lorsque l'organisation a son siège social ou a été constituée aux États-Unis ;

<sup>55</sup> Cour de cassation belge, 1<sup>er</sup> décembre 2015, P.13.2082.N.

<sup>56</sup> U.S. Court of Appeals, Second Circuit, 14 juillet 2016, *Microsoft Corporation v United States of America*, 138 S. Ct. 1186 (2018).

<sup>57</sup> VERGNOLLE, p. 216 s. Voir aussi TF, arrêt 6B\_216/2020 du 1<sup>er</sup> novembre 2021.

<sup>58</sup> BERENGAUT/GOODLOE.

<sup>59</sup> SWIRE/DASKAL. Voir aussi la page du site du Department of Justice intitulée *Cloud Act Resources*.

<sup>60</sup> 18 U.S.C. § 2713.

- une compétence spéciale, laquelle requiert une analyse factuelle afin de déterminer si l'organisation a suffisamment de liens avec les États-Unis<sup>61</sup>.

La compétence spéciale laisse une place importante à l'interprétation et génère une certaine incertitude quant à l'étendue exacte des pouvoirs reconnus aux autorités d'enquête américaines vis-à-vis d'entreprises étrangères<sup>62</sup>. En pratique, il semble que la compétence spéciale sera reconnue dans de nombreux cas dès lors que les juridictions américaines ont déjà reconnu qu'un « simple acte » en lien avec les États-Unis permet de reconnaître une telle compétence, tant qu'il crée « une connexion substantielle »<sup>63</sup>. Selon une lecture littérale de ces critères, il est donc parfaitement envisageable qu'un fournisseur de *cloud* suisse ou européen ayant une présence aux États-Unis puisse être soumis à ces règles et soit obligé de fournir les données situées en Suisse mais accessibles depuis le territoire américain. Il sera alors particulièrement difficile pour le fournisseur de *cloud* de réconcilier cette obligation avec l'interdiction posée par l'article 271 du Code pénal suisse, lequel prévoit que « celui qui, sans y être autorisé, aura procédé sur le territoire suisse pour un État étranger à des actes qui relèvent des pouvoirs publics [...] sera puni d'une peine privative de liberté [...] ou d'une peine pécuniaire ». D'autant qu'aux demandes des autorités pénales peuvent également s'ajouter les accès par les services de renseignements.

Bien entendu, le *CLOUD Act* prévoit des critères encadrant les motifs pour lesquels ces demandes peuvent être effectuées ainsi que les standards permettant de justifier de tels accès<sup>64</sup>. Il demeure que ce texte a apporté d'importantes incertitudes et a généré une certaine défiance à l'égard des autorités américaines.

Les États-Unis ne sont pas le seul pays ayant des règles produisant des effets au-delà de ses frontières territoriales<sup>65</sup>. Certaines dispositions du Règlement européen sur la protection des données ont également été qualifiées comme ayant des effets extraterritoriaux<sup>66</sup>. Ce texte a d'ailleurs été suivi très rapidement d'une proposition de règlement européen relatif aux preuves électroniques (projet « *e-evidence* »<sup>67</sup>), dont les dispositions sont similaires à celles du *CLOUD Act*<sup>68</sup>. Introduite en 2018, la proposition de règlement est toujours en cours de négociation.

---

<sup>61</sup> BERENGAUT/GOODLOE.

<sup>62</sup> DAVIS/GUNKA, p. 52 s. Pour plus de précisions, voir Department of Justice, White Paper, p. 8.

<sup>63</sup> U.S. Supreme Court, *Burger King Corp. c. Rudzewicz*, p. 475 s.

<sup>64</sup> SWIRE/DASKAL.

<sup>65</sup> DAVIS/GUNKA, p. 55 s. ; TRIMBLE, p. 3.

<sup>66</sup> HERT/CZERNIAWSKI, p. 231.

<sup>67</sup> Commission européenne, Proposition de Règlement 2018/0108 du 17 avril 2018 relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale.

<sup>68</sup> BISMUTH, p. 681.

L'utilisation croissante des services numériques et du *cloud* renouvelle la conception de la compétence territoriale. Il y a fort à parier que les États vont continuer de se reconnaître la possibilité d'accéder non seulement aux données situées matériellement sur leur territoire, mais également à celles qui sont accessibles depuis leur territoire.

#### IV. Observations conclusives

Si le territoire a longtemps marqué les contours de la délimitation de la compétence des États, le numérique semble avoir remis en cause, ou du moins renouvelé, cette vision traditionnelle. Il est vrai que la structure du *cloud*, notamment du fait de ses rattachements multiterritoriaux, a tendance à éprouver la définition statique du territoire. Le *cloud* et le territoire entretiennent donc des rapports complexes.

Pour préserver leur souveraineté, les États ont adopté des mesures politiques et législatives pour rétablir une territorialisation du numérique et des données. Ces mesures présentent de nombreuses limites, et des problèmes d'articulation entre les différentes normes nationales existent. Certains États ont en effet édicté des règles qui s'imposent aux entreprises et entrent parfois en contradiction avec celles d'autres États. Les entreprises se retrouvent alors dans des situations inextricables dans lesquelles, quelle que soit leur action, elles seront en violation du droit d'au moins un État.

Dès lors, il faut se demander si la technique ne peut pas contribuer à apporter quelques pistes de simplification. Actuellement, des entreprises mettent en place du chiffrement des données de bout en bout, c'est-à-dire non seulement lors du transport des données mais aussi lorsqu'elles se trouvent dans le *cloud*. Ces entreprises conservent ainsi sur leurs serveurs des données chiffrées pour lesquelles elles n'ont pas les clés de déchiffrement. Elles sont donc incapables de déchiffrer les données ou de les communiquer en clair à des tiers. Avec les développements dans le domaine du chiffrement homomorphe, il sera bientôt possible d'effectuer, dans le *cloud*, des traitements plus complexes sur ces données chiffrées, garantissant ainsi une meilleure confidentialité et sécurité des données<sup>69</sup>. De telles solutions diminuent le nombre de droits applicables puisque le nombre de personnes ayant accès aux données en clair est moins élevé, réduisant donc nécessairement le nombre de personnes auxquelles des réquisitions peuvent être adressées. Une difficulté persiste : celle de savoir sur quel territoire le client va conserver les clés de déchiffrement dès lors que le droit de cet État trouvera à s'appliquer.

---

<sup>69</sup> BRADLEY.

Si les doutes entourant les questions juridiques relatives au *cloud* et au territoire laissent parfois penser que le nuage est noir, il ne faut pas oublier qu'une de ses faces reste orientée vers le soleil et que des solutions pourront toujours être trouvées.

## V. Bibliographie

### A. Littérature

**Juliette ANCELLE/Karim FERDJANI**, Les contrats informatiques, in Alexandre RICHA/Damiano CANAPA (éds), *Droit et économie numérique*, CEDIDAC, 2021, vol. 73, p. 131 ss ; **Mathieu BOURGEOIS/Marion MOINE**, CLOUD COMPUTING. – Cloud et protection des données à caractère personnel, *JurisClasseur Communication*, Fascicule 961, 1<sup>er</sup> mai 2020 ; **Alexander BERENGAUT/Katherine GOODLOE**, Reaching for the CLOUD, in *Global Data Review*, 2019 ; **Régis BISMUTH**, Le Cloud Act face au projet européen e-evidence : confrontation ou coopération ?, in *Revue critique de droit international privé*, 2019, p. 681 ss ; **Jeremy BRADLEY**, The (r)Evolution of FHE, in *Zama*, 2022 ; **Dominique CARREAU/Fabrizio MARRELLA**, *Droit international*, Pedone, 2012 ; **Anupam CHANDER/Uyên LÊ**, Data nationalism, in *Emory Law Journal*, 2015, vol. 64, p. 677 ss ; **Nigel CORY/Luke DASCOLI**, How barriers to cross-border data flows are spreading globally, what they cost, and how to address them, *Information Technology & Innovation Foundation*, 2021 ; **Frederick DAVIS/Charlotte GUNKA**, Perquisitionner les nuages – *CLOUD Act*, souveraineté européenne et accès à la preuve dans l'espace pénal numérique, in *Revue critique de droit international privé*, 2021, p. 43 ss ; **Alexis FITZJEAN Ó COBHTHAIGH**, Le cloud et la souveraineté numérique dans le nouveau monde, in *Revue pratique de la prospective et de l'innovation*, 2021, n° 1, p. 16 ss ; **Solange GHERNAOUTI/Christian AGHROUM**, Cyber-résilience, risques et dépendances : pour une nouvelle approche de la cyber-sécurité, in *Sécurité et stratégie*, 2012, vol. 4, p. 74 ss ; **Jack GOLDSMITH**, The Internet and the Abiding Significance of Territorial Sovereignty, in *Indiana Journal of Global Legal Studies*, 1998, vol. 5, p. 475 ss ; **Nicolas GREVET**, *Le cloud computing : évolution ou révolution ? Pourquoi, quand, comment et surtout faut-il prendre le risque ?*, Mémoire de recherche, Cergy-Pointoise, 2009 ; **Paul DE HERT/Michal CZERNIAWSKI**, Expanding the European data protection scope beyond territory : Article 3 of the General Data Protection Regulation in its wider context, in *International Data Privacy Law*, 2016, vol. 6, p. 230 ss ; **Jerzy KRANZ**, Notion de souveraineté et le droit international, in *Archiv des Völkerrechts*, vol. 30, n° 4, 1992, p. 411 ss ; **Michael MONTAVON**, L'externalisation du traitement de données dans le *cloud*, in *Cyberadministration et protection des données*, Schultess, 2021, p. 457 ss ; **Jérémie MÜLLER**, For et droit pénal applicable au *cloud computing*, in *ForumPoenale*, Stämpfli, 2013, p. 306 ss ; **Jyoti PANDAY/Jeremy MALCOLM**, The political economy of data localization, in *The open journal of sociopolitical studies*, 2018, vol. 4, p. 511 ss ; **Isabelle SCHERRER**, Internet, un réseau sans frontière ? Le cas de la frontière franco-belge, in *Annales de géographie*, 2005, n° 645, p. 471 ss ; **David ROSENTHAL/Samira STUDER**, La nouvelle loi sur la protection des données, in *Jusletter*, 16 novembre 2020 ; **Peter SWIRE/Jennifer DASKAL**, Frequently asked questions about the U.S. CLOUD Act, 2019 ; **Peter SWIRE/Justin HEMMINGS/Suzanne VERGNOLLE**, A mutual legal assistance case study : the United States and France, in *Wisconsin International Law Journal*, 2017, vol. 34, p. 324 ss ; **Marketa TRIMBLE**, Extraterritorial



Enforcement of National Laws in Connection with Online Commercial Activity, in John ROTHCHILD (éd), Research handbook on electronic commerce law, Edward Elgar, 2016 ; **Suzanne VERGNOLLE**, Understanding the French criminal justice system as a tool for reforming international legal cooperation and cross-border data requests, in Data Protection, Privacy and European Regulation in the Digital Age, University Press of Helsinki, 2016, p. 205 ss.

## B. Documents officiels

**CNIL**, « Définition de Cloud Computing », <<https://www.cnil.fr/fr/definition/cloud-computing>> (consulté le 5 juin 2022) ; **Commission européenne**, Trans-Atlantic Data Privacy Framework, mars 2022, <<https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf>> (consulté le 5 juin 2022) ; **Conseil Fédéral**, Communiqué « Le Conseil Fédéral commande une étude sur la faisabilité d'un « Swiss Cloud » », 16 avril 2020 ; **Commission européenne**, Décision 2000/520 du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique ; **Département fédéral des finances, UPIC**, Rapport sur l'évaluation des besoins d'un nuage informatique suisse (« Swiss Cloud »), décembre 2020 ; **Department of Justice (DOJ)**, White Paper, Promoting Public Safety, Privacy, and the Rule of Law Around the World : The Purpose and Impact of the CLOUD Act, avril 2019 ; **Department of Justice (DOJ)**, CLOUD Act Resources, <<https://www.justice.gov/dag/cloudact>> (consulté le 5 juin 2022) ; **EDPB**, Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework, 6 avril 2022 ; **FINMA**, Circulaire 2018/3 sur les externalisations dans le secteur des banques, des entreprises d'assurance et de certains établissements financiers au sens de la LEFin, entrée en vigueur le 1<sup>er</sup> avril 2018 ; **Ministère français de l'Europe et des affaires étrangères, ministère de l'économie, des finances et de la relance et secrétariat d'État chargé de la transition numérique et des communications électroniques sur la souveraineté numérique de l'Union européenne**, Communiqué conjoint du 7 février 2022 ; **Ministère français de l'économie et des finances et Commissaire européen au marché intérieur, sur la souveraineté numérique et la stratégie industrielle de l'Union européenne**, Déclarations du 7 février 2020 ; **Ministère français de l'intérieur et de la culture**, Note d'information du 5 avril 2016 relative à l'informatique en nuage (*cloud computing*) ; **Franck MONTAUGÉ/Gérard LONGUET**, Rapport sur la souveraineté numérique, Sénat Français, n° 7, 2019 ; **Préposé fédéral à la protection des données et à la transparence (PFPDT)**, Explications concernant l'informatique en nuage (*cloud computing*) ; **Premier ministre français** François Fillon, Discours sur le thème du très haut débit et l'économie numérique, Vélizy, 18 janvier 2010 ; **Cédric VILLANI**, Donner un sens à l'intelligence artificielle. Pour une stratégie nationale européenne, 2018 ; **Ursula VON DER LEYEN**, A Union that strives for more. My agenda for Europe, Political guidelines for the next European Commission 2019-2024, 2019.

