Collection lausannoise
CEDIDAC

Sylvain Métille
(éditeur)

L'informatique en nuage

Stämpfli Editions

Collection lausannoise
CEDIDAC

Sylvain Métille
(éditeur)

L'informatique en nuage

Collection lausannoise
CEDIDAC

Volume 90

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 continuée 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

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.

Print ISBN 978-3-7272-4456-8

Dans notre librairie en ligne www.staempflishop.com,
la version suivante est également disponible :

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

printed in
switzerland

FSC
www.fsc.org
MIXTE
Papier | Pour une gestion forestière responsable
FSC® C016087

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

Avant-propos ..... **V**

Table des principales abréviations ..... **XI**

Contrats *cloud* : qualification, gestion des données et sortie de la relation **1**
Alexandre Jotterand

L'utilisation de services *cloud* par des responsables du traitement privés **35**
Philipp Fischer
Sébastien Pittet

Überlegungen zu Recht und Risiko bei behördlicher Cloudnutzung **83**
Daniel Dzamko-Locher

L'informatique en nuage à l'État de Vaud – État des lieux, enjeux et solutions **119**
Nicolas Savoy
Mélanie Garcia
Ludivine Epiney
Catherine Pugin

Le Code de conduite CISPE des fournisseurs d'infrastructures Cloud relatif à la protection des données **201**
Aurélien Rocher

Le dossier électronique du patient : révolution ou désillusion ? **219**
Frédéric Erard

***Cloud* et territoire** **243**
Suzanne Vergnolle

Table des principales abréviations

a.a.O	*am angegebenen Ort*
Abs.	*Absatz*
ACV	Administration cantonale vaudoise
ad art./par.	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	*Aktuelle Juristische Praxis*
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	*Application Programming Interface*
Art.	*Artikel*
art.	Article
ASB	Association suisse des banquiers
ASP	*Application Service Provider*
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
AWS	*Amazon Web Services*
B2C	*Business to Consumer*
BBl	*Bundesblatt*
BCR	*Binding Corporate Rules*
BGE	*Bundesgerichtsentscheid*
BGer	*Schweizerisches Bundesgericht*
BGÖ	*Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung, SR 152.3*
BJ	*Bundesamt für Justiz*
BLV	Base législative vaudoise
BO CE	Bulletin officiel du Conseil des États
BO CN	Bulletin officiel du Conseil national

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

CLOUD	*Clarifying Lawful Overseas Use of Data*
CLOUD Act	*Clarifying Lawful Overseas Use of Data Act*
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.	*Corporation*
CP	Code pénal suisse du 21 décembre 1937, RS 311.0
CSA	*Cloud Security Alliance*
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	*Comma-separated values*
CyrV	*Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung, SR 120.73*
d.h.	*das heißt*
DaaS	*Desktop as a Service*
DBaaS	*Database as a Service*
DBG	*Bundesgesetz vom 14. Dezember 1990 über die direkte Bundessteuer, SR 642.11*
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	*Department of Justice* (États-Unis d'Amérique)
DRP	*Disaster Recovery Plan*
DSFA	*Datenschutz-Folgenabschätzung*
DSG	*Bundesgesetz vom 19. Juni 1992 über den Datenschutz, SR 235.1*
DSGVO	*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*
E.	*Erwägungsgrund*
e.g.	*Exempli gratia*

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

GDPR	*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.*
GE	Canton de Genève
GEVER-Verordnung	*Verordnung vom 3. April 2019 über die elektronische Geschäftsverwaltung in der Bundesverwaltung, SR 172.010.441*
ggf.	*Gegebenenfalls*
grds.	*Grundsätzlich*
Hinw.	*Hinweis*
HK	*HandKommentar*
Hrsg.	*Herausgeber*
HYOK	*Hold Your Own Key*
i.e.	*id est,* c'est-à-dire
i.e.S.	*Im engeren Sinne*
i.K.	*Inkrafttreten*
i.S.	*Im Sinne*
i.S.v.	*Im Sinne von*
i.V.m.	*In Verbindung mit*
IaaS	*Infrastructure as a Service*
IAPP	*International Association of Privacy Professionals*
Ibid.	*Ibidem*, même endroit
IBM	*International Business Machines Corporation*
ID	*Identification*
IDG	*Informations- und Datenschutzgesetz des Kanton Zürich*
IKS	*Internes Kontrollsystem*
IKT	*Informations- und Kommunikationstechnik*
in	dans
in fine (*i.f.*)	à la fin
infra	plus bas
inkl.	*inklusive*
insbes.	*Insbesondere*
IP	*Internet Protocol*
ISB	*Informatiksteuerungsorgan des Bundes*

ISchV	*Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes, SR 510.411*
ISG	*Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund, BBl 2017 3077*
ISO	*International Organization for Standardization*
ITSL	*Center for Information Technology, Society, and Law*
JCP	Juris-Classeur Périodique
JdT	Journal des tribunaux
JO L	Journal officiel de l'Union européenne
JSON	*JavaScript Object Notation*
JU	Canton du Jura
KPI	*Key Performance Indikator*
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	*Lecture Notes in Computer Science*
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	*Life Science Recht*
m.E.	*meines Erachtens*
MLAT	*Mutual Legal Assistance Treaties*
N	Numéro(s) marginaux
N°/n°/n./No/no/Nr.	Numéro
NB	*Nota bene*
nDSG	*Bundesgesetz vom 25. September 2020 über den Datenschutz, Inkrafttreten am 1. September 2023, BBl 2020 7639*
NIST	*National Institute of Standards and Technology*
nLPD	Loi fédérale du 25 septembre 2020 sur la protection des données, entrée en vigueur le 1er septembre 2023, FF 2020 7397
NOYB	*None Of Your Business*
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
PaaS	*Platform as a Service*
par.	Paragraphe(s)
PCA	Plan de continuité des activités
PDF	*Portable Document Format*
PFPDT	Préposé fédéral à la protection des données et à la transparence
PII	*Personal Identifiable Information*

PIIEC	Projet important d'intérêt européen commun
PJA	Pratique juridique actuelle
PK	*Praxiskommentar*
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.	*Public Law number*
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	*Regierungsratsbeschluss*
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	*Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997, SR 172.010*
RVOV	*Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998, SR 172.010.1*
Rz.	*Randziffer*
S.	*Seite*

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

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

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

I. Introduction 219

II. Caractéristiques et fonctionnement du DEP 221
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

III. Questions choisies 231
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

IV. Conclusion 240

V. Bibliographie 241
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[1]. 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[2]. L'adoption en 2015 de la LDEP[3] – 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)[4] 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

1 Conseil fédéral, Stratégie 2030, p. 12 ss.
2 Office fédéral de la santé publique, Stratégie Cybersanté (eHealth) Suisse, 27 juin 2007, p. 3.
3 Loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP), RS 816.1.
4 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[5].

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[6]. 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[7].

---

5 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.

6 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.

7 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[8].

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[9]. 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[10]. 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)[11]. 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)[12]. Les art. 9 à 12 ODEP[13] 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[14]. Sept communautés

8 Message LDEP 2013, FF 2013 4747, p. 4757 s.
9 Art. 10 al. 1 LDEP.
10 Message LDEP 2013, FF 2013 4747, p. 4763 ; SPRECHER/HOFER, p. 53.
11 Art. 10 al. 2 LDEP.
12 SPRECHER/HOFER, p. 55.
13 Ordonnance du 27 mars 2017 sur le dossier électronique du patient (ODEP), RS 816.11.
14 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)[15]. 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[16]. 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[17].

C. Caractère facultatif

1. Pour les patients

L'ouverture d'un DEP requiert le consentement du patient et est donc purement facultative[18]. 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[19].

---

15 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).

16 WIDMER, Das elektronische Patientendossier, p. 770.

17 WIDMER, Das elektronische Patientendossier, p. 769 ; SPRECHER/HOFER, p. 59 ; ERARD, Le secret médical, N 169.

18 Art. 3 al. 1 LDEP.

19 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. 19*c* CC. Ces actes peuvent ainsi être valablement opérés par un mineur agissant seul à la condition qu'il soit capable de discernement[20]. 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[21]. 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'inaptitude (art. 360 ss CC) et prend alors effet lorsque les conditions légales sont réunies (p. ex. incapacité de discernement pour les directives anticipées)[22]. 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*[23], 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[24]. 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

20 eHealth Suisse, Représentation dans le cadre du DEP, p. 11.

21 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.

22 eHealth Suisse, Représentation dans le cadre du DEP, p. 22 s.

23 eHealth Suisse, Représentation dans le cadre du DEP, p. 24 s.

24 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[25].

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 49*a* 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[26].

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 1er 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 1er 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[27]. Or, sans autre forme de précision légale, la

25 Conseil fédéral, Le Conseil fédéral veut développer davantage le dossier électronique du patient, communiqué de presse du 27 avril 2022.

26 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.

27 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[28]. 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'efficience 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)* »[29]. Les lignes directrices contiennent également un schéma d'aide à la décision pour établir si des informations sont pertinentes ou non pour le traitement[30]. 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[31]. 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[32], même si les établissements médicaux devraient adopter des directives institutionnelles à cet égard[33].

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[34]. 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 effectuées par les organes publics cantonaux (de surcroît dans le domaine de la santé) étant par principe soumis au droit cantonal de la protection des

28 Message LDEP 2013, p. 4797.
29 eHealth Suisse, Informations pertinentes, p. 7.
30 eHealth Suisse, Informations pertinentes, p. 10.
31 DONZALLAZ, N 6531 ss.
32 FELLMANN/ODERMATT, N 10.
33 FELLMANN/ODERMATT, N 11.
34 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* »[35].

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[36]. 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 1er 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[37]. 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[38].

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[39]. 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

35 V. en particulier l'intervention du rapporteur de la Commission du Conseil national Ignazio Cassis, BO (CN) 2015, p. 437.

36 SCHINDLER/TSCHUMI, N 24.

37 SCHINDLER/TSCHUMI, N 25.

38 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.

39 Art. 2 let. a LDEP.

alimenté par des applications mobiles de santé (*mHealth*)[40]. 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[41]. 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[42].

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[43]. 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* »[44]. 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[45].

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[46]. Le débiteur du droit du patient d'accéder aux données de son DEP est la communauté de référence à laquelle le patient est affilié[47]. Le droit d'accès direct du patient à ses informations médicales est en phase avec l'art. 25 al. 3 de la LPD

40 Pour une vue générale des travaux menés : <www.e-health-suisse.ch/fr/mise-en-oeuvre-communautes/activites-ehealth/mhealth.html> (*consulté le 7 mai 2022*).
41 ISLER, N 143.
42 Art. 23 let. c ODEP.
43 Art. 7 al. 1 LDEP.
44 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.
45 DONZALLAZ, N 6540.
46 Art. 8 al. 1 LDEP.
47 Art. 10 al. 2 let. B ch. 2 LDEP.

révisée (nLPD)[48] 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[49] 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[50], lequel ne peut en aucun cas être contraint de rendre ses données accessibles[51]. 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[52]. 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[53]. 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[54]. 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

48 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.
49 Loi fédérale sur la protection des données du 19 juin 1992 (LPD), RS 235.1.
50 Art. 9 al. 1 LDEP.
51 Art. 3 al. 4 LDEP.
52 Art. 2 al. 1 ODEP.
53 ERARD, Secret médical, N 175.
54 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[55].

Le patient peut attribuer différents niveaux de confidentialité aux documents de son DEP (normal, restreint ou secret)[56]. Par défaut, les données saisies dans le DEP ont un niveau de confidentialité « normal », sauf si le soignant en décide autrement[57]. 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 »[58]. Les données auxquelles le patient attribue un niveau de confidentialité « secret » sont uniquement accessibles par le patient[59].

En cas d'urgence, les professionnels de la santé peuvent accéder aux données du DEP de niveau « normal », même sans autorisation du patient[60]. 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[61]. Le patient doit en être informé dans un délai approprié après un accès en cas d'urgence par un professionnel de la santé[62].

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[63]. Les documents concernés sortent alors du champ de contrôle des règles applicables au DEP[64].

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[65]. Les données enregistrées par le patient lui-même sont quant à elles conservées sans limite

55 § 1.6 Annexe 2 de l'Ordonnance du DFI du 22 mars 2017 sur le dossier électronique du patient (ODEP-DFI), RS 816.111.
56 Art. 1 al. 1 ODEP.
57 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.
58 Office fédéral de la santé publique, Rapport explicatif ODEP, p. 10.
59 Office fédéral de la santé publique, Rapport explicatif ODEP, p. 10.
60 Art. 9 al. 5 LDEP ; art. 2 al. 2 ODEP.
61 Art. 4 let. e ODEP.
62 Art. 9 al. 5 LDEP ; art. 2 al. 2 ODEP.
63 WIDMER, Das elektronische Patientendossier, p. 772.
64 ERARD, Secret médical, N 183.
65 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[66]. La révocation n'est soumise à aucune forme et n'a pas à être motivée[67]. Dans ce cas, le DEP doit est 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)[68]. La déclaration de révocation du consentement est gérée par la communauté de référence auprès de laquelle le patient est affilié[69].

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[70].

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[71]. 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

66 Art. 3 al. 3 LDEP ; art. 21 al. 1 ODEP.
67 Message LDEP 2013, FF 2013 4747, p. 4800.
68 Message LDEP 2013, FF 2013 4747, p. 4800.
69 Message LDEP 2013, FF 2013 4747, p. 4801.
70 Art. 21 al. 2 ODEP.
71 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[72]. 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[73].

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.)[74]. 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[75].

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.

72 Message LDEP 2013, FF 2013 4747, p. 4796.
73 WIDMER, ePatientdossier, p. 162.
74 ERARD, Secret médical, N 875.
75 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[76]. 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[77]. Comme les communautés doivent également faire l'objet d'une certification[78], 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[79].

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[80].

Un regard attentif sur la LDEP montre que la Confédération a déduit ses compétences législatives des articles 95 al. 1 Cst. (activités économiques lucratives

---

76 Sur le partage délicat des compétences en matière de santé numérique, v. en particulier : SCHWEIZER, p. 205.

77 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.

78 Art. 11 ss LDEP.

79 Art. 2 al. 1 et Annexe 2 ODEP-DFI.

80 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* »[81].

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[82]. 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* »[83]. 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

81 Message LDEP 2013, FF 2013 4747, p. 4769.

82 Conseil fédéral, Le Conseil fédéral veut développer davantage le dossier électronique du patient, communiqué de presse du 27 avril 2022.

83 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[84]. 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[85].

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[86]. 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[87]. Pour être

84 Art. 10 al. 1 LDEP.
85 Art. 15 al. 1 ODEP.
86 P. ex. art. 5 let. j nLPD.
87 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[88]. 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. 10*a* 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[89]. 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[90]. 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

88 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).

89 JOTTERAND/ERARD, N 83.

90 WIDMER, Das elektronische Patientendossier, p. 770 ; SPRECHER/HOFER, p. 59.

l'art. 10*a* LPD (pour autant que la LPD s'applique à la personne ou l'entité qui externalise le traitement de données)[91]. 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[92] 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

91 WIDMER, Das elektronische Patientendossier, p. 770 ; SPRECHER/HOFER, p. 59.
92 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[93].

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 »[94]. Si l'on se rapporte au rapport WEHRLI[95], 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[96]. 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[97]. Les travaux préparatoires de la LDEP

93 § 4.9 Annexe 2 ODEP-DFI.
94 Conseil fédéral, Le Conseil fédéral veut développer davantage le dossier électronique du patient, communiqué de presse du 27 avril 2022.
95 Rapport WEHRLI, p. 5.
96 Rapport WEHRLI, p. 5.
97 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* »[98].

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[99]. Dans sa réponse, le Conseil fédéral a exposé qu'il convenait d'appliquer les prescriptions de la LRH[100] 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

98 Message LDEP 2013, FF 2013 4747, p. 4796.

99 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 nº 19.4136.

100 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[101].

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

[101] 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)[102]. 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> (*consulté le 7 mai 2022*) ; **Frédéric ERARD**, Le Conseil fédéral veut faire avancer le dossier électronique du patient,

[102] 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> (*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/communiques.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).