Collection lausannoise
CEDIDAC

Sylvain Métille
(éditeur)

Protection des données personnelles et recherche

Stämpfli Editions

Collection lausannoise
CEDIDAC

Sylvain Métille
(éditeur)

Protection des données personnelles et recherche

Collection lausannoise
CEDIDAC

Volume 97

Volumes 1 à 72 publiés dans la collection Recherches juridiques lausannoises

Sous-collection CEDIDAC (volume 120) 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

Protection des données personnelles et recherche

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.

www.staempfliverlag.com

Print ISBN 978-3-7272-8231-7

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

E-Book ISBN 978-3-7272-6361-3

printed in
switzerland

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

Avant-propos

Le présent ouvrage *Protection des données personnelles et recherche* est le troisième livre consacré à la protection des données personnelles que j'ai le plaisir de publier dans la Collection lausannoise après *Le droit d'accès* (2021) et *L'informatique en nuage* (2022). Il fait suite à la Journée CEDIDAC de la protection des données qui a eu lieu le 17 mars 2023 à Lausanne, même si les sujets abordés dans les sept contributions ne se recoupent que partiellement avec la conférence.

Les tensions entre les droits individuels (notamment le droit à l'autodétermination informationnelle et plus généralement le droit à la sphère privée), l'intérêt du chercheur et l'intérêt commun ou public ne sont pas qu'apparentes mais bien réelles. Quant à la liberté de choix de ceux que l'on appelle « les participants » dans le droit de la recherche (alors que l'on peut se demander s'ils prennent encore part à la recherche ou n'en sont finalement qu'un objet) et « les personnes concernées » dans le droit de la protection des données (leurs données personnelles font l'objet d'un traitement), elle n'est souvent qu'un leurre et ne peut pas justifier raisonnablement une atteinte à la sphère privée. Finalement, les données liées à la santé sont précieuses (pour la personne concernée comme pour le chercheur) et bien souvent uniques, ce qui rend une anonymisation impossible. Il faut donc plutôt admettre que la donnée est, et, restera personnelle (souvent pseudonymisée) avec les droits et obligations qui en découlent, notamment en matière de sécurité, plutôt que de feindre une anonymisation qui semble à première vue pratique mais représente en réalité des risques importants, à nouveau tant pour le chercheur que la personne concernée.

C'est donc sans grande surprise que presque tous les auteurs ont traité à un moment ou à un autre et avec plus ou moins de détails, de cette notion difficile et controversée de donnée anonyme. Plusieurs se sont intéressés également à la portée du privilège de la recherche.

FRÉDÉRIC ERARD dresse un panorama des règles applicables à la réutilisation des données personnelles dans le contexte de la recherche, ainsi que la relation entre les règles générales de la protection des données prévues par la Loi fédérale sur la protection des données (LPD) et la *lex specialis* qu'est la Loi fédérale relative à la recherche sur l'être humain (LRH), alors que RACHEL CHRISTINAT s'intéresse aux droits des personnes concernées par le traitement de leurs données personnelles et plus particulièrement les conditions du traitement de ces données, les moyens de vérification et les mesures judiciaires qu'elles peuvent engager.

VLADISLAVA TALANOVA, ALEXANDRE DOSCH, GÉRALDINE MARKS SULTAN et DOMINIQUE SPRUMONT abordent plus spécifiquement le droit d'opposition et le droit de consentent de la personne concernée, le consentement présumé et le rôle des commissions d'éthique de la recherche en particulier sous l'angle de l'autorisation de projets de recherches.

SAMAH POSSE présente le traitement de données personnelles avec une finalité de recherche particulière, soit le traitement à des fins statistiques, alors que VALENTIN CONRAD et TANIA GERMOND se penchent sur la valorisation des données de recherche notamment dans les domaines de l'intelligence artificielle, de la science ouverte et de la médecine personnalisée.

FABIAN LÜTZ montre les liens entre le droit de la protection des données personnelles et droit de la non-discrimination, notamment le rôle des chercheurs de la protection dès la conception et des analyses d'impact. Finalement, CÉCILE DE TERWANGNE analyse l'impact de la Stratégie européenne pour les données, en particulier la Directive 2019/1024 sur les données ouvertes et la réutilisation des données du secteur public, le Règlement sur la gouvernance des données et la Proposition de règlement sur les données (*Data Act*).

Je profite également de remercier chaleureusement les auteurs sans qui cet ouvrage n'existerait pas, ainsi que ENZO BASTIAN, assistant-doctorant au CEDIDAC pour sa relecture attentive et la mise en forme du présent ouvrage.

Bonne lecture !

Sylvain Métille

Sommaire

Table des principales abréviations

Abs.	*Absatz*
Aff.	Affaire
AI Act	Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (Législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM/2021/206 final.
al.	Alinéa
aLPD	Ancienne loi fédérale du 19 juin 1992 sur la protection des données, RS 235.1
AMM	Association médicale mondiale
API	*Application Programming Interface*
Art.	*Artikel*
art.	Article
ARWU	*Academic Ranking of World Universities*
ASP	*Application Service Provider*
ASSM	*Académie suisse des sciences médicales*
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
BAAI	*Beijing Academy of Artificial Intelligence*
BEUC	*Bureau européen des unions de consommateurs*
BLV	Base législative vaudoise
BNS	Banque nationale suisse
BSK	*Basler Kommentar*
BVGer	*Bundesverwaltungsgericht* (Allemagne)
c.	contre
c.-à-d.	C'est-à-dire
CARA	Association intercantonale regroupant les cantons de Genève, du Valais, de Vaud, de Fribourg et du Jura
CC	Code civil suisse du 10 décembre 1907, RS 210.
CdE	Conseil de l'Europe
CE	Commission européenne

CEDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950, RS 0.101
EDPB	Comité européen de la protection des données
CEPD	Contrôleur européen de la protection des données (Union européenne)
CEPF	Conseil des Écoles polytechniques fédérales
CER-VD	Commission vaudoise d'éthique de la recherche
CER(s)	Commission(s) d'éthique de la recherche
cf.	*confer*
CH	Suisse
ch.	Chiffre(s)
CHUV	Centre Hospitalier Universitaire Vaudois
CIOMS	*Council for International Organizations of Medical Sciences*
CJCE	Cour de justice des communautés européennes
CJUE	Cour de justice de l'Union Européenne
CLDN	Conférence latine des directeurs du numérique
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
CoE	*Council of Europe*
coll.	Collection
cons./c.	Considérant(s)
Convention 108	Convention du Conseil de l'Europe pour la protection des données à caractère personnel
Convention 108+	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel
CourEDH	Cour européenne des droits de l'Homme
CP	Code pénal suisse du 21 décembre 1937, RS 311.0
CPC	Code de procédure civile du 19 décembre 2008, RS 272

CPDT-JUNE	Convention intercantonale du 9 mai 2012 relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel, RS/NE 150.30
CPP	Code de procédure pénale suisse du 5 octobre 2007, RS 312.0.
CRU	Conseil de résolution unique (Union européenne)
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DGA	*Data Governance Act* - Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (Texte présentant de l'intérêt pour l'EEE), JO L 152 du 3.6.2022, p. 1 ss
Directive 2003/98	Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, JO L 345/90, 31.12.2003, p. 90 ss
Directive 2019/1024	Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, JO L 172/56, 2.6.2019, p. 56 ss
DMA	*Digital Market Act* – Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (Texte présentant de l'intérêt pour l'EEE), JO L 265 du 12.10.2022, p. 1 ss
DSA	*Digital Services Act* – Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022

	relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (Texte présentant de l'intérêt pour l'EEE), JO L 277 du 27.10.2022, p. 1 ss
DSG	*Bundesgesetz vom 19. Juni 1992 über den Datenschutz, SR 235.1*
e.g.	*Exempli gratia*
Eawag	Institut fédéral pour l'aménagement, l'épuration et la protection des eaux
EC	*European Commission*
éd.	Édition
éd/éds/édit.	Éditeur(s)
EDÖB	*Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter*
EDPB	*European Data Protection Board*
EDPL	*European Data Protection Law Review*
EDPS	*European Data Protection Supervisor*
EEE	Espace Économique Européen
ég.	Également
EHDS	*European Health Data Space*
ELI	*European Law Institute*
Empa	Laboratoire fédéral d'essai des matériaux et de recherche
EMRK	*Konvention zum Schutze der Menschenrechte und Grundfreiheiten, SR 0.101*
EMS	Établissements médico-sociaux
ENISA	*European Network and Information Security Agency*
EPF	Écoles polytechniques fédérales
EPFL	École polytechnique fédéral de Lausanne
et al.	*Et alii*
etc.	*et cætera*
ETHZ	*Eidgenössiche Technische Hochschule Zürich*
EU	*European Union*
EUREC	Association européenne des Commissions d'éthique de la recherche

ex.	Exemple
FAIR	*Findable*, *Accessible*, *Interoperable*, *Reusable*
FEKI	*Freiburger Ethik-Kommission International*
FF	Feuille fédérale
FNS	Fonds national suisse
FRA	*European Union Agency for Fundamental Rights*
HK	*HandKommentar*
HPV	Virus de papillome humain
Hrsg.	*Herausgeber*
HUG	Hopitaux Universitaires Genevois
i.e.	*Id est*
IA	Intelligence artificielle
ICESCR	*International Covenant on Economic, Social and Cultural Rights*
in	Dans
in fine (*i.f.*)	à la fin
infra	plus bas
IP	*Internet Protocol*
IPOT	Indice des prix de l'offre totale
ISO	*International Organization for Standardization*
JdT	Journal des tribunaux
JO L	Journal officiel de l'Union européenne
JORF	Journal officiel de la République française
JRC	*Joint Research Centre*
LACI	Loi fédérale du 25 juin 1982 sur l'assurance-chômage obligatoire et l'indemnité en cas d'insolvabilité, RS 837.0
LAGH	Loi fédérale du 15 juin 2018 relative à l'analyse génétique humaine, RS 810.12
LAr	Loi fédérale du 26 juin 1998 sur l'archivage, RS 152.1
LAsi	Loi fédérale du 26 juin 1998 sur l'asile, RS 142.31
LB	Loi fédérale du 8 novembre 1934 sur les banques et les caisses d'épargne, RS 952.0

LBN	Loi fédérale du 3 octobre 2003 sur la banque nationale suisse, RS 951.11
LEI	Loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration, RS 142.20
LEp	Loi fédérale du 28 septembre 2012 sur la lutte contre les maladies transmissibles de l'homme, RS 818.101
LERI	Loi fédérale du 14 décembre 2012 sur l'encouragement de la recherche et de l'innovation, RS 410.1
let.	Lettre
LGéo	Loi fédérale du 5 octobre 2007 sur la géoinformation, RS 510.62
LIDE	Loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises, RS 431.03
LIPAD	Loi cantonale genevoise sur l'information du public, l'accès aux documents et la protection des données personnelles, RS/GE A 2 08
LN	Loi fédérale du 20 juin 2014 sur la nationalité suisse, RS 141.0
LOGA	Loi fédérale du 21 mars 1997 sur l'organisation du gouvernement et de l'administration, RS 172.010
Loi sur les EPF	Loi fédérale du 4 octobre 1991 sur les écoles polytechniques fédérales, RS 414.110
LPD	Loi fédérale du 25 septembre 2020 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
LPMéd	Loi fédérale du 23 juin 2006 sur les professions médicales universitaires, RS 811.11
LPrD-VD	Loi cantonale vaudoise du 11 septembre 2007 sur la protection des données, BLV 172.65
LPSan	Loi fédérale du 30 septembre 2016 sur les professions de la santé, RS 811.21
LPsy	Loi fédérale du 18 mars 2011 sur les professions relevant du domaine de la psychologie, RS 935.81.
LRens	Loi fédérale du 25 septembre 2015 sur le renseignement, RS 121

LRH	Loi fédérale du 30 septembre 2011 relative à la recherche sur l'être humain, RS 810.30
LSF	Loi fédérale du 9 octobre 1992 sur la statistique fédérale, RS 431.01
LSI	Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération, RS 128
LTrans	Loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration, RS 152.3
N	Numéro(s) marginaux
N°/n°/n./No/no/Nr.	Numéro
NB	*Nota bene*
NIH	*National Institutes of Health*
not.	Notamment
OALSP	Ordonnance du 14 juin 1993 concernant les autorisations de lever le secret professionnel en matière de recherche médicale
OClin	Ordonnance fédérale du 20 septembre 2013 sur les essais cliniques, RS 810.305
OCPD	Ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données, RS 235.13.
OFJ	Office fédéral de la justice
OFS	Office fédéral de la statistiques
OFSP	Office fédéral de la santé publique
OICM	Office intercantonal de contrôle des médicaments
OIDE	Ordonnance du 26 janvier 2011 sur le numéro d'identification des entreprises, RS 431.031
OMC	Organisation mondiale du commerce
OMS	Organisation mondiale de la santé
OPDo	Ordonnance fédérale du 31 août 2022 sur la protection des données, RS 235.11.
ORD	*Open Research Data*
Ordonnance sur le recensement	Ordonnance du 19 décembre 2008 sur le recensement fédéral de la population, RS 431.112.1
Ordonnance sur les relevés statistiques	Ordonnance du 30 juin 1993 concernant l'exécution des relevés statistiques fédéraux, RS 431.012.1

OREE	Ordonnance du 30 juin 1993 sur le Registre des entreprises et des établissements, RS 431.903.
ORegBL	Ordonnance du 9 juin 2017 sur le Registre fédéral des bâtiments et des logements, RS 431.841
ORH	Ordonnance fédérale du 20 septembre 2013 relative à la recherche sur l'être humain, RS 810.301
p.	Page(s)
p. ex.	Par exemple
PA	Loi fédérale du 20 décembre 1968 sur la procédure administrative, RS 172.021
PaaS	*Platform as a Service*
par.	Paragraphe(s)
PFPDT	Préposé fédéral à la protection des données et à la transparence
PHRT	*Personalized Health and Related Technologies*
PSI	Institut Paul Scherrer
pt.	point
REE	Registre des entreprises et des établissements
RegBL	Registre fédéral des bâtiments et des logements
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) (texte présentant de l'intérêt pour l'EEE), JO L 119 du 4 mai 2016, p. 1 ss.
RO	Recueil officiel du droit fédéral
RS	Recueil systématique du droit fédéral
RS/GE	Recueil systématique genevois
RS/NE	Recueil systématique neuchâtelois
s.	Suivant(e)
SBP	*Swiss Biobanking Platform*
SEFRI	Secrétariat d'État à la formation, à la recherche et à l'innovation

SJ	Semaine judiciaire
SPHN	*Swiss Personalized Health Network*
ss.	Suivante(e)s
supra	au-dessus
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
THE	*Times Higher Education*
UE	Union européenne
UK	*United Kingdom*
UN	*United Nations*
UNIL	Université de Lausanne
unimedsuisse	Association Médecine Universitaire Suisse
*v/*v.	*Versus*
VD	Canton de Vaud
VIH	Virus de l'immunodéficience humaine
vol.	Volume
VwVG	*Verwaltungs-Vollstreckungsgesetz* (Allemagne)
WSL	Institut fédéral de recherches sur la forêt, la neige et le paysage

La protection des données dans la recherche

FRÉDÉRIC ERARD
Dr iur., avocat, CIPP/E, responsable du département légal et du transfert de technologie au SIB Institut Suisse de Bioinformatique, chargé de cours Unidistance

Table des matières

I. Introduction[1]

Les moyens technologiques déployés aujourd'hui pour observer, traquer, surveiller ou analyser les gestes et pensées des individus sont sans commune mesure avec tout ce qui a pu exister par le passé et génèrent de nouveaux risques, aussi bien à l'échelon individuel que sociétal. Le secteur de la recherche, qui dépend étroitement de la collecte et de l'analyse de données, est particulièrement touché par ce phénomène, qui génère des champs de tension entre la liberté de la recherche d'une part et la protection des personnes concernées d'autre part.

La présente contribution offre un aperçu général du cadre légal applicable aux traitements de données personnelles dans le contexte de la recherche, essentiellement à la lumière du droit suisse. Quelques éclairages sur le droit européen seront apportés lorsque cela paraît utile.

Même s'il y est beaucoup question de données de santé, le présent article ne se limite pas à la protection des données dans la recherche biomédicale, mais s'étend à la recherche scientifique au sens large. Les traitements de données à des fins de recherche sont par exemple définis par le rapport explicatif de la Convention 108+[2] comme ceux visant « *à fournir à la recherche une information qui contribue à la compréhension de phénomènes dans divers domaines scientifiques (épidémiologie, psychologie, économie, sociologie, linguistique, politologie, criminologie, etc.) en vue d'établir des permanences, des lois de comportement ou des schémas de causalité qui transcendent tous les individus qu'ils concernent* »[3]. Dans un style marqué par la concision helvétique, la LERI[4] se contente pour sa part de définir la recherche comme la « *recherche*

1 Les analyses et réflexions menées dans cette contribution relèvent de l'opinion personnelle de son auteur et n'engagent en rien celle de leur employeur, à savoir le *SIB Institut Suisse de Bioinformatique*, ou celle d'autres entités telles que *Swiss Personalized Health Network* (SPHN). Le *SIB Institut Suisse de Bioinformatique* est chargé, en collaboration avec l'*Académie suisse des sciences médicales* (ASSM), de la mise en œuvre de l'initiative SPHN, qui comprend également l'établissement du réseau *BioMedIT*. L'auteur est partiellement rémunéré par des fonds SPHN dans le cadre de ses activités professionnelles pour le *SIB Institut Suisse de Bioinformatique*. L'auteur remercie Mathilde HEUSGHEM pour sa relecture attentive et ses remarques avisées.

2 Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

3 Conseil de l'Europe, Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 10 octobre 2018, N 50.

4 Loi fédérale du 14 décembre 2012 sur l'encouragement de la recherche et de l'innovation (LERI), RS 410.1.

méthodique de connaissances nouvelles », qui comprend la recherche fondamentale et la recherche appliquée[5].

On distingue généralement l'utilisation « primaire » des données de la « réutilisation » ou utilisation « secondaire » de ces dernières. L'utilisation primaire des données à des fins de recherche peut intervenir dans le contexte d'essais cliniques, lors desquels des données sont collectées et traitées exclusivement dans le but de l'essai clinique concerné. L'utilisation secondaire consiste quant à elle à réutiliser des données existantes dans un but nouveau, que les données aient été collectées en vue d'un autre projet de recherche ou dans d'autres contextes. Lorsque les données sont collectées en dehors du contexte de la recherche, à l'image des données collectées par un hôpital pour traiter des patients, on parle alors de « données en vie réelle » ou « *real world data* ». Le traitement de ce type de données génère un certain nombre de difficultés, notamment pour de raisons techniques liées au format ou à l'interopérabilité des données, mais il présente aussi l'avantage de réduire les biais possibles liés aux études dans lesquelles les données ont été collectées et offre un accès à des données plus nombreuses, variées et représentatives[6].

Le présent article se concentre principalement sur les conditions de réutilisation des données à des fins de recherche (utilisation secondaire), dans la mesure où cette thématique est celle qui fait l'objet des discussions les plus nourries à l'heure actuelle. Les technologies liées à l'intelligence artificielle ou au *big data* sont en effet directement liées à l'accès à de larges volumes de données, idéalement en situation de vie réelle.

II. Droit applicable et champ d'application

La liberté de la recherche scientifique est expressément consacrée par l'art. 20 Cst.[7], qui enjoint le législateur à garantir aux chercheurs le libre choix de leurs questions de recherche et des méthodes de recherche employées[8]. Plusieurs intérêts publics peuvent néanmoins s'opposer à la liberté de la recherche, à l'instar de la protection des droits fondamentaux de tiers, de la dignité humaine, de la protection de la personnalité ou de la protection des données[9]. Cette dernière fait d'ailleurs l'objet d'une protection constitutionnelle spécifique par le prisme de l'art. 13 al. 2 Cst., selon lequel « *toute personne a le droit*

5 Art. 2 let. a LERI.
6 Dans le même sens : THOUVENIN *et al.,* N 3.
7 Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.), RS 101.
8 CR Cst. I-BOILLET, art. 20, N 14.
9 CR Cst. I-BOILLET, art. 20, N 26.

d'être protégée contre l'emploi abusif des données qui la concernent ». Conformément à l'opinion largement partagée aujourd'hui, la lettre de cette disposition est toutefois trop restrictive. Elle ne protège pas seulement l'individu contre l'emploi abusif de ses données, mais aussi contre tout emploi contraire à sa détermination, consacrant ainsi un droit à l'autodétermination informationnelle[10].

Le droit à l'autodétermination informationnelle est concrétisé aussi bien par des législations générales sur la protection des données que par des législations spéciales, propres à certains secteurs d'activité. Avant d'entreprendre une activité de recherche impliquant des traitements de données personnelles, il est donc primordial de commencer par identifier le droit applicable. Celui-ci peut dépendre de différents facteurs propres au champ d'application respectif de chaque législation, en particulier la qualité de l'auteur du traitement (personne privée, organe public fédéral ou organe public cantonal), la nature de l'activité envisagée (p. ex. recherche sur l'être humain) ou encore le caractère transnational de cette dernière.

Du point de vue de la recherche menée en Suisse, les législations générales susceptibles de trouver application sont les suivantes :

– La LPD[11] est une loi générale qui s'applique aux traitements de données personnelles concernant des personnes physiques effectués par des personnes privées (y compris des personnes morales) ou des organes fédéraux[12].
– Les lois cantonales sur la protection des données sont des lois générales qui s'appliquent aux traitements de données personnelles effectués par les organes publics cantonaux, à l'image des établissements médico-hospitaliers publics de droit cantonal (p. ex. CHUV ou HUG). Chaque canton s'est doté de sa propre loi sur la protection des données, à l'exception des cantons du Jura et de Neuchâtel qui ont adopté une convention intercantonale commune[13].
– Le RGPD[14] est un règlement européen qui déploie néanmoins des effets extraterritoriaux en Suisse dans certaines situations[15]. Il en va ainsi lorsqu'un responsable de traitement ou un sous-traitant effectue des traitements

10 FLÜCKIGER, p. 847 ss et réf. citées. Dans un sens similaire : ATF 140 I 2, c. 9.1 ; Message nLPD, p. 6631.
11 Loi fédérale du 25 septembre 2020 sur la protection des données (LPD), RS 235.1.
12 Art. 2 al. 1 LPD.
13 Convention intercantonale du 9 mai 2012 relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE), RS/NE 150.30.
14 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).
15 Pour un examen des situations dans lesquelles le RGPD peut trouver application en Suisse dans un contexte de recherche biomédicale : JOTTERAND/ERARD, N 12 ss.

de données personnelles relatifs à des personnes qui se trouvent sur le territoire de l'Union européenne et que le traitement est lié à l'offre de biens ou de services dans l'Union européenne ou au suivi du comportement de personnes dans l'Union européenne[16]. Dans le contexte d'activités de recherche, un effet extraterritorial du RGPD est ainsi envisageable en cas de mesures en temps de réels de comportements de personnes se trouvant dans l'Union européenne au moyen d'appareils connectés par exemple. De manière plus générale, le RGPD s'impose souvent comme standard en cas de collaboration avec des institutions de recherche européennes[17].

En parallèle des législations « générales », le législateur a adopté des législations « spéciales » visant à encadrer l'exercice d'activités particulières, que ce soit en raison des risques accrus liés aux activités concernées ou pour protéger certains intérêts dignes de protection. Se conformant au mandat donné par l'art. 118*b* Cst., le législateur fédéral a par exemple légiféré sur la recherche sur l'être humain en adoptant la LRH[18], qui est entrée en vigueur le 1er janvier 2014 (*cf. infra* III.D.1).

En tant que loi spéciale, la LRH l'emporte sur les lois générales de protection des données (LPD et lois cantonales sur la protection des données) dans la mesure où elle règle spécifiquement des aspects liés aux traitements de données personnelles liées à la santé à des fins de recherche sur l'être humain (application du principe *lex specialis derogat generali*)[19]. Les aspects de protection des données qui ne sont pas traités par la LRH sont alors régis à titre résiduel et de manière complémentaire par le droit de la protection des données général applicable (pour plus de détails sur les règles posées par la LRH en matière de protection des données, *cf. infra* III.D.2-3).

Sous l'angle des traitements de données, les lois générales sur la protection des données (LPD, lois cantonales sur la protection des données) ainsi que la LRH s'appliquent uniquement aux traitements de données « personnelles » et non aux données anonymes ou anonymisées[20]. Par ailleurs, le champ d'application de la LRH ne s'étend qu'aux traitements de données personnelles « liées à la santé », c'est-à-dire celles qui ont un lien avec l'état de santé ou la maladie d'une personne, y compris les données génétiques[21]. En dépit de légères variations textuelles, la notion de données personnelles est définie de la même manière par les lois générales sur la protection des données et la LRH, à savoir l'ensemble

16 Art. 3 par. 2 RGPD.
17 JOTTERAND/ERARD, N 17.
18 Loi fédérale du 30 septembre 2011 relative à la recherche sur l'être humain (LRH), RS 810.30.
19 BRUDERER, N 467 ; THOUVENIN *et al*., N 7 et 14 ; MÄTZLER, N 56. Voir aussi dans le présent ouvrage : TALANOVA/DOSCH/MARKS SULTAN/SPRUMONT, II.B.
20 Voir notamment art. 2 al. 1 LPD et art. 2 LRH.
21 Art. 2 et 3 let. f LRH.

des informations concernant une personne physique identifiée ou identifiable[22]. À l'inverse, les données anonymisées sont celles qui ne peuvent être rattachées à une personne qu'aux prix d'efforts disproportionnés, de telle sorte que personne ne s'y attellerait[23].

Dans le contexte de la recherche et plus particulièrement de la recherche biomédicale, les données sont souvent traitées sous forme « pseudonymisée » ou, pour reprendre la terminologie de la LRH, sous forme « codée », les deux termes étant ici synonymes. La LRH définit les données codées comme celles qui ne peuvent être mises en relation avec une personne déterminée qu'au moyen d'une clé[24] et facilite les conditions de réutilisation de telles données à des fins de recherche sur l'être humain (*cf. infra* III.D.3)[25]. Même si elles sont considérées comme anonymisées du point de vue d'un éventuel destinataire, les données codées conservent leur statut de données personnelles dans le contexte des activités soumises à la LRH[26]. En dehors du champ d'application de la LRH, les données correctement pseudonymisées devraient à l'inverse être considérées comme anonymes du point de vue de ceux qui ne sont pas en mesure de réidentifier la personne sans déployer des efforts disproportionnés[27]. Le caractère anonyme de données liées à la santé ne doit néanmoins être retenu qu'avec de grandes précautions en raison du lien étroit entre l'information et les caractéristiques, notamment physiologiques, de la personne concernée. Par ailleurs, les nouvelles technologies et la disponibilité croissante de données complémentaires rendent elles aussi l'anonymisation des données personnelles toujours plus difficile à atteindre[28]. Pour des considérations plus détaillées sur la notion de données personnelles dans la recherche, il est fait renvoi aux contributions de CHRISTINAT (section II.) et TALANOVA/DOSCH/MARKS SULTAN/SPRUMONT (section IV.) dans le présent ouvrage.

---

22 Art. 5 let. a LPD. Voir aussi : art. 3 let. f LRH, qui définit les données personnelles liées à la santé comme « *les informations concernant une personne déterminée ou déterminable qui ont un lien avec son état de santé ou sa maladie, données génétiques comprises* ». En pratique, la notion de personne identifiable ou déterminable peut être difficile à évaluer, voir p. ex. : JUNOD/ELGER, N 16. Pour une analyse détaillée de la notion générale de données personnelles ou anonymes : JOTTERAND.

23 Art. 3 let. i LRH ; Message nLPD, p. 6639 s. Sur la notion de données anonymisées, voir en particulier : SHK HFG-RUDIN, art. 35, N 7 ; MEIER, N 440 ; JOTTERAND ; ERARD, p. 608 s ; ERARD/HEUSGHEM/PARISATO, N 28 ss.

24 Art. 3 let. h LRH. Voir aussi : art. 26 Ordonnance fédérale du 20 septembre 2013 relative à la recherche sur l'être humain (ORH), RS 810.301. À noter qu'en avril 2023, le Conseil fédéral a mis en consultation publique un projet de révision de l'ORH qui amende les art. 25 (anonymisation) et 26 (codage) ORH.

25 Art. 32 et 33 LRH.

26 À ce sujet : ERARD, Les données codées, p. 606 ss.

27 En ce sens : Message nLPD, p. 6640. Pour une approche similaire en droit européen : TUE, arrêt du 26 avril 2023, affaire T-557/20 *(CRU/CEPD)*.

28 JUNOD/ELGER, N 16.

Il faut encore noter que le processus d'anonymisation des données constitue lui-même une activité de traitement, qui peut faire l'objet d'un encadrement légal. Dans le contexte de la LRH, l'anonymisation de données génétiques à des fins de recherche doit par exemple faire l'objet d'une information préalable et la personne concernée doit avoir la possibilité de s'y opposer[29]. Les modalités de l'anonymisation et de la pseudonymisation des données font quant à elles l'objet de prescriptions spécifiques dans le contexte de la LRH[30].

III. Protection des données et « privilège » de la recherche

Il n'est pas rare que la conduite d'activités de recherche suscite des tensions avec certains principes généraux du droit de la protection des données (pour une description générale des principes généraux, *cf.* dans le présent ouvrage POSSE, III.B.]). Conformément au principe de finalité par exemple[31], les traitements ultérieurs de données devraient se limiter aux finalités déterminées et reconnaissables lors de la collecte. Or, en pratique, la recherche scientifique nécessite souvent l'accès à des données collectées originairement pour des fins différentes (p. ex. : données médicales collectées dans le contexte des soins). Quant au principe général de proportionnalité[32], il impose entre autres de limiter la conservation des données personnelles à la seule durée nécessaire pour atteindre la finalité envisagée, à savoir la conduite d'un projet de recherche si l'on se concentre sur le contexte scientifique. Dans les faits toutefois, il existe souvent un intérêt à conserver des données pour un usage prolongé, potentiellement pour mener de nouveaux projets de recherche dans le futur. Une telle conservation s'inscrit d'ailleurs en droite ligne avec le mouvement de science ouverte ou *open science*.

Les tensions entre protection des données et recherche scientifique ont par conséquent conduit à chercher un nécessaire compromis, justifié par l'intérêt public important qui sous-tend la recherche scientifique. Ce compromis implique l'assouplissement de certaines règles de protection des données, que l'on qualifie parfois de « privilège de la recherche ». Ces aménagements sont notamment reconnus à l'échelon international par la Convention 108[33], et bientôt par la Convention 108+[34]. Cette dernière autorise par exemple des dérogations

29 Art. 32 al. 3 LRH.

30 Art. 35 LRH ; art. 25 et 26 ORH. On notera que ces dispositions font l'objet d'un projet de révision mis en consultation publique par le Conseil fédéral en avril 2023 : www.bag.admin.ch/bag/fr/home/medizin-und-forschung/forschung-am-menschen/revision-verordnungen-hfg.html.

31 Art. 6 al. 3 LPD.

32 Art. 6 al. 2 LPD.

33 Art. 9 par. 3 Convention 108.

34 Art. 5 par. 4 let. b et 11 Convention 108+.

au principe de finalité en cas de traitement de données ultérieur à des fins scientifiques à condition d'adopter des garanties de protection supplémentaires[35]. Elle permet aussi aux législateurs nationaux de restreindre l'application du principe de transparence ou les droits des personnes concernées en cas de traitement à des fins scientifiques, lorsqu'il n'existe pas de risque identifiable d'atteinte aux droits et libertés fondamentales des personnes concernées[36].

Les paragraphes qui suivent présentent brièvement comment le privilège de la recherche a été mis en œuvre en droit suisse et dans le RGPD. Les règles qui y sont décrites s'appliquent exclusivement aux utilisations secondaires de données et non aux utilisations primaires, qui restent quant à elles soumises aux règles ordinaires en matière de protection des données.

A. Loi fédérale sur la protection des données

Pour rappel, le champ d'application de la LPD s'étend aux traitements de données personnelles réalisés par les personnes privées et les organes publics fédéraux, sous réserve de l'éventuelle application de lois spéciales (p. ex. : LRH pour la recherche sur l'être humain). La LPD prévoit des dispositions particulières facilitant les traitements de données à des fins de recherche menés aussi bien par les personnes privées que par les organes publics fédéraux, mais ces règles diffèrent dans un cas et dans l'autre.

1. Personnes privées

Contrairement à la logique du RGPD qui requiert que tout traitement de données personnelles repose sur un des motifs légaux énoncés à son art. 6, voire cumulativement sur un des motifs énoncés à son art. 9 en cas de traitement de catégories particulières de données, la LPD n'impose pas qu'un traitement de données personnelles repose sur un motif particulier. La LPD est construite autour du concept d'atteinte à la personnalité et consacre le principe selon lequel « *celui qui traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées* »[37].

Les situations de traitements de données personnelles qui impliquent une atteinte à la personnalité ne sont pas décrites exhaustivement par la LPD, mais cette dernière pose une fiction irréfragable d'atteinte à la personnalité dans trois cas

35 Art. 5 par. 4 let. b Convention 108+.
36 Art. 11 par. 2 Convention 108+.
37 Art. 30 al. 1 LPD. Voir aussi : BRUDERER, N 471 ss.

spécifiques. Il s'agit des traitements effectués en contradiction avec les principes généraux énoncés aux art. 6 et 8 LPD, des traitements de données personnelles contre la manifestation expresse de la volonté de la personne concernée, et de la communication de données sensibles à des tiers.

Les atteintes à la personnalité sont par définition considérées comme illicites, mais l'illicéité peut être levée en présence d'un motif justificatif. En droite ligne avec la systématique générale du Code civil pour les atteintes à la personnalité (art. 28 CC[38]), l'art. 31 LPD énonce qu'une atteinte à la personnalité peut être justifiée par le consentement de la personne concernée, par un intérêt privé ou public prépondérant ou par la loi. En l'absence d'un consentement ou d'une disposition légale justifiant l'atteinte, il faut donc procéder à une pesée d'intérêts entre les intérêts à la protection de la personnalité de la personne concernée et l'intérêt du responsable du traitement à traiter les données concernées. L'art. 31 al. 2 LPD offre à cet égard une liste exemplative d'intérêts prépondérants qui peuvent entrer en considération, étant entendu que l'existence d'un de ces intérêts ne suffit pas en soi à justifier une atteinte.

Le législateur fédéral a inscrit dans la liste exemplative d'intérêts prépondérants à prendre en considération pour justifier une atteinte la situation où les données personnelles sont traitées à des fins « *ne se rapportant pas à des personnes* », notamment dans le cadre de la recherche[39]. Les traitements de données ne se rapportant pas à des personnes signifie que l'identité des personnes concernées ne joue aucun rôle pour la finalité du traitement[40]. Les chercheurs en généalogie ne peuvent donc pas se prévaloir de cet intérêt puisque leurs travaux se rapportent précisément à l'identité de personnes[41]. En présence de traitements de données ne se rapportent pas à des personnes, le législateur a estimé que les conséquences d'une éventuelle violation des principes généraux étaient moins graves puisque les traitements seraient sans conséquence directe pour les personnes concernées[42].

L'intérêt prépondérant lié aux traitements ne se rapportant pas à des personnes n'est pas propre à la recherche scientifique. En plus de la recherche, l'art. 31 al. 2 let. e LPD mentionne les exemples de la planification et de la statistique, mais cette liste n'est pas exhaustive[43]. Des activités de traitements liées à l'amélioration des moyens de mobilité pourraient par exemple tomber dans la catégorie des traitements ne se rapportant pas à des personnes, pour autant que des

38 Code civil suisse du 10 décembre 1907 (CC), RS 210.
39 Art. 31 al. 2 let. e LPD.
40 MÄTZLER, N 21.
41 Message aLPD, p. 469.
42 Message aLPD, p. 469.
43 Message aLPD, p. 469.

données personnelles soient traitées. Par ailleurs, le motif justificatif du traitement ne se rapportant pas à des personnes n'est pas limité aux seules activités qui poursuivraient des objectifs de nature purement idéale, mais peut aussi être invoqué à l'appui d'activités commerciales[44].

L'intérêt prépondérant lié aux traitements ne se rapportant pas à des personnes ne peut toutefois être avancé pour justifier une atteinte à la personnalité que si les conditions énoncées à l'art. 31 al. 2 let. e LPD sont réunies. Ces critères ont fait l'objet d'un renforcement par rapport à l'ancien art. 13 al. 2 let. e aLPD[45], notamment pour mieux répondre aux défis posés par le monde numérique et les technologies liées au *big data*[46]. Les trois conditions cumulatives sont désormais les suivantes :

– Les données doivent être anonymisées dès que la finalité du traitement le permet. Dans la situation où une anonymisation n'est pas possible ou exigerait des efforts disproportionnés, le responsable du traitement doit prendre des mesures appropriées pour que les personnes concernées ne puissent pas être réidentifiées. En cas de communication des données, de telles mesures peuvent prendre la forme d'une pseudonymisation des données à condition que la clé de réidentification reste chez le responsable du traitement[47].
– Lorsqu'une communication de données sensibles au sens de l'art. 5 let. c LPD entre en considération, le responsable du traitement ne peut communiquer de telles données à des tiers que sous une forme qui ne permet pas d'identifier les personnes concernées. Dans le cas où cela serait impossible, il doit alors adopter des mesures, en particulier contractuelles, qui garantissent que le destinataire des données ne traitera lui aussi les données qu'à des fins ne se rapportant pas à des personnes.
– Enfin, le responsable du traitement doit publier les résultats sous une forme ne permettant pas d'identifier les personnes concernées.

La réalisation des trois conditions permet seulement au responsable du traitement de faire valoir l'intérêt au traitement de données ne se rapportant pas à des personnes. Cet intérêt doit encore être mis en balance avec les intérêts à la protection de la personnalité des personnes concernées. C'est uniquement dans le cas où l'intérêt au traitement ne se rapportant pas à des personnes surpasse celui des personnes concernées que l'atteinte à la personnalité est justifiée[48]. Soulignons encore que le motif justificatif de l'intérêt prépondérant au sens de l'art. 31 LPD ne permet pas de déroger à une obligation spéciale de garder le

44 Dans le même sens : BRUDERER, N 484.
45 Loi fédérale du 19 juin 1992 sur la protection des données (aLPD), RS 235.1.
46 Message nLPD, p. 6692.
47 Message nLPD, p. 6692.
48 Message nLPD, p. 6689 ; BRUDERER, N 490.

secret[49]. Une communication de données personnelles couvertes par le secret des art. 321 CP (secret professionnel) ou 320 CP (secret de fonction) doit par conséquent respecter les prescriptions imposées par ces dispositions[50].

2. Organes publics fédéraux

Sur la base des mêmes motifs que ceux invoqués pour assouplir les conditions de traitements à des fins ne se rapportant pas à des personnes effectués par des personnes privées, à savoir que ce type de traitements est justifié par des intérêts publics et présente des risques moins importants[51], le législateur a aussi adopté des allégements pour les traitements de données ne se rapportant pas à des personnes effectués par les organes publics fédéraux (p. ex. : OFSP). Les conditions légales sont réglées par l'art. 39 LPD, qui reprend dans une bonne mesure les conditions qui prévalaient sous le régime de l'ancienne LPD (art. 22 aLPD).

La logique prévue par l'art. 39 LPD diffère néanmoins de celle qui gouverne la justification des atteintes illicites par des personnes privées. Les organes publics étant liés par le principe de légalité, les traitements de données personnelles effectués par ces derniers doivent en principe reposer sur une base légale[52]. En tant que tel et en dépit d'une formulation trompeuse (« *Les organes fédéraux sont en droit de traiter des données personnelles à des fins ne se rapportant pas à des personnes* […] »), l'art. 39 LPD ne constitue pas lui-même une base légale légitimant un traitement de données personnelles par un organe public et le traitement doit donc reposer sur une base légale distincte[53]. En matière de recherche, l'art. 36*c* de la Loi sur les EPF[54] constitue par exemple une telle base légale. Dans la même ligne, l'art. 39 LPD s'applique uniquement aux données personnelles qui se trouvent d'ores et déjà en main d'un organe public fédéral et ne crée pas une base légale sur laquelle un organe public fédéral pourrait s'appuyer pour collecter de nouvelles données en vue d'un traitement de données à des fins ne se rapportant pas à des personnes, notamment à des fins de recherche[55].

---

49 ERARD/HEUSGHEM/PARISATO, N 49.
50 MEIER, N 1711.
51 Message aLPD, p. 479.
52 BSK DSG-MAURER-LAMBROU/KUNZ, art. 22, N 4.
53 BSK DSG-MAURER-LAMBROU/KUNZ, art. 22, N 4.
54 Loi fédérale du 4 octobre 1991 sur les écoles polytechniques fédérales (Loi sur les EPF), RS 414.110.
55 MÄTZLER, N 21.

Concrètement, l'art. 39 LPD se limite à assouplir certaines exigences légales (indiquées exhaustivement à l'art. 39 al. 2 LPD, décrites en détail plus bas) lorsque les conditions suivantes sont réunies :

– Les données sont rendues anonymes dès que la finalité du traitement le permet.
– Les données sensibles ne sont communiquées à des « *personnes privées* » que sous une forme qui ne permet pas d'identifier les personnes, étant entendu que les données peuvent dans ce cas être communiquées sous forme pseudonymisée si la clé reste chez l'organe public qui a envoyé les données[56]. *A contrario*, cette condition ne s'applique pas aux communications de données sensibles entre organes fédéraux. Cette exigence est nouvelle par rapport à l'ancienne LPD.
– Le destinataire des données ne communique les données à des tiers qu'avec le consentement de l'organe fédéral qui les lui a transmises. L'organe public fédéral doit s'assurer du respect de cette condition au moyen d'instructions ou en concluant un contrat avec le destinataire[57]. La réutilisation par le tiers n'est autorisée que pour des traitements ne se rapportant pas à des personnes[58].
– Si une publication des résultats qui découlent du traitement à des fins ne se rapportant pas à des personnes est envisagée, celle-ci ne doit pas permettre d'identifier les personnes concernées.

Si le traitement de données envisagé ne se rapporte pas à des personnes et que les conditions susmentionnées sont réunies, l'art. 39 al. 2 LPD prévoit l'inapplicabilité de trois dispositions légales de la LPD, énumérées de manière exhaustive.

L'organe public fédéral peut en premier lieu déroger au principe de finalité énoncé par l'art. 6 al. 3 LPD. En d'autres termes, il n'est pas tenu par son obligation de traiter les données conformément à la finalité initiale et peut donc réutiliser ou communiquer les données à d'autres fins dans la mesure où ces dernières ne se rapportent pas à des personnes, telles que la recherche ou la statistique.

Les assouplissements prévus par l'art. 39 al. 2 LPD permettent ensuite de faire tomber l'exigence de la base légale formelle exigée par l'art. 34 LPD pour certains types de traitements de données réalisés par les organes publics fédéraux. Il s'agit des traitements de données mettant en jeu des données sensibles, des profilages, ainsi que les traitements dont la finalité ou les modalités sont susceptibles de porter gravement atteinte aux droits fondamentaux des personnes concernées. Il est néanmoins primordial de souligner que l'art. 39 al. 2 LPD

56 Message nLPD, p. 6699.
57 BSK DSG-Maurer-Lambrou/Kunz, art. 22, N 26 ; Message aLPD, p. 480.
58 BSK DSG-Maurer-Lambrou/Kunz, art. 22, N 27.

permet uniquement de déroger à l'exigence d'une base légale « formelle », et non pas au principe général de légalité au sens de l'art. 34 al. 1 LPD. Sous réserve des exceptions prévues à l'art. 34 al. 4 LPD, notamment si la personne concernée a consenti au traitement en l'espèce, les traitements de données à des fins ne se rapportant pas à des personnes effectués par un organe public fédéral doivent donc *a minima* reposer sur une base légale matérielle.

Enfin, l'art. 39 al. 2 LPD supprime l'exigence d'une base légale au sens de l'art. 34 al. 1 à 3 LPD pour les aspects spécifiquement liés à la communication de données à des tiers.

Comme le rappelle l'art. 35 OPDo[59], ces dérogations s'appliquent uniquement aux traitements effectués à des fins ne se rapportant pas à des personnes. On veillera dans tous les cas à observer les règles particulières éventuellement imposées par les législations spéciales applicables. Les traitements de données à des fins de recherche effectués par les institutions du domaine des EPF doivent par exemple respecter les exigences posées par les art. 36*c* ss de la Loi sur les EPF, qui prescrivent par exemple des règles particulières en lien avec la durée de conservation des données ou l'obligation d'informer les personnes concernées de la collecte et du traitement de données les concernant dans le cadre d'un projet de recherche.

B. Lois cantonales sur la protection des données

Dans la mesure où les traitements de données personnelles effectués par les organes publics cantonaux sont soumis aux législations cantonales sur la protection des données, les règles imposées par ces dernières ont une importance non négligeable pour le secteur de la recherche. Sous réserve de l'éventuelle application de lois spéciales fédérales (p. ex. : LRH), c'est en effet le droit cantonal qui régit les traitements de données réalisés dans le contexte des recherches menées par les universités publiques cantonales, telles que les universités de Lausanne, Genève, Neuchâtel ou Fribourg.

À l'instar de la LPD, les législations cantonales relatives à la protection des données personnelles prévoient généralement des assouplissements pour les traitements de données à des fins de recherche, de planification ou de statistique. Ces règles font néanmoins l'objet de disparités cantonales[60] et il convient de mener un examen attentif des règles juridiques applicables dans chaque cas d'espèce.

59 Ordonnance fédérale du 31 août 2022 sur la protection des données (OPDo), RS 235.11.
60 THOUVENIN *et al.*, N 10.

Dans le canton de Vaud, l'art. 24 LPrD-VD[61] assouplit par exemple les exigences légales pour les traitements de données personnelles effectués à des fins de recherche, de planification ou de statistique. Reprenant les exigences posées par l'ancienne LPD pour les organes publics fédéraux (anonymisation dès que possible, communication par le destinataire seulement avec l'accord de l'autorité émettrice et publication des résultats ne permettant pas l'identification des personnes), l'art. 24 LPrD-VD supprime l'application des règles imposées par cette même loi en lien avec le respect des principes de légalité (art. 5) et de finalité (art. 6) ainsi que celles qui règlent la communication de données (art. 15).

Dans le canton de Genève, l'art. 41 LIPAD[62] règle les conditions auxquelles les institutions publiques cantonales peuvent traiter des données personnelles à des fins générales de statistique, de recherche scientifique, de planification ou d'évaluation de politiques publiques, pour autant que ces activités s'inscrivent dans l'accomplissement de leurs tâches légales. Outre certaines conditions relativement similaires à celles requises par la LPD pour les traitements de données à des fins ne se rapportant pas à des personnes par les organes publics fédéraux, l'art. 41 LIPAD impose des obligations supplémentaires d'annonce ou d'autorisation. Ainsi, les traitements de données susmentionnés doivent par principe faire l'objet d'une information préalable au Préposé cantonal à la protection des données et à la transparence. Par ailleurs, un traitement qui porte sur des données sensibles ou implique l'établissement de profils de la personnalité nécessite une autorisation délivrée par le Conseil d'État, qui requiert au préalable le préavis du Préposé cantonal à la protection des données et à la transparence.

De manière générale, l'examen des règles cantonales instituant des « privilèges de la recherche » laisse parfois planer des doutes quant à leur application concrète. Cela découle notamment du fait que les bases légales fondant les traitements de données personnelles par les institutions publiques cantonales de recherche ne sont pas toujours explicites, voire parfois même inexistantes. Il est par conséquent important que les législateurs cantonaux mettent à jour les législations concernées pour établir des bases légales claires sur lesquelles les institutions de recherche publiques cantonales peuvent s'appuyer pour traiter des données personnelles, comme cela a été fait au niveau fédéral avec les art. 36*c* ss de la Loi sur les EPF.

61 Loi cantonale vaudoise du 11 septembre 2007 sur la protection des données personnelles (LPrD-VD), BLV 172.65.

62 Loi cantonale genevoise sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD), RS/GE A 2 08.

C. *Excursus* : Règlement général sur la protection des données (RGPD)

À l'inverse du droit suisse, le RGPD ne recourt pas à la notion de traitements de données à des fins ne se rapportant pas à des personnes. Reconnaissant l'importance des enjeux liés à la recherche scientifique[63], il prévoit néanmoins des assouplissements pour les traitements de données personnelles effectués dans ce but[64].

De manière générale, l'art. 89 par. 1 RGPD impose à ceux qui traitent des données personnelles à des fins de recherche scientifique d'adopter des garanties appropriées pour les droits et libertés de la personne concernée, qui doivent se matérialiser par la mise en place de mesures techniques et organisationnelles[65]. Conformément au principe de minimisation des données, la mise en œuvre de ces mesures doit conduire à la pseudonymisation des données à chaque fois que cela est possible et impose au responsable du traitement de privilégier systématiquement les solutions qui ne permettent pas ou plus l'identification des personnes concernées pour des traitements ultérieurs.

Le respect des garanties appropriées imposées par l'art. 89 par. 1 RGDP ouvre la voie à un certain nombre de dérogations au RGPD, dont certaines sont énoncées ci-dessous de manière non exhaustive :

– Du point de vue des droits des personnes, l'art. 89 par. 2 RGPD prévoit par exemple que le droit de l'Union ou les droits nationaux peuvent restreindre l'exercice de certains droits (droits d'accès, de rectification, de limitation du traitement et d'opposition) si ces droits risquent de rendre impossible ou d'entraver sérieusement la réalisation des recherches et si de telles dérogations sont nécessaires pour atteindre ces finalités. Le droit à l'effacement (art. 17 RGPD) est limité si son exercice est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs des traitements de données nécessaires à des fins de recherche scientifique ou historique (art. 17 par. 3 let. d RGPD).
– Par principe et sous réserve des situations listées par l'art. 9 par. 2 RGPD, l'art. 9 par. 1 RGPD interdit le traitement des catégories particulières de données personnelles, dont font partie les données concernant la santé ou les données génétiques. L'art. 9 par. 2 let. j RGPD autorise expressément le traitement de catégories particulières de données à des fins de recherche scientifique ou historique « *sur la base du droit de l'Union ou du droit d'un*

63 Voir notamment Considérant 157 RGPD. La recherche scientifique doit être interprétée largement, *cf.* Considérant 159 RGPD.

64 Pour des plus amples développements relatifs à un privilège de la recherche en droit européen, voir : BRUDERER, N 508 ss.

65 BRUDERER, N 527 ss.

État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ».

– L'art. 5 par. 1 let. b RGPD relativise le principe de finalité en stipulant de manière générale que les traitements de données ultérieurs à des fins de recherche scientifique ou historique ne sont pas considérés comme incompatibles avec les finalités initiales.
– En dérogation du principe de limitation de la conservation des données (art. 5 par. 1 let. e RGPD), les données personnelles traitées à des fins de recherche scientifique peuvent être conservées pour des durées plus longues.

Il est encore important de souligner que l'art. 9 par. 4 RGPD permet aux États membres d'adopter des réglementations plus strictes pour encadrer le traitement de données concernant la santé, de données génétiques et de données biométriques. Cette possibilité offerte aux États membres est aujourd'hui largement utilisée, ce qui conduit à une situation réglementaire morcelée à travers l'Union européenne pour les traitements de ce type de données, notamment à des fins de recherche[66].

D. Loi spéciale : Loi fédérale relative à la recherche sur l'être humain

1. Genèse et champ d'application

En mars 2010, le peuple a accepté en votation populaire l'introduction d'un nouvel art. 118*b* Cst. qui octroie aujourd'hui à la Confédération des compétences pour légiférer de manière étendue et uniforme dans le domaine de la recherche sur l'être humain, « *dans la mesure où la protection de la dignité humaine et de la personnalité l'exige* ». Le but premier de cette disposition constitutionnelle consiste donc à protéger la dignité et la personnalité de l'être humain tout en prenant en compte la liberté de la recherche ainsi que l'importance de la recherche pour la santé et la société[67]. Des risques pour la dignité humaine et la personnalité doivent en principe être reconnus si un lien peut être établi entre les données de recherche et les personnes concernées[68]. Le mandat constitutionnel de l'art. 118*b* Cst. énonce par ailleurs certains principes centraux qui doivent être respectés par le législateur fédéral lorsqu'il légifère dans le

66 Commission européenne, Assessment of the EU Member States' rules on health data in the light of GDPR, p. 55 ss ; BRUDERER, N 551 ; THOUVENIN *et al*., N 11.
67 Message article constitutionnel recherche, p. 6352. À ce sujet, voir aussi : DUCOR, N 12 ss.
68 Message article constitutionnel recherche, p. 6359 ; DUCOR, N 33.

domaine spécifique de la recherche en biologie et en médecine impliquant des personnes. Parmi ceux-ci, l'art. 118*b* al. 2 let. a Cst. indique qu'un « *projet de recherche ne peut être réalisé que si la personne y participant ou la personne désignée par la loi a donné son consentement éclairé ; la loi peut prévoir des exceptions ; un refus est contraignant dans tous les cas* ». Ce principe vaut non seulement pour les activités de recherche menées directement sur le corps humain, mais aussi pour celles menées sur les données personnelles relatives aux participants.

La nécessité de protéger les données personnelles dans le contexte de la recherche sur l'être humain découle aussi de textes juridiques ou éthiques internationaux, à l'image de la Convention sur les Droits de l'homme et la biomédecine[69] ou encore de la Déclaration de Taipei relative à la recherche sur les bases de données de santé, les *big data* et les biobanques[70].

Suite à l'introduction de l'art. 118*b* Cst. en 2010, l'Assemblée fédérale a adopté la LRH et ses ordonnances d'application (notamment l'ORH[71] et l'OClin[72]), toutes entrées en vigueur le 1er janvier 2014. Celles-ci s'appliquent sans égard à la nature de l'auteur des traitements, qu'il s'agisse d'organes publics fédéraux, d'organes publics cantonaux ou de personnes privées. Leur champ d'application matériel s'étend à la recherche méthodologique visant à obtenir des connaissances généralisables sur les maladies humaines et sur la structure et le fonctionnement du corps humain, pratiquée entre autres sur les données personnelles liées à la santé (sur la notion de données personnelles liées à la santé et l'exclusion des données anonymes, *cf. supra* II.)[73]. La recherche sur les maladies humaines vise l'ensemble des recherches sur les causes, la prévention, le diagnostic, le traitement et l'épidémiologie des troubles physiques et psychiques de la santé[74]. Quant à la recherche sur la structure et le fonctionnement du corps humain, elle est définie par la loi comme « *la recherche fondamentale, en particulier dans les domaines de l'anatomie, de la physiologie et de la génétique du corps humain ainsi que la recherche non axée sur une maladie relative aux interventions sur le corps humain* »[75].

---

69 Convention du 4 avril 1997 pour la protection des Droits de l'Homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine, entré en vigueur pour la Suisse le 1er novembre 2008, RS 0.810.2, en particulier ses art. 10 (Vie privée et droit à l'information) et 16 (Protection des personnes se prêtant à une recherche).

70 Association Médicale Mondiale, Déclaration de Taipei sur les considérations éthiques concernant les bases de données de santé et les biobanques, octobre 2016.

71 Ordonnance fédérale du 20 septembre 2013 relative à la recherche sur l'être humain (ORH), RS 810.301.

72 Ordonnance fédérale du 20 septembre 2013 sur les essais cliniques (OClin), RS 810.305.

73 Art. 2 al. 1 let. e et 2 al. 2 let. a et c LRH.

74 Art. 3 let. b LRH.

75 Art. 3 let. c LRH.

Les activités de recherche qui ont par exemple pour objet le marketing, le racisme ou encore l'économie de la santé ne tombent donc pas dans le champ d'application de la LRH[76]. En pratique, la distinction entre activité de recherche et autres types d'activités se révèle parfois difficile à opérer[77]. En 2020, *swissethics* a publié des lignes directrices pour guider les chercheurs sur la distinction entre recherche sur l'être humain et activités d'assurance de la qualité[78]. Ces dernières s'articulent autour de quatre points d'analyse, à savoir le but du projet, l'objet du projet, le caractère généralisable des connaissances et la méthodologie du projet.

Comme déjà mentionné (*cf. supra* II.), la LRH et ses ordonnances d'application constituent des législations spéciales qui l'emportent sur d'éventuelles législations générales (notamment en matière de protection des données), dans la mesure où les législations spéciales règlent des aspects de manière spécifique. Les aspects en lien avec la protection des données qui ne sont pas réglés spécifiquement par la LRH ou ses ordonnances sont soumis de manière résiduelle aux règles imposées par les législations générales en matière de protection des données (LPD ou législations cantonales sur la protection des données).

2. Protection des données et LRH

Certaines étapes des traitements de données personnelles effectués dans le contexte d'un projet de recherche soumis à la LRH font l'objet d'un encadrement légal spécifique. La présente section dresse de manière succincte et non exhaustive les contours des règles les plus significatives en la matière. La « réutilisation » de données existantes à des fins de recherche est traitée de manière séparée dans la section suivante (*cf. infra* III.D.3).

Par principe, une personne ne peut participer à un projet de recherche soumis à la LRH que si elle y a consenti de manière éclairée. Les informations qui doivent être fournies à la personne à cette occasion sont décrites par l'art. 16 al. 2 LRH, qui prévoit notamment une information relative aux mesures destinées à assurer la protection des données personnelles. Dans ce contexte, ce ne sont pas les détails techniques qui sont pertinents, mais essentiellement le lieu et le mode de conservation (données codées ou non codées), les droits d'accès ou encore les éventuelles obligations de divulgation[79]. Dans le cas où une réutilisation ultérieure des données personnelles relatives à la santé est d'ores et déjà envisagée lors de la collecte initiale, les chercheurs sont tenus d'en informer les

76 DUCOR, N 32.
77 JUNOD/ELGER, N 16.
78 Swissethics, Assurance de la qualité ou recherche soumise à autorisation ?, version 1.0 du 4 février 2020.
79 SHK HFG-SPRECHER/VAN SPYK, art. 16, N 54.

participants et de recueillir leur consentement à ce moment-là[80]. Les participants doivent également être informés qu'ils ont la possibilité de s'opposer à une telle réutilisation.

Le consentement à la participation à une recherche ou à la réutilisation des données peut être révoqué en tout temps par la personne concernée[81]. Dans ce cas, les données doivent être anonymisées après avoir été analysées, sauf si la personne y renonce au moment de la révocation ou s'il est évident depuis le début du projet de recherche qu'une anonymisation n'est pas possible et que la personne concernée a consenti à participer au projet après avoir été suffisamment informée de cette circonstance[82].

Lorsqu'ils conservent des données personnelles de recherche liées à la santé, les chercheurs doivent les protéger de toute utilisation illégale en adoptant des mesures techniques et organisationnelles appropriées[83]. Ils doivent par ailleurs respecter les exigences techniques liées aux conditions d'exploitation. Les mesures techniques et organisationnelles sont détaillées par les art. 5 ORH et 18 OClin, qui prévoient des exigences identiques. Celles-ci imposent notamment aux chercheurs de limiter l'accès aux données aux seules personnes qui en ont besoin pour accomplir leurs tâches, d'empêcher la publication, la modification, la suppression et la copie des données sans autorisation ou par inadvertance, ainsi que de mettre en place un système de traçabilité. À mon sens, les mesures de sécurité imposées par les législations générales sur la protection des données applicables (p. ex. : art. 1 ss OPDo pour les traitements effectués par des personnes privées ou des organes publics fédéraux) doivent s'appliquer à titre complémentaire.

On notera que les chercheurs sont par ailleurs soumis à une obligation d'observer le secret professionnel dont la violation est réprimée pénalement par l'art. 321bis CP, qui renvoie à l'art. 321 CP (secret professionnel). L'art. 321bis ch. 2 CP prévoit que le secret professionnel peut être levé à des fins de recherche aux conditions posées par la LRH et pour autant que la commission d'éthique compétente autorise la levée du secret.

Conformément au principe de finalité, les données personnelles liées à la santé collectées ou réutilisées dans le contexte de la recherche sur l'être humain ne peuvent pas être réutilisées à d'autres fins que la recherche sur l'être humain. L'art. 41 LRH permet néanmoins de déroger à cette limitation dans deux cas particuliers. C'est d'abord le cas si une base légale le prévoit, notamment si elle autorise la réutilisation ou la communication de données de recherche dans un

80 Art. 17 LRH.
81 Art. 7 al. 2 LRH.
82 Art. 10 ORH.
83 Art. 43 al. 1 LRH.

contexte spécifique. Dans le cadre d'une procédure pénale par exemple, les chercheurs peuvent être amenés à communiquer des informations couvertes par le secret de la recherche (art. 321bis CP) si l'intérêt à la manifestation de la vérité l'emporte sur l'intérêt au maintien du secret (art. 173 CPP[84]). Ensuite, les données peuvent être réutilisées à d'autres fins si la personne concernée donne « *son consentement éclairé en l'espèce* ». Le consentement à une réutilisation à d'autres fins que la recherche doit donc être donné au cas par cas et ne peut pas être donné de manière générale. Les conditions d'accès restrictives aux données de recherche ne représentent pas une question anodine à l'heure des nouvelles technologies reposant sur le *big data* ou sur des algorithmes d'apprentissage. En effet, ces dernières nécessitent des accès élargis aux données non seulement durant leur phase de développement, mais aussi en cours d'utilisation en routine. Or, de telles utilisations ne relèvent plus du domaine de la recherche. Ces obstacles pourraient bien conduire les opérateurs de tels systèmes à exercer une pression croissante pour assouplir les conditions d'accès aux données de recherche en vue de ce type d'utilisations.

L'art. 43 LRH prévoit pour sa part des règles particulières pour l'envoi à l'étranger de données à des fins de recherche. Les données génétiques ne peuvent être exportées à l'étranger à des fins de recherche qu'avec le consentement éclairé de la personne concernée, qui peut aussi être donné sous forme de consentement général (*cf. infra* III.D.3). Quant à l'exportation d'autres données personnelles liées à la santé, elle n'est pas soumise à l'autorisation expresse de la personne concernée. Celle-ci n'est toutefois possible que si les conditions posées par la LPD pour les communications à l'étranger (art. 16 ss LPD) sont respectées. L'art. 43 al. 2 LRH a donc pour effet d'écarter les prescriptions des législations cantonales générales sur la protection des données (traitements effectués par des organes publics cantonaux tels que les hôpitaux universitaires) au profit des règles imposées par la LPD en cas de communication de données à l'étranger dans un contexte de recherche sur l'être humain.

Par ailleurs, en vertu de l'art. 44 LRH, les dispositions relatives à la transmission des données à des fins autres que la recherche (art. 41 LRH), à l'exportation de données à l'étranger (art. 42 LRH) et aux conditions de conservation des données (art. 43 LRH) s'appliquent par analogie aux données qui concernent les personnes décédées, les embryons et les fœtus, y compris aux enfants mort-nés, aux parties de ceux-ci et aux données relevées dans ce contexte. Ces données ne sont pas considérées comme des données « personnelles », de telle sorte que le champ d'application de la LRH excède sur ces questions celui des législations générales sur la protection des données.

84 Code de procédure pénale suisse du 5 octobre 2007 (CPP), RS 312.0.

Enfin, la réalisation d'un projet de recherche au sens de la LRH est soumise l'approbation d'une commission d'éthique au sens de l'art. 47 LRH[85]. Celle-ci n'est délivrée que si les exigences éthiques, juridiques et scientifiques prévues par la LRH sont remplies[86].

3. Réutilisation des données à des fins de recherche sur l'être humain

a) Régime légal

Le chapitre 4 de la LRH (art. 32-35) définit les conditions auxquelles des données personnelles liées à la santé peuvent être réutilisées à des fins de recherche sur l'être humain. Plus précisément, les art. 32 ss LRH établissent des règles qui allègent le principe général de finalité et autorisent, sous certaines conditions, la réutilisation de données personnelles de santé qui auraient été collectées dans un autre contexte que la recherche envisagée, par exemple dans le cadre d'une relation thérapeutique (p. ex. : données collectées par un hôpital) ou dans celui d'une autre recherche[87]. En tant que règles spéciales, elles priment les règles instituant des privilèges de la recherche pour les traitements de données à des fins ne se rapportant pas à des personnes, telles qu'instituées par la LPD ou les lois cantonales générales sur la protection des données (*cf. supra* II.)[88].

La réutilisation est définie de manière large par l'art. 24 ORH, qui y assimile toute opération effectuée à des fins de recherche avec des données déjà collectées. Les opérations en question peuvent couvrir la collecte, le regroupement, le catalogage, la conservation ou encore la mise à disposition des données[89]. Il est néanmoins indispensable que ces opérations soient réalisées « *à des fins de recherche* », faute de quoi elles sortiraient du champ de la LRH. Ainsi, la simple création d'un catalogue de données personnelles liées à la santé ne constitue en principe pas un projet de recherche[90]. Dans le contexte de la réutilisation de données, la limite entre ce qui constitue ou non un projet de recherche au sens de la LRH peut parfois être difficile à tracer[91].

---

85 Art. 45 al. 1 LRH.
86 Art. 45 al. 2 LRH.
87 BRUDERER, N 663.
88 THOUVENIN *et al*., N 7 ; MÄTZLER, N 57.
89 Art. 24 ORH.
90 DUCOR, N 82.
91 Pour différents exemples pratiques : DUCOR, N 82, qui cite notamment les cas où il faut réutiliser des données pour valider ou tester une méthode en vue d'une recherche

Les règles de réutilisation établies par la LRH reposent sur une appréciation des risques pour les personnes concernées et s'articulent autour d'un double critère : la nature des données (génétiques ou non génétiques) et la forme des données (non codées/en clair, codées ou anonymisées).

Les données génétiques non codées étant considérées comme les plus sensibles, la personne concernée doit consentir à leur réutilisation pour chaque projet de recherche individuel impliquant la réutilisation de telles données[92]. Les données génétiques codées et les données non génétiques en clair (non codées) peuvent quant à elles faire l'objet d'une réutilisation sur la base d'un consentement général, c'est-à-dire un consentement donné « *à des fins de recherche* » et non pas pour un projet de recherche en particulier[93]. En théorie et conformément à la lettre de la LRH, les données non génétiques codées sont considérées comme moins sensibles et pourraient être réutilisées si la personne concernée ne s'y est pas opposée après avoir été informée de la possibilité d'une réutilisation (système d'*opt-out*)[94]. Néanmoins, en pratique et pour des raisons éthiques notamment, les institutions de recherche conditionnent également la réutilisation de données non génétiques codées à l'obtention du consentement général[95]. Eu égard à la nature des données, la LRH établit également un système d'*opt-out* pour l'anonymisation des données génétiques, c'est-à-dire que les données génétiques ne peuvent être anonymisées (si tant est qu'elles puissent l'être !) à des fins de recherche seulement si la personne ne s'y est pas opposée après en avoir été informée.

L'information qui doit être fournie aux personnes concernées dans les différents types de situations (réutilisation pour une recherche particulière, à des fins de recherche ou pour l'anonymisation de données génétiques) est décrite en détail aux art. 28 ss ORH. Des travaux successifs menés notamment sous l'égide de l'*Académie Suisse des Sciences Médicales* (ASSM), de *swissethics* et de l'*Association Médecine Universitaire Suisse* (*unimedsuisse*) ont permis d'établir un modèle unifié de consentement général[96]. En pratique, la mise en œuvre de ce dernier diffère toutefois selon les hôpitaux.

Lorsque les conditions de réutilisation exposées aux art. 32 et 33 LRH ne sont pas réunies, en particulier lorsque le consentement des personnes concernées

ultérieure, fournir des services d'analyse à un tiers ou mener une analyse pilote en vue d'une étude de plus grande ampleur.

92 Art. 32 al. 1 LRH.

93 Art. 32 al. 2 et 33 al. 1 LRH.

94 Art. 33 al. 2 LRH.

95 Pour plus de détails sur cette question : SPRUMONT/TALANOVA, p. 246 s.

96 Consultable ici : <www.unimedsuisse.ch/fr/projets/consentment-general>.

fait défaut, l'art. 34 LRH permet de déroger « *à titre exceptionnel* » aux conditions de réutilisation imposées par la loi[97]. Pour ce faire, le chercheur doit démontrer que l'obtention du consentement est impossible ou pose des difficultés disproportionnées, qu'aucun document n'atteste le refus de la personne concernée et que l'intérêt de la science prime celui de la personne concernée à décider de la réutilisation de son matériel biologique ou de ses données. Les conditions posées par l'art. 34 LRH doivent être interprétées de manière restrictive[98].

Dans tous les cas, si les conditions de réutilisation des données sont réunies, il convient encore de prendre toutes les mesures nécessaires pour encadrer juridiquement le partage des données personnelles. Les parties en présence devront notamment conclure un contrat de partage de données (*Data Sharing Agreement* ou *Data Transfer and Use Agreement*) qui doit entre autres assurer que le destinataire des données ne les utilisera que pour les buts convenus et prendra toutes les mesures pour en garantir la sécurité[99]. En Suisse, le *Swiss Personalized Health Network* (SPHN) a développé, d'entente avec des institutions de recherche helvétiques, des modèles de contrats de partage de données qui sont disponibles en ligne[100].

b) Critique du système

Au cours des dernières années, la systématique légale imposée par la LRH pour la réutilisation des données à des fins de recherche a fait l'objet de critiques régulières. On a notamment reproché au système de reposer sur des distinctions entre données qui sont difficiles à opérer (p. ex. : données génétiques *vs* données non génétiques)[101], de se trouver en inadéquation avec les réalités de la recherche actuelle qui doit composer avec des données innombrables générées d'innombrables contextes (p. ex. : *smartphones*, *wearables*) et pour lesquelles il serait difficile d'obtenir des consentements éclairés[102], ou encore de voir les déficiences du système compensées par un large recours à l'art. 34 LRH alors que cette disposition a été conçue comme une exception[103]. Sur la base de ces différents arguments, il a notamment été proposé de basculer vers un système d'*opt-out général* qui partirait du principe que les données

97 Pour une analyse des conditions de l'exception prévue par l'art. 34 LRH, voir notamment : DRIESSEN/CHRISTEN/GERVASONI ; SPRUMONT/TALANOVA.
98 THOUVENIN *et al*., N 19.
99 Pour de plus amples informations sur le cadre contractuel du partage de données de recherche : JOTTERAND/ERARD.
100 <www.sphn.ch/dtua>.
101 JUNOD/ELGER, N 20.
102 MÄTZLER, N 59.
103 THOUVENIN *et al*., N 21 ; MÄTZLER, N 59.

peuvent être réutilisées à des fins de recherche sauf si les personnes concernées s'y sont opposées[104] ou encore d'introduire un nouveau « privilège » de la recherche dans le domaine de la recherche sur l'être humain, en s'inspirant des dispositions relatives aux traitements de données ne se rapportant pas à des personnes dans les législations générales sur la protection des données[105].

D'autres auteurs rejettent à l'inverse certaines de ces critiques et défendent le système du consentement général[106]. S'appuyant sur l'art. 118*b* Cst. ainsi que sur la jurisprudence de la Cour européenne des droits de l'homme[107], ils rappellent le rôle cardinal du consentement dans la recherche et la nécessité de respecter un éventuel refus de participer à une recherche. Ils se réfèrent notamment à des études montrant un taux d'acceptation du consentement général qui varie entre 80 et 85 %[108]. Cela signifie à la fois qu'une partie importante de la population accepte de mettre ses données médicales à disposition de la recherche, mais aussi qu'une part non négligeable s'y oppose et que ce choix doit être respecté. Par ailleurs, le consentement général ayant été introduit en 2014, la quantité de données disponibles ne cesse de croître d'année en année et réduit dans les faits la nécessité de recourir à la clause d'exception de l'art. 34 LRH.

Je partage l'avis selon lequel les catégories de données établies par la LRH sont difficiles à manier, en particulier lorsqu'il faut distinguer les données génétiques des données non génétiques ou les données de santé des autres données. Une réflexion de fond devrait être menée sur cette question en vue d'offrir une meilleure sécurité juridique. En ce qui concerne le consentement général, il constitue pour sa part une approche équilibrée pour la réutilisation de données à des fins de recherche, tout particulièrement lorsque les données concernées sont collectées dans le contexte médical. Bien que le consentement général ne soit pas exempt de défauts (p. ex. : visibilité limitée sur la réutilisation concrète des données dans le futur), il permet néanmoins d'assurer une information minimale aux personnes concernées et leur offre surtout une possibilité efficace de s'opposer à une réutilisation non souhaitée, conformément au principe d'autodétermination. Les exigences liées à la gestion du consentement général n'apparaissent pas superflues si l'on garde à l'esprit que la réutilisation des données de santé à des fins de recherche implique souvent des dérogations importantes au secret médical. Or, le bon fonctionnement de ce dernier repose non seulement sur la protection individuelle de la vie privée des patients, mais aussi sur la confiance du public à l'égard des professions de soins et des institutions de santé. Il ne doit donc être limité qu'à des conditions restrictives. Un système de

104 JUNOD/ELGER, N 21 ss.
105 THOUVENIN *et al*., N 32 ; MÄTZLER, N 60.
106 SPRUMONT/TALANOVA, p. 250 s.
107 CourEDH, Arrêt du 13 janvier 2015, *Elberte c. Lettonie*, nº 61243/08 (dans le contexte d'une transplantation de tissus).
108 SPRUMONT/TALANOVA, p. 249.

consentement à la réutilisation des données médicales à des fins de recherche, même donné de manière générale, offre les garanties minimales pour préserver cette confiance. On notera par ailleurs que le Conseil fédéral a récemment proposé de moderniser les modalités du consentement avec un consentement qui, sous certaines conditions, pourrait être donné de manière électronique[109].

De manière plus générale, il serait par ailleurs réducteur de concentrer les problèmes de réutilisation des données à des fins de recherche sur le seul consentement général. Comme le montrent certaines études récentes, la réutilisation efficace des données à des fins de recherche en Suisse dépend aussi de nombreux autres facteurs, à l'instar du développement d'infrastructures pour le partage de données, de la création d'incitatifs au partage de données (p. ex. : reconnaissance appropriée des institutions qui fournissent les données) ou du comportement des détenteurs de données qui est en bonne mesure influencé par les risques induits par le partage de données (non seulement les risques pour la vie privée des personnes concernées ou le respect des législations sur la protection des données personnelles, mais aussi les risques liés à la divulgation d'informations sur les pratiques internes ou les performances par exemple)[110]. En Suisse, des efforts importants ont été fournis au cours des dernières années pour favoriser le partage de données de recherche biomédicales, en particulier à travers les initiatives de SPHN. Celles-ci comprennent par exemple la mise en place d'une infrastructure informatique fédérée et sécurisée pour le partage de données de santé sensibles (réseau *BioMedIT*[111]), l'adoption de standards éthiques[112] et de sécurité des données[113], un cadre d'interopérabilité sémantique[114], un outil permettant d'explorer l'existence de données disponibles pour la recherche dans les cinq hôpitaux universitaires helvétiques (*Federated Query System*[115]) ou encore le développement de modèles de contrats pour le partage de données et les collaborations de recherche[116].

109 <www.bag.admin.ch/bag/fr/home/medizin-und-forschung/forschung-am-menschen/revision-verordnungen-hfg.html.>
110 MARTANI *et al*., p. 12 ss.
111 <www.biomedit.ch>.
112 SPHN, Ethical Framework for Responsible Data Processing in Personalized Health Research, v. 2, 7 mai 2018.
113 SPHN, SPHN/BioMedIT Information Security Policy, v. 2, 8 octobre 2020.
114 <https://sphn.ch/network/data-coordination-center/the-sphn-semantic-interoperability-framework/>
115 <www.sphn.ch/fqs>.
116 <www.sphn.ch/dtua>.

c) Perspectives législatives

Les enjeux importants liés à la réutilisation des données de santé, notamment à des fins de recherche, donnent actuellement lieu à différentes initiatives législatives au niveau suisse et européen.

En mai 2022, la Commission européenne a publié une proposition de règlement créant un nouvel espace européen des données de santé (*European Health Data Space*, EHDS)[117]. Ce texte vise entre autres à régler l'utilisation secondaire des données de santé électroniques, en obligeant de nombreux détenteurs de données de santé à mettre ces données à disposition pour certains types de réutilisation. Les réutilisations autorisées comprendraient par exemple la recherche scientifique ayant trait aux secteurs de la santé ou le développement d'algorithmes, de systèmes d'IA ou d'applications de santé numériques. L'EHDS établirait un nouveau système de gouvernance où des organismes désignés par les États valideraient les requêtes d'accès[118].

En Suisse, le Conseil fédéral a rendu en mai 2022 un long rapport sur la réutilisation des données médicales[119]. Celui-ci recommande la mise en place d'un « *espace de données* », défini comme « *la structure des relations entre les acteurs des données, c'est-à-dire les personnes concernées, les producteurs de données/responsables et les utilisateurs secondaires de données* »[120]. Un tel espace de données impliquerait la prise en compte d'aspects techniques, juridiques ou sémantiques, mais aussi le développement d'une culture commune de réutilisation des données. Pour ce faire, le rapport propose la mise en place d'un système national de réutilisation et d'appariement des données médicales à des fins de recherche, qui impliquerait entre autres la mise en place d'un organe national de coordination des données, un catalogue de métadonnées, ainsi qu'une infrastructure sûre pour le traitement et l'enregistrement des données[121].

Plus récemment, la Commission de la science, de l'éducation et de la culture du Conseil des États a déposé une motion pour charger le Conseil fédéral de « *créer, dans une loi-cadre, les bases nécessaires afin que des infrastructures spécifiques permettant de réutiliser des données dans les domaines stratégiques soient rapidement développées et mises en place* »[122]. Cette motion appelle l'adoption d'une approche réglementaire pragmatique pour établir des

117 <https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_fr>.
118 Pour un résumé des contours de la proposition d'EHDS : HEUSGHEM/PARISATO.
119 CONSEIL FÉDÉRAL, Rapport Humbel.
120 CONSEIL FÉDÉRAL, Rapport Humbel, p. 25.
121 CONSEIL FÉDÉRAL, Rapport Humbel, p. 34 ss.
122 Motion de la Commission de la science, de l'éducation et de la culture du Conseil des États, nº 22.3890, « Élaboration d'une loi-cadre sur la réutilisation des données » du 22 août 2022.

espaces de données communs et fiables, qui ne serait toutefois pas limitée à la santé et qui pourrait s'étendre à tout secteur stratégique (recherche, énergie, formation, environnement, *etc.*). La future loi-cadre devrait en particulier régler « *le pilotage des infrastructures de données par des organisations publiques ou d'économie mixte, leur financement, le traitement, l'accessibilité et le croisement des données issues de sources publiques et privées, l'application de la protection des données et de la sécurité des données lors de l'utilisation secondaire des données et l'interopérabilité des infrastructures sectorielles d'utilisation des données* ». La motion a été adoptée par les deux conseils et a été transmise au Conseil fédéral. Les efforts pour donner l'impulsion à un tel projet de loi en Suisse doivent être salués. Dans la mesure où la loi-cadre devrait régler certains aspects liés aux traitements de données personnelles, l'un des défis consistera certainement à fonder les compétences législatives de la Confédération pour adopter une loi-cadre globale, qui doit aussi permettre d'englober les opérations liées aux données personnelles traitées par les organes publics cantonaux. C'est peut-être pour cette raison que la motion insiste sur le développement d'« infrastructures » plutôt que sur la création d'un véritable « espace » de données.

IV. Conclusion

Les considérations qui précèdent offrent panorama général et non exhaustif des règles en matière de réutilisation de protection des données personnelles dans le contexte de la recherche. Les aspects liés à l'utilisation primaire des données, à l'image des modalités de traitement de données collectées dans le contexte d'un essai clinique spécifique ont notamment été mis de côté. Des conclusions générales sur la protection des données personnelles peuvent cependant être tirées de cette analyse générale.

Le constat le plus évident est typique du système fédéral helvétique et tient au caractère particulièrement morcelé des législations applicables. De manière générale, lorsqu'on évoque les grands obstacles au partage de données, on regrette souvent l'existence de « silos » de données, ce par quoi il faut entendre l'absence de connexions ou d'interopérabilité entre des bases de données existantes. À regarder le paysage juridique helvétique en matière de protection des données et de recherche, on pourrait tout aussi bien y voir des « silos législatifs ».

L'ensemble des législations examinées prévoient des assouplissements pour les traitements de données à des fins de recherche, mais les conditions de ces « privilèges » de la recherche varient selon l'auteur du traitement (personne privée, organe public fédéral, organe public cantonal) ou la nature de l'activité exercée (recherche sur l'être humain ou non). Les chercheurs qui naviguent dans cet archipel législatif ont par conséquent tout intérêt à vérifier soigneusement

le droit qui s'applique à leurs traitements de données, si besoin en recourant aux services de conseillers juridiques.

Comme on l'a vu, le régime de réutilisation des données à des fins de recherche sur l'être humain fait quant à lui l'objet d'un certain nombre de critiques, parfois à juste titre. Le système des art. 32 à 34 LRH repose en effet sur des catégories de données qui sont difficiles à distinguer et qui ont probablement perdu de leur légitimité en raison des avancées de la science et des nouvelles technologies. Cette systématique devrait être repensée et simplifiée. En dépit des critiques, le système du consentement général présente quant à lui une solution équilibrée qui favorise mise à disposition de données de santé toujours plus nombreuses en permettant aux personnes concernées de se déterminer par rapport à une réutilisation à des fins de recherche.

Il est par ailleurs primordial d'élargir la réflexion à l'ensemble des facteurs qui permettront de favoriser le partage des données à des fins de recherche, parmi lesquels figurent l'existence d'infrastructures adéquates, la volonté des détenteurs de données ou la reconnaissance adéquate de ces derniers. Dans le domaine biomédical, l'initiative SPHN a par exemple fourni des efforts importants pour améliorer les conditions-cadres de partage de données au cours des dernières années. Quant aux obstacles dressés par la protection des données, ils ne devraient pas être considérés comme rédhibitoires « par défaut ». Aujourd'hui, de nombreuses technologies respectueuses de la vie privée (*privacy-enhancing technologies*) sont en cours de développement pour « partager sans partager », notamment par le biais d'analyses fédérées, de création de données synthétiques présentant des propriétés statistiques similaires aux données originales ou de techniques de chiffrement des données qui permettent d'opérer des calculs statistiques sur ces dernières (chiffrement homomorphique)[123]. Un partage des données de recherche efficace et respectueux des participants passe par un partenariat étroit entre le droit et la technologie.

Enfin, on constate une activité législative dynamique aussi bien à l'échelon européen avec l'EHDS qu'au niveau suisse avec la proposition d'une loi-cadre sur la réutilisation des données. Il conviendra de suivre de près ces évolutions législatives, en souhaitant qu'elles permettent de favoriser les partages de données et les avancées scientifiques tout en garantissant la protection et l'autodétermination des participants, ainsi que la nécessaire confiance de la population à l'égard des milieux de la recherche.

[123] Pour un état des lieux récent de ces technologies et des exemples d'application concrets : Office of Science and Technology Policy, National strategy to advance privacy-preserving data sharing and analytics, mars 2023. Pour un bref aperçu, voir aussi : ERARD/HEUSGHEM/PARISATO, N 54 ss.

V. Bibliographie

A. Littérature

Hélène BRUDERER, La réutilisation des données personnelles liées à la santé à des fins de recherche scientifique. Étude de droit suisse avec des perspectives de droit comparé, thèse Genève, Zurich 2023 ; **Susanne DRIESSEN/Andri CHRISTEN/Pietro GERVASONI**, Humanforschung, Weiterverwendung und informierte Einwilligung. Analyse zur Weiterverwendung von gesundheitsbezogenen Personendaten und biologischem Material sowie Anwendung von Artikel 34 HFG, Jusletter 1er février 2021 ; **Philippe DUCOR**, La protection de la personnalité des sujets de recherche, Jusletter 26 janvier 2015 ; **Frédéric ERARD**, Les données codées dans le contexte de la recherche : personnelles ou anonymes ?, AJP/PJA 2021/5, p. 606 ss (cité : ERARD, Les données codées) ; **Frédéric ERARD/Mathilde HEUSGHEM/Clément PARISATO**, Recherche biomédicale et Open Data. Perspectives en droit suisse, Jusletter 30 janvier 2023 ; **Frédéric ERARD/Alexandre JOTTERAND**, Recherche sur l'être humain et données personnelles. Gestion des échanges et répartition des responsabilités, Jusletter 30 août 2021 ; **Alexandre FLÜCKIGER**, L'autodétermination en matière de données personnelles : un droit (plus) si fondamental à l'ère digitale ou un nouveau droit de propriété ?, AJP/PJA 2013/6, p. 837 ss ; **Mathilde HEUSGHEM/Clément PARISATO**, La proposition de règlement EHDS : nouvel instrument de l'Union à fort potentiel, 17 mai 2023 *in* www.swissprivacy.law/227 ; **Alexandre JOTTERAND**, Personal Data or Anonymous Data: where to draw the lines (and why)?, Jusletter 15 août 2022 ; **Valérie JUNOD/Bernice ELGER**, Données codées, non-codées ou anonymes : des choix compliqués dans la recherche médicale rétrospective, Jusletter 10 décembre 2018 ; **Samuel MÄTZLER**, Datenschutz in der (Human-) Forschung: Grundlagen und Probleme bei der Sekundärnutzung von Personendaten, Jusletter 30 janvier 2023 ; **Vincent MARTENET/Jacques DUBEY** (éds), Constitution fédérale I, Commentaire romand, Bâle 2021 (cité : CR Cst. I-AUTEUR, art. X, N Y) ; **Urs MAURER-LAMBROU/Blechta GABOR-PAUL** (éds), Datenschutzgesetz. Öffentlichkeitsgesetz, Basler Kommentar, 3e éd., Bâle 2014 (cité : BSK DSG-AUTEUR, art. X, N Y) ; **Andrea MARTANI *et al.***, Sensing the (digital) pulse. Future steps for improving the secondary use of data for research in Switzerland, Digital Health, vol. 9, 20 avril 2023 ; **Philippe MEIER**, Protection des données, Berne 2010 ; **Dominique SPRUMONT/Vladislava TALANOVA**, La recherche sans consentement : l'exceptionnelle exception, *in* Evelyne CLERC/Jean-Philippe DUNAND/Dominique SPRUMONT (éds), Alea jacta est : Santé ! Mélanges en l'honneur d'Olivier Guillod, Bâle 2021, p. 235 ss ; **Bernhard RÜTSCHE**, Humanforschungsgesetz (HFG). Bundesgesetz vom 30. September 2011 über die Forschung am Menschen, Berne 2015 (SHK HFG-AUTEUR, art. X, N Y) ; **Florent THOUVENIN/Thomas GÄCHTER/Kento REUTIMANN/Samuel MÄTZLER**, Datenschutz in der Humanforschung: ein Forschungsprivileg für die Sekundärnutzung von Personendaten, Jusletter 30 janvier 2023 (cité : THOUVENIN *et al.*).

B. Documents officiels

Commission européenne/DG Health and Food Safety, Assessment of the EU Member States' rules on health data in the light of GDPR, Luxembourg: Publications Office of the European Union, 2021 (cité : Commission européenne, Assessment of the EU Member States' rules on health data in the light of GDPR) ; **Conseil de l'Europe**, Rapport explicatif du

Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 10 octobre 2018 ; **Conseil fédéral**, Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988, FF 1988 II 421 ss (cité : Message aLPD) ; **Conseil fédéral**, Message relatif à l'article constitutionnel concernant la recherche sur l'être humain du 12 septembre 2007, FF 2007 6345 ss (cité : Message article constitutionnel recherche) ; **Conseil fédéral**, Message sur la loi fédérale relative à la recherche sur l'être humain du 21 octobre 2009, FF 2009 7259 ss (cité : Message LRH) ; **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, FF 2017 6565 ss (cité : Message nLPD) ; **Conseil fédéral**, Rapport du Conseil fédéral donnant suite au postulat 15.4225 Humbel du 18 décembre 2015, Mieux utiliser les données médicales pour assurer l'efficience et la qualité des soins, 4 mai 2022 (cité : Rapport Humbel) ; **Office of Science and Technology Policy**, National strategy to advance privacy-preserving data sharing and analytics, mars 2023 ; **Swissethics**, Assurance de la qualité ou recherche soumise à autorisation ?, v. 1.0, 4 février 2020.

Protection des données et recherche

Le droit des personnes concernées

RACHEL CHRISTINAT
Avocate et Docteure en droit

Table des matières

I. Introduction

La protection des données dans le domaine de la recherche est un sujet particulièrement intéressant, car il confronte des intérêts communément considérés comme étant louables. En effet, l'intérêt privé de tout individu à la protection de ses données personnelles est incontesté en tant que tel, mais il en va de même de l'intérêt public de la recherche et du progrès. Une personne privée préférera souvent que les scientifiques ne s'emparent pas de ses données librement, donc sans qu'elle y ait consenti. Ceci est d'autant plus vrai en ce qui concerne les données sensibles. À l'inverse, l'accès à des données personnelles et sensibles est indispensable à la conduite de la plupart des études. L'échange de données déjà collectées entre des centres de recherche et des projets de recherches multicentriques contribuent notablement aux percées scientifiques. *A priori*, des données collectées, qui ne permettent pas à celles et ceux qui les traitent d'identifier la personne concernée grâce à une opération préalable d'anonymisation ou de pseudonymisation, devraient pouvoir être échangées facilement dans le milieu scientifique. Or les experts du domaine révèlent que toutes les avancées technologiques, notamment le développement de l'informatique couplé au *big data*, offrent désormais des possibilités d'analyse tellement puissantes que l'appariement de données permet dans certains cas de rétablir un lien avec la

personne concernée[1]. Le risque de causer une atteinte à la personnalité est ainsi tangible. Au travers de ses normes juridiques, la société doit par conséquent arbitrer ce conflit délicat et passionnant. La présente contribution s'inscrit dans ce vaste sujet, en se focalisant sur les droits des personnes concernées. Le propos est donc orienté puisqu'il vise la protection de ces dernières.

Dans le domaine de la recherche sur l'être humain en particulier, la Confédération légifère dans la mesure où la protection de la dignité humaine et de la personnalité l'impose (art. 118*b* Cst.). La pesée des intérêts entre la dignité humaine et la protection de la personnalité d'un côté et la liberté de la recherche de l'autre est par conséquent déjà révélée par le mandat constitutionnel délivré à la Confédération[2]. Cette dernière doit veiller à la liberté de la recherche et considérer son importance pour la santé et la société. Le droit constitutionnel exige le consentement éclairé de la personne qui participe à la recherche, sauf exception légale et il reconnaît qu'un refus est toujours contraignant (art. 118*b* al. 2 let. a Cst.). Le droit à l'autodétermination du sujet de recherche constitue ainsi l'un des principes directeurs de la recherche sur l'être humain[3]. DUCOR observe que la législation sur la recherche relative à l'être humain distingue trois types d'études. Le premier cause les risques les plus élevés pour la dignité humaine et pour la liberté personnelle. Il s'agit des essais cliniques. Le deuxième type englobe la collecte de données personnelles liées à la santé (ou le prélèvement de matériel biologique) sans intégrer d'intervention liée à la santé. Enfin, le troisième type d'études réutilise des données déjà collectées (ou du matériel biologique déjà prélevé). Selon l'auteur, ils occasionnent seulement un risque limité pour la dignité et pour la personnalité des personnes concernées[4]. Nous verrons que la gradation du risque se retrouve dans la réglementation.

Les réflexions principales de la présente contribution portent sur les conditions auxquelles la chercheuse et le chercheur peuvent utiliser les données de la personne concernée, sur les moyens de vérification dont cette dernière dispose et sur les mesures qu'elle peut prendre en cas de violation de la protection de ses données. Comme elles se posent dans tout traitement de données intervenant à l'occasion d'une recherche, ces questions constituent une sorte de tronc commun. Néanmoins, les dispositions qui permettent d'y répondre sont éparpillées

1 Pour des exposés détaillés du conflit entre les intérêts des personnes concernées et ceux des chercheuses et des chercheurs, se référer à DUCOR, p. 190 ; ERARD, p. 613 s ; ERARD/HEUSGHEM/PARISATO, N 1 ss (qui développent les intérêts de la recherche et exposent notamment les principes de l'*Open Science*, de l'*Open Data* et de l'*Open Research Data*, en les mettant en perspective avec les risques d'atteinte aux droits de la personne concernée) et N 19 ss.

2 DUCOR, p. 167.

3 ERARD, p. 614.

4 DUCOR, p. 183.

dans plusieurs textes légaux. Sans doute s'agit-il là d'une difficulté conséquente de la thématique. Aussi, les juristes doivent constamment conserver à l'esprit une arborescence qui leur permet d'identifier le droit applicable aux circonstances d'un cas d'espèce.

Le premier embranchement distingue les données personnelles des données non personnelles, que l'on désigne « données anonymes ». En principe, les règles sur la protection des données couvrent uniquement les premières. Les secondes peuvent être appréhendées tout au plus par des dispositions générales, comme le secret professionnel, ou par des clauses contractuelles. Certaines exceptions relativisent néanmoins ce principe.

Lorsque la recherche utilise des données personnelles, la deuxième ramification sépare la législation générale sur la protection des données des lois spéciales sur la recherche sur l'être humain d'une part et sur l'analyse génétique humaine d'autre part. En effet et conformément aux principes généraux de l'interprétation du droit, les secondes priment si elles posent des règles spécifiques à la protection des données[5]. Pour faciliter la présentation de la matière, nous commencerons systématiquement par exposer les règles générales avant les règles spéciales. Confronté à un cas pratique, il convient cependant de vérifier en premier si des dispositions spéciales sont pertinentes avant de se focaliser sur les normes générales.

La présente contribution examine de façon transversale les réflexions en lien avec les droits de la personne concernée. De ce fait, elle énonce les conditions de traitement des données dans le cadre d'une recherche (*infra* III), puis elle énumère les moyens à disposition d'une personne concernée pour vérifier si ses données sont traitées conformément au droit (*infra* IV), et elle développe les mesures dont la personne dispose en cas de violation de la protection de ses données (*infra* V). Avant d'entrer dans le cœur du sujet, nous commençons par présenter le droit applicable (*infra* II), ce qui nous amènera à définir les données anonymes car elles échappent à la réglementation sur la protection des données.

II. Droit applicable

A. LPD, LRH, LAGH et droit cantonal

La matière est présentée ici succinctement pour que la lectrice et le lecteur disposent d'un raisonnement complet. Nous renvoyons pour les détails à la contribution de ERARD qui la développe de manière approfondie[6].

5 ROSENTHAL, p. 169.
6 Voir dans cet ouvrage, ERARD, p. 1 ss.

Face à une problématique de protection des données, le premier texte légal qui se presse à l'esprit est évidemment la loi fédérale sur la protection des données[7]. Selon l'article 2, ce texte réglemente effectivement le traitement de données personnelles concernant des personnes physiques qui est effectué par les personnes privées, par exemple les industriels, et par les organes fédéraux, comme les écoles polytechniques fédérales. *A contrario*, le traitement de données par des organes cantonaux, tels que les universités et les hôpitaux universitaires, est régi par le droit cantonal[8].

Lorsque la recherche porte sur les maladies humaines ou sur la structure et le fonctionnement du corps humain et qu'elle est pratiquée sur des données personnelles liées à la santé, la loi relative à la recherche sur l'être humain[9] s'applique en tant que loi spéciale (art. 2 al. 1 let. e LRH)[10]. Cette loi ne couvre donc pas toutes les recherches. Le traitement de données personnelles sans lien avec la santé qui porterait sur le racisme, la religion, l'économie ou le droit est exclu de son champ d'application[11].

La loi sur l'analyse génétique humaine[12] entre en considération dans le contexte particulier des analyses génétiques et prénatales humaines ainsi que des données qui en sont issues. Ainsi, les règles fédérales et cantonales en matière de protection des données régissent aussi le traitement des données génétiques, à moins que la loi spéciale aille au-delà[13]. Si des données génétiques sont utilisées dans le cadre d'une recherche, leur traitement peut cependant être soumis à la loi sur la recherche sur l'être humain. En effet, l'article 2 al. 4 LAGH soumet expressément les analyses génétiques humaines et prénatales réalisées dans le cadre de la recherche sur les maladies humaines ainsi que sur la structure et le fonctionnement du corps humain à la loi sur la recherche, de sorte que les données génétiques traitées à des fins de recherches sont protégées par cette dernière[14]. Dans ce contexte, il est intéressant de citer l'article 12 LAGH qui pose des conditions à la réutilisation de données génétiques à des fins de recherche. Une interprétation uniquement littérale de la loi pourrait laisser penser à tort que cette disposition appréhende toute recherche. Or, l'analyse systématique s'oppose à cette interprétation, ce que le message confirme : « *S'agissant de l'utilisation des échantillons et des données génétiques à des fins de recherche sur les maladies humaines et sur la structure et le fonctionnement du corps humain,*

7 Loi fédérale du 25 septembre 2020 sur la protection des données (LPD), RS 235.1.
8 ERARD/HEUSGHEM/PARISATO, N 23 ; THOUVENIN et *al*., N 9.
9 Loi fédérale du 30 septembre 2011 relative à la recherche sur l'être humain (Loi relative à la recherche sur l'être humain, LRH), RS 810.30.
10 ERARD, p. 613 ; THOUVENIN et *al*., N 13 s.
11 DUCOR, p. 175.
12 Loi fédérale du 15 juin 2018 relative à l'analyse génétique humaine (LAGH), RS 810.12.
13 Message LAGH, p. 5323.
14 Message LAGH, p. 5325.

le droit à l'autodétermination de la personne concernée est déjà protégé par la LRH ; c'est pourquoi la présente disposition n'est pas applicable en la matière […]. *En référence à celle-ci, il est justifié d'inscrire aussi dans la LAGH une norme analogue de protection matérielle des données pour l'utilisation à d'autres fins que la recherche au sens de la LRH* »[15]. Par conséquent, l'article 12 LAGH régit la réutilisation de données génétiques à des fins de recherche qui ne porte pas sur les maladies humaines ainsi que sur la structure et le fonctionnement du corps humain. Il peut s'agir par exemple d'une étude conduite sur le « *développement technique d'appareil de laboratoire, de méthodes d'analyses ou de moyens informatiques* »[16].

Certains types de données sont cependant exclus du champ d'application des lois précitées. À cet égard, la loi fédérale sur la protection des données régit le traitement de données personnelles (art. 2), soit toutes les informations concernant une personne physique identifiée ou identifiable (art. 5 let. a). Les données anonymisées sortent par conséquent du champ d'application de la loi. L'article 2 al. 2 let. c LRH exclut les données liées à la santé qui ont été collectées anonymement ou qui ont été anonymisées[17]. Ces deux lois sont donc cohérentes quant au type de données écartées et le traitement de données anonymes se dérobe de leur champ d'application[18]. Il convient par conséquent de définir la notion de « données anonymes » pour maîtriser l'étendue des lois précitées (*infra* B).

B. Données anonymisées

Dans la LPD, les données anonymes se définissent par opposition à celles qui sont personnelles. Ces dernières couvrent toutes les informations qui se rapportent à une personne physique identifiée ou identifiable (art. 5 let. a). Dans son message, le Conseil fédéral précise qu'une corrélation d'informations issues du contexte ou tirées des circonstances suffit. Il cite le numéro d'identification, les données de localisation, les éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de la personne. En outre, l'identification peut résulter non seulement d'un seul élément comme le numéro de téléphone ou les empreintes digitales mais encore du recoupement de plusieurs données telles que l'adresse, la date de naissance et l'état civil. Le message mentionne ensuite qu'une possibilité purement théorique d'identifier une personne, c'est-à-dire lorsqu'une identification nécessiterait des moyens tels qu'on ne les déploierait pas dans le cours ordinaire des choses, est insuffisante. L'appréciation d'une situation concrète doit considérer les

15 Message LAGH, p. 5325.
16 Message LAGH, p. 5326.
17 ERARD, p. 607 ; ERARD/HEUSGHEM/PARISATO, N 26.
18 ERARD/HEUSGHEM/PARISATO, N 28.

moyens raisonnablement utilisés pour identifier la personne. Ceux-ci dépendent de toutes les circonstances et en particulier du coût, du temps nécessaire ainsi que des technologies accessibles lors du traitement des données et de leur évolution[19].

L'article 3 let. i LRH est le point de départ du raisonnement dans le domaine de la recherche sur l'être humain. Selon cette disposition, les données anonymisées liées à la santé sont celles qui ne peuvent pas être mises en relation avec une personne déterminée ou qui ne peuvent pas l'être sans engager des efforts démesurés. L'article 35 charge le pouvoir exécutif de préciser les exigences auxquelles doivent répondre l'anonymisation et le codage des données, ainsi que les conditions de leur décodage[20]. Usant de sa compétence, le Conseil fédéral a défini que l'anonymisation de données personnelles commande que toutes les informations qui, combinées, permettent de rétablir l'identité de la personne sans efforts disproportionnés doivent être rendues définitivement méconnaissables ou être détruites ; il a précisé qu'il s'agit en particulier du nom, de l'adresse, de la date de naissance et des numéros d'identification caractéristiques (art. 25 ORH[21]). Le caractère démesuré des efforts est admis si l'on ne doit pas s'attendre qu'un tiers intéressé les initie[22]. Chaque cas particulier doit être évalué selon le contexte[23]. ERARD observe que « *pour mener cette appréciation, il faut non seulement prendre en considération l'importance des moyens techniques à déployer, mais aussi l'intérêt propre de celui qui souhaiterait réidentifier les données, voire la durée de conservation prévue des données. À l'inverse, l'engagement du destinataire des données de ne pas tenter de réidentifier les données n'a pas d'influence sur le caractère anonyme ou non d'une donnée. Eu égard aux évolutions technologiques (big data, intelligence artificielle), du caractère toujours moins onéreux de l'accès à ces technologies et à l'augmentation du nombre de bases de données disponibles, la nécessité de déployer des efforts disproportionnés pour rattacher des données à une personne particulière ne saurait toutefois être reconnue facilement* »[24].

La doctrine spécialisée relève qu'une anonymisation absolue est désormais impossible en raison des avancées technologiques[25]. Le législateur se contente par conséquent d'une anonymisation de fait[26].

19 Message sur la révision totale de la LDP, p. 6639 s.
20 ERARD, p. 608.
21 Ordonnance relative à la recherche sur l'être humain à l'exception des essais cliniques (Ordonnance relative à la recherche sur l'être humain, ORH) du 20 septembre 2013, RS 810.301.
22 ERARD, p. 608.
23 ERARD/HEUSGHEM/PARISATO, N 30.
24 ERARD, p. 608 s et les nombreuses références citées par l'auteur.
25 DUCOR, p. 191 et n. 144 ; TALANOVA/SPRECHER, p. 1197.
26 ERARD, p. 608.

C. Données codées (ou pseudonymisées)

La difficulté saillante a trait aux données qui ne sont pas purement anonymes ou anonymisées mais qui sont codées, soit les données dites pseudonymisées. En effet, le codage implique le remplacement des données caractéristiques qui permettent l'identification d'un individu[27]. Celles et ceux qui détiennent la clé peuvent néanmoins remonter aux données personnelles, de sorte que le processus est réversible[28]. L'examen du droit applicable requiert par conséquent de déterminer si les données pseudonymisées sont réputées anonymes ou pas pour les personnes qui ignorent la clé d'identification.

Deux approches s'envisagent. Selon l'approche absolue, une donnée ne peut pas être qualifiée d'anonyme tant que la réidentification de la personne source au moyen d'une clé est possible pour l'un des acteurs de la communication. Le fait qu'un seul acteur dispose du code implique que la donnée est qualifiée de « donnée personnelle » également pour tous les autres. À l'inverse, l'approche relative reconnaît le caractère anonyme des données pseudonymisées traitées par celles et ceux qui ne détiennent pas le code. Elle attribue le statut de données personnelles uniquement dans le cadre des traitements opérés par celles et ceux qui disposent de la clé de réidentification. Dans l'approche relative, la qualification de donnée personnelle ou pseudonymisée diffère selon que la personne qui la traite dispose ou non du code[29]. Ainsi que le relève ERARD, les individus actifs dans la recherche disposent d'un intérêt évident à pouvoir traiter librement un grand nombre de données. De ce fait, le libre accès à des banques de données pseudonymisées regroupant autant de données que possible favorise le progrès. Les études multicentriques et les échanges de données entre les institutions sont aussi de plus en plus demandées. L'approche retenue revêt ainsi une importance pratique considérable puisque l'approche absolue soustrait les données codées à la réglementation et permet un traitement libre des données. En revanche, l'approche relative soumet le traitement des données codées à la loi, même si la chercheuse ou le chercheur ne possède pas la clé. Cette approche protège par conséquent le droit à l'autodétermination de la personne source[30].

La Cour de Justice des communautés européennes a examiné si une adresse IP dynamique devait être considérée comme une donnée personnelle ou non du point de vue du fournisseur de services de médias en ligne alors que seul le fournisseur d'accès à Internet pouvait identifier l'ordinateur utilisé. Elle a admis que tel est le cas si le fournisseur de services de médias en ligne dispose

27 Art. 3 let. h LRH ; ERARD, p. 609.
28 ERARD, p. 609.
29 Pour tout le paragraphe : ERARD, p. 609 ; voir aussi ERARD/HEUSGHEM/PARISATO, N 32.
30 ERARD, p. 613 s.

de moyens légaux qui lui permettent d'obtenir l'identité la personne concernée au moyen des informations supplémentaires dont le fournisseur d'accès à Internet de cette personne dispose[31].

La LPD ne définit pas les données pseudonymisées mais en traite indirectement à l'article 31 al. 2 let. e, en considérant un traitement avec une finalité particulière. Après le rappel du principe selon lequel toute atteinte à la personnalité doit reposer sur un motif justificatif (al. 1), l'article énonce une liste exemplative d'intérêts prépondérants du responsable du traitement des données (al. 2). La lettre e consacre précisément le cas des données personnelles traitées à des fins qui ne se rapportent pas à des personnes, notamment à des fins de recherche, de planification et de statistique. Cette disposition reconnaît ainsi un intérêt supérieur au traitement de données personnelles dans un but de recherche si trois conditions sont cumulativement remplies. Premièrement, le responsable du traitement doit anonymiser les données dès que la finalité du traitement le lui permet. Si l'anonymisation est impossible ou si elle requiert des efforts disproportionnés, des mesures s'imposent pour que les personnes concernées ne puissent pas être identifiées. Selon le message, cette première condition est déjà respectée si « *les données sont communiquées sous une forme pseudonymisée et que la clé pour réidentifier la personne reste chez celui qui transmet les données (anonymisation factuelle)* »[32]. Le Conseil fédéral a donc retenu ici l'approche relative. La première condition a donc été passablement limitée, puisqu'une anonymisation en tant que telle n'est pas nécessaire. Des mesures propres à éviter la réidentification de la personne concernée par le chercheur ou la chercheuse suffisent. La deuxième condition ne concerne que les données sensibles et contraint le responsable du traitement à ne les communiquer à des tiers que sous une forme qui ne permet pas l'identification de la personne concernée. En cas d'impossibilité, il convient de prendre les mesures pour garantir que les tiers ne traiteront les données qu'à des fins ne se rapportant pas à des personnes. Enfin, la troisième condition commande une publication des résultats sous une forme qui empêche l'identification des personnes sources. À notre sens, l'interprétation de la première condition s'applique ici par analogie de sorte qu'une anonymisation factuelle devrait suffire. La doctrine adhère à l'application de l'approche relative dans le contexte de la législation générale sur la protection des données personnelles[33].

À teneur de la LRH, les données personnelles codées liées à la santé requièrent une clé pour être mises en relation avec un individu déterminé (art. 3 let. h). La

---

31 CJCE, C-582/14 arrêt du 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*. § 31 ss.

32 Message sur la révision totale de la LPD, p. 6692.

33 ERARD, p. 609 ss et p. 613 ; ERARD/HEUSGHEM/PARISATO, N 33 et les nombreuses références citées.

loi définit par conséquent la notion. Concernant en particulier les données personnelles liées à la santé, l'ordonnance précise qu'elles sont réputées correctement codées lorsqu'elles sont qualifiées d'anonymisées pour celles et ceux qui ne possèdent pas la clé[34]. Cette dernière doit être conservée séparément des données personnelles et par une personne qui n'est pas impliquée dans le projet de recherche (art. 26 ORH). À ce stade, nous pourrions penser à tort que les données pseudonymisées échappent au champ d'application de la loi relative à la recherche sur l'être humain, qui retient en réalité l'approche absolue[35]. Il faut effectivement conserver à l'esprit que cette loi confère une protection particulière à certaines données personnelles qui sont particulièrement sensibles puisqu'elles sont liées à la santé. Le risque de causer une atteinte à la personnalité s'en trouve par conséquent accru. De ce fait, la loi encadre plus étroitement la réutilisation des données liées à la santé et distingue selon qu'il s'agit de données génétiques ou pas. En bref, seule la réutilisation de données personnelles liées à la santé préalablement anonymisées échappe à la loi. La réutilisation de données personnelles liées à la santé, pseudonymisées ou non, n'est autorisée qu'à certaines conditions que nous développerons plus loin (art. 32 et 33 LRH ; *infra* III.D.*3*).

D. Synthèse intermédiaire

En bref, les données purement anonymes échappent à la loi sur la protection des données et aussi à la loi relative à la recherche sur l'être humain. Seule l'anonymisation de données génétiques pour les conserver en vue d'une nouvelle exploitation dans une recherche ultérieure est encadrée (art. 32 al. 3 LRH).

En vertu de l'application de l'approche relative, les données pseudonymisées ne sont pas couvertes par la loi sur la protection des données. La loi relative à la recherche sur l'être humain retient en revanche l'approche absolue. Le régime spécial déroge donc au système général de la protection des données sur ce point[36].

Enfin, les données personnelles sont pleinement appréhendées par les deux lois.

34 Voir aussi JOTTERAND, N 17 ss.
35 ERARD/HEUSGHEM/PARISATO, N 33.
36 ERARD, p. 615.

III. Conditions au traitement des données personnelles

A. Remarques liminaires

Avant d'entrer dans l'examen des règles plus spécifiques, nous rappelons que tout traitement de données doit se conformer aux grands principes de la loi sur la protection des données (art. 6 LPD). Au vu de l'absence de particularité pour le sujet qui nous occupe, nous nous permettons de renvoyer à la contribution d'ERARD dans le présent ouvrage collectif[37].

Au vu de la délicate pesée des intérêts antagonistes de la protection de la dignité humaine et de la liberté personnelle d'une part, et de la liberté scientifique d'autre part, le législateur s'en est d'emblée saisi. Il énonce qu'un traitement de données personnelles ne doit pas causer une atteinte illicite à la personnalité (art. 30 LPD). Il rappelle ensuite que toute atteinte à la personnalité est illicite, à moins que l'auteur puisse se prévaloir d'un motif justificatif, soit du consentement de la personne concernée, d'une base légale ou d'un intérêt privé ou public prépondérant (art. 32 al. 1 LPD)[38]. Dans la liste exemplative des intérêts prépondérants, le législateur aborde directement les données personnelles traitées à des fins qui ne se rapportent pas à des personnes, notamment dans le cadre de la recherche (art. 32 al. 2 let. c LPD). La révision de la loi a renforcé ce motif justificatif en y assortissant des conditions[39]. Le législateur a voulu tenir « *compte des possibilités offertes par les mégadonnées et de l'importance toujours plus grande du numérique dans la vie quotidienne, qui implique également une augmentation du nombre de traitements de données sensibles* »[40].

Avec cette disposition, le législateur admet que la chercheuse ou le chercheur peut se prévaloir de l'intérêt scientifique si deux conditions sont remplies de manière cumulative.

– D'une part, le responsable du traitement doit anonymiser les données dès que la finalité du traitement le permet. Dans l'hypothèse où l'anonymisation serait impossible ou exigerait des efforts disproportionnés, il est tenu de prendre les mesures appropriées pour que les personnes concernées ne puissent pas être identifiées (ch. 1). Ainsi, l'anonymisation factuelle, c'est-à-dire la pseudonymisation, suffit (*supra* II.C)[41]. Cette condition renforce le principe énoncé à l'article 6 al. 4 LPD. En effet, la violation de ce principe

37 Voir dans cet ouvrage, ERARD, p. 1 ss.

38 Il s'agit bien d'une concrétisation dans le domaine de la protection des données des principes généraux de la protection de la personnalité édifiés à l'art. 28 CC (Message sur la révision totale de la LPD, p. 6687).

39 Message sur la révision totale de la LPD, p. 6692.

40 Message sur la révision totale de la LPD, p. 6692.

41 Message sur la révision totale de la LPD, p. 6692.

cause une atteinte illicite à la personnalité, à moins que le responsable du traitement ne se fonde sur un motif justificatif. Le nouvel article 31 al. 2 let. e ch. 1 LPD empêche désormais la chercheuse ou le chercheur de justifier une violation de l'article 6 al. 4 LPD en invoquant que le traitement intervient à des fins de recherche.

– D'autre part, les résultats doivent être publiés sous une forme qui ne permet pas d'identifier les personnes concernées (ch. 3).

La lectrice et le lecteur perspicaces auront constaté qu'il manque une condition, soit celle qui est mentionnée au chiffre 2. Comme elle concerne la réutilisation de données, nous l'aborderons ci-dessous (*infra* D.). Soulignons que le législateur ne reconnaît pas le caractère prépondérant de l'intérêt de la recherche. Le texte mentionne effectivement que « *les intérêts prépondérants du responsable du traitement entrent notamment en considération* » dans les situations abordées à l'article 31 al. 2 LPD. Les motifs évoqués ne sont donc pas absolus[42], et il convient de procéder concrètement à la pesée des intérêts en présence. Cette appréciation suppose d'examiner toutes les circonstances du cas d'espèce.

B. Collecte

1. Loi sur la protection des données

Lors de la collecte de données, le responsable du traitement et le sous-traitant assument un devoir d'information envers la personne concernée (art. 19 LPD). Cette dernière doit notamment recevoir les renseignements utiles pour faire valoir ses droits. Grâce à cette information obligatoire, elle est supposée connaître l'identité et les coordonnées du responsable du traitement des données, la finalité du traitement et les éventuels destinataires, ou les catégories de destinataires, auxquels les données seront transmises (al. 2). Le message relève que l'information vise à renforcer la transparence, car la personne concernée ignore souvent que ses données sont traitées en l'absence de renseignements et ne peut pas faire valoir ses droits dans ce cas. En l'occurrence, le renforcement des droits de la personne concernée par l'amélioration de la transparence du traitement des données était l'un des buts de la révision[43].

La loi aborde spécifiquement l'hypothèse où les données ne sont pas collectées directement auprès de la personne concernée. Le responsable doit lui communiquer au moins les catégories de données traitées (art. 19 al. 3 LPD). La loi impose aussi des règles minimales dans l'hypothèse d'une communication des

42 Message sur la révision totale de la LPD, p. 6689.
43 Message sur la révision totale de la LPD, p. 6668.

données à l'étranger, auquel cas la personne concernée doit être informée sur le nom de l'État ou de l'organisme international destinataire (art. 19 al. 4 LPD).

L'article 20 LPD énonce cependant des exceptions. Certaines d'entre elles ne questionnent pas les droits de la personne concernée. Tel est le cas de la dispense d'informations si cette dernière détient déjà les renseignements ou si le traitement des données découle d'une base légale ou encore lorsque le responsable du traitement est une personne privée liée par une obligation légale de garder le secret (art. 20 al. 1 LPD)[44].

À l'inverse, d'autres exceptions heurtent *a priori* le sentiment de défense de la personne concernée. La loi dispense effectivement d'informer lorsque les données personnelles ne sont pas collectées auprès de la personne concernée si l'information est impossible à délivrer ou si elle nécessite des efforts disproportionnés (art. 20 al. 2 LPD). L'information est impossible lorsque la personne concernée n'est pas identifiable. La simple supposition que l'identification est impossible ne suffit pas, encore faut-il avoir effectué des recherches « *dans les limites du raisonnable* »[45]. À l'ère des nouvelles technologies, notamment du *big data*, de l'intelligence artificielle et de la puissance de l'informatique, il est délicat d'apprécier le contour des démarches raisonnables qui doivent être entreprises pour identifier une personne. Concernant les efforts disproportionnés, le message dispose qu'il convient d'évaluer les démarches que la personne responsable devrait mettre en œuvre par rapport au bénéfice que la personne concernée retirerait des renseignements. Le nombre de personnes concernées constitue l'un des critères. Les exceptions s'interprètent restrictivement, car il est attendu que le responsable du traitement prenne toutes les mesures nécessaires pour respecter son obligation. L'information est réputée impossible uniquement si ces efforts demeurent infructueux[46]. La défense des droits de la personne concernée commande dans ces situations d'établir les moyens et les connaissances du responsable du traitement d'une part ainsi que les accès dont elle dispose aux bases de données privées et publiques d'autre part.

Enfin, l'article 20 al. 3 LPD permet au responsable du traitement de restreindre ou de différer la communication des informations, voire d'y renoncer, dans certains cas, notamment si les intérêts prépondérants d'un tiers l'exigent. L'intérêt public de la recherche constitue très vraisemblablement un autre intérêt qui mérite d'être mis en balance avec celui de la personne concernée à être informée du traitement de ses données.

---

44 Nous ne discutons pas ici l'exception à l'information en lien avec les restrictions au droit d'accès aux médias à caractère périodique (art. 20 al. 1 let. d *cum* art. 27 LPD) qui n'a pas d'effet sur le sujet de la contribution.

45 Message sur la révision totale de la LPD, p. 6671.

46 Message sur la révision totale de la LPD, p. 6671.

Le traitement des données par les organes fédéraux répond à des règles précises (art. 33 ss LPD). Nous renonçons à présenter ici l'ensemble du dispositif et nous limitons aux particularités en lien avec la recherche. L'article 39 LPD consacre spécifiquement le traitement de données par des organes fédéraux à des fins qui ne se rapportent pas à des personnes, notamment dans le cadre d'une recherche. Cette base légale, qui a repris assez largement l'article 22 aLPD[47], pose des conditions qui renforcent la protection des personnes concernées (al. 1). Premièrement, les données doivent être anonymisées aussitôt que la finalité du traitement le permet (let. a). Deuxièmement, les organes fédéraux ne peuvent communiquer des données sensibles à des personnes privées que sous une forme qui ne permet pas d'identifier les personnes concernées (let. b). La révision a ajouté cette condition pour améliorer la protection des données sensibles. La pseudonymisation des données suffit lorsque le code de réidentification est détenu uniquement par la personne qui transmet les données[48]. Troisièmement, le destinataire ne peut communiquer les données à des tiers que si l'organe fédéral qui les lui a transmises y a consenti (let. c). Enfin, la publication des résultats doit respecter une forme qui ne permet pas d'identifier les personnes concernées (let. d). Le second alinéa instaure une dérogation à certaines autres dispositions. Notamment, l'article 34 al. 2 LPD, qui exige que le traitement des données par les organes fédéraux repose sur une base légale formelle, et l'article 36 al. 1 LPD, selon lequel la communication de données personnelles n'est admissible que si l'article 34 al. 1 à 3 LPD, ne s'applique pas. Une loi au sens matériel suffit par conséquent pour que les organes fédéraux puissent traiter des données personnelles à des fins de recherche.

Nous verrons par la suite que les principes liés à la collecte des données peuvent être malmenés en cas de réutilisation des données (*infra* D).

2. Loi relative à la recherche sur l'être humain

L'article 16 LRH requiert le consentement éclairé et écrit de la personne concernée pour qu'elle puisse être associée à un projet de recherche, ce qui suppose qu'elle soit dûment informée. Parmi les renseignements qui doivent lui être transmis, oralement et par écrit, figurent les mesures destinées à assurer la protection de ses données personnelles et ses droits (al. 2 let. d et e). En outre, la personne concernée doit disposer d'un délai de réflexion raisonnable (al. 3).

47 Message sur la révision totale de la LPD, p. 6699.
48 Message sur la révision totale de la LPD, p. 6699.

Le consentement des personnes incapables de discernement est régi par les articles 21 ss LRH. Bien qu'il s'agisse d'un droit personnel soumis à représentation, le sujet de recherche doit être impliqué autant que possible. Au demeurant, la capacité de discernement des personnes mineures ne suffit pas, leurs représentants légaux doit aussi se prononcer sauf lorsque la personne concernée est adolescente et que les risques ainsi que les contraintes du projet de recherche sont minimaux. Dans l'application de cette loi spéciale, l'adolescence est reconnue dès que la personne mineure a 14 ans (art. 3 let. j et k LRH). La doctrine relève qu'il s'agit d'une limite naturelle qui correspond au stade de développement des jeunes et qu'elle tient compte du concept de capacité de discernement en Suisse selon lequel la faculté de jugement est une notion relative qui doit être examinée dans chaque cas concret[49]. Cette distinction ne se substitue pas à l'examen de la capacité de discernement de la personne concernée en cause, elle permet seulement de définir le champ d'application des articles 22 et 23 LRH[50]. Afin d'éviter de paraphraser les articles 24 ss LRH, nous présentons ci-dessous la matière sous forme de tableaux :

Figure 1. Enfant (art. 22 LRH)

ENFANT (art. 22 LRH)	Bénéfice direct escompté	Sans bénéfice direct escompté
Capable de discernement	- Consentement éclairé de l'enfant - Consentement éclairé et écrit du représentant légal	- Consentement éclairé de l'enfant - Consentement éclairé et écrit du représentant légal - Risques et contraintes inhérents au projet minimaux - Espoir de résultats essentiels
Incapable de discernement	- Pas de manifestation d'un refus de l'enfant - Consentement éclairé et écrit du représentant légal	- Pas de manifestation d'un refus de l'enfant - Consentement éclairé et écrit du représentant légal - Risques et contraintes inhérents au projet minimaux - Espoir de résultats essentiels

49 HFG-RUDIN, art. 3, N 66.
50 HFG-RUDIN, art. 3, N 66.

Figure 2. Adolescent (art. 23 LRH)

ADOLESCENT (art. 23 LRH)	Bénéfice direct escompté	Sans bénéfice direct escompté
Capable de discernement	- Consentement éclairé et écrit de l'adolescent - Consentement éclairé et écrit du représentant légal en cas de risques et contraintes inhérents au projet NON minimaux	
Incapable de discernement	- Pas de manifestation d'un refus de l'adolescent - Consentement éclairé et écrit du représentant légal	- Pas de manifestation d'un refus de l'adolescent - Consentement éclairé et écrit du représentant légal - Risques et contraintes inhérents au projet minimaux - Espoir de résultats essentiels

Figure 3. Adulte (art. 24 LRH)

ADULTE (art. 24 LRH)	Bénéfice direct escompté	Sans bénéfice direct escompté
Incapable de discernement	- Pas de manifestation d'un refus de la personne concernée - Consentement de la personne concernée avant de perdre le discernement et attesté dans un document ou - Consentement éclairé et écrit du représentant légal, d'une personne de confiance ou d'un proche	- Pas de manifestation d'un refus de la personne concernée - Consentement de la personne concernée avant de perdre le discernement et attesté dans un document ou - Consentement éclairé et écrit du représentant légal, d'une personne de confiance ou d'un proche - Risques et contraintes inhérents au projet minimaux - Espoir de résultats essentiels

Figure 4. Urgence (art. 30 LRH)

URGENCE (art. 30 LRH)	Bénéfice direct escompté	Sans bénéfice direct escompté
Tant que dure l'incapacité d'exprimer la volonté	- Dispositions prises pour établir la volonté de la personne concernée dans les meilleurs délais - Pas de manifestation d'un refus de la personne concernée - Médecin « extérieur » est consulté pour défendre les intérêts de la personne concernée	- Dispositions prises pour établir la volonté de la personne concernée dans les meilleurs délais - Pas de manifestation d'un refus de la personne concernée - Médecin « extérieur » est consulté pour défendre les intérêts de la personne concernée - Risques et contraintes inhérents au projet minimaux - Espoir de résultats essentiels
Dès que la capacité d'exprimer la volonté renaît	+ - Information et détermination (consentement *a posteriori* ou refus)	+ - Information et détermination (consentement *a posteriori* ou refus)

Plusieurs recherches portant sur des maladies humaines ou sur la structure et le fonctionnement du corps humain collectent des données personnelles liées à la santé à l'occasion d'une prise en charge médicale. Dans ces cas, un patient consulte pour des raisons de santé et se voit proposer de livrer ses données de santé à un projet de recherche. La préoccupation majeure de la patiente ou du patient porte alors sans doute sur son état de santé et sur la prise en charge médicale qui lui est proposée. À cette occasion, elle ou il reçoit déjà de nombreuses informations sur le diagnostic (également sur les éventuels diagnostics différentiels), sur les thérapies envisageables, sur les pronostics, sur les risques, sur le comportement thérapeutique et sur les aspects financiers du traitement[51].

[51] Pour plus de détails sur l'étendue du devoir d'information médicale, se référer notamment à CHRISTINAT, N 319 ss et DONZALLAZ, N 3662 ss, et les nombreuses sources citées par ces auteurs.

La personne atteinte dans sa santé doit déjà absorber toute cette masse de renseignements qui peuvent lui être fournis dans un moment de vie difficile et par conséquent de vulnérabilité. On songe par exemple aux victimes d'un cancer, d'une maladie chronique ou d'un accident. Alors que la personne se bat avec ses pensées et ses réflexions, on lui demande encore de participer à une étude. Comme l'information doit lui être délivrée oralement et par écrit, elle sera convoquée à un entretien (qui est souvent conduit par du personnel de soins, mais pas par la chercheuse ou le chercheur) où on lui présentera (art. 16 al. 2 LRH) la nature, les buts, la durée et le déroulement du projet de recherche (let. a), les risques et les contraintes prévisibles (let. b), le bénéfice escompté du projet de recherche, notamment pour elle-même et pour les tiers (let. c) et, au milieu de cette vague d'éléments nouveaux et potentiellement angoissants (si l'on se réfère à l'information sur son état de santé), les mesures destinées à garantir la protection de ses données personnelles (let. d). Même si la personne concernée reçoit encore une information écrite à l'issue de l'entretien et qu'elle dispose d'un délai raisonnable pour se déterminer, il est fortement envisageable qu'elle ne mesure pas l'impact de son choix sur le traitement de ses données personnelles et sensibles et qu'elle n'ait pas non plus une vraie liberté de choix. Enfin, l'expérience enseigne que plusieurs projets de recherche peuvent être soumis à une patiente ou à un patient dans le cadre d'une seule prise en charge (p. ex. : recherche sur la maladie détectée chez la personne concernée en lien avec son groupe sanguin et son mode de vie, recherche sur les résultats de l'opération planifiée, recherche sur le matériel biologique retiré de son corps et recherche sur les réactions au réveil à la suite d'une anesthésie générale). Cette multiplication d'informations que de tels cas de figure impliquent peuvent contribuer à noyer les patient·es sous une vague de renseignements et générer un effet contre-productif (« trop d'informations tuent l'information »).

À ce constat s'ajoute que plusieurs recherches sont conduites dans les hôpitaux par les professeurs qui pilotent l'équipe médicale et soignante. Par conséquent, la personne concernée pourrait craindre d'être moins bien traitée en cas de refus et se sentir contrainte d'accepter l'utilisation de ses données dans un projet de recherche[52].

[52] Nous ne prêtons pas de mauvaises intentions aux corps médical et soignant. Nous sommes bien au contraire convaincue qu'un refus ne serait pas sanctionné dans la prise en charge médicale de la personne concernée. Cela ne signifie pas pour autant que la personne concernée le prenne également ainsi. Dans son message, le Conseil fédéral énonce d'ailleurs : « *La personne qui refuse de participer à un projet de recherche ne saurait subir aucun préjudice, notamment en ce qui concerne d'éventuels suivis ou traitements médicaux. Dans ce cas, le traitement ou le suivi standard doit s'effectuer avec la diligence nécessaire. Il serait illicite de renvoyer un patient à un autre centre de soins en raison de son refus de participer à un projet de recherche, ou de proposer des consultations à une fréquence moins régulière* » (Message LRH, p. 7314). Il faut

La personne concernée peut certes revenir sur son consentement en tout temps et sans motivation (art. 7 al. 2 LRH). Néanmoins, cette disposition ne couvre pas les données liées à la santé collectées jusqu'à la révocation. Celles-ci peuvent donc être utilisées pour le projet de recherche en cours malgré le retrait du consentement de la personne concernée. Le message légitime cette solution avec le principe de la proportionnalité, en avançant le risque lié à l'impossibilité de poursuivre les travaux entrepris particulièrement en cas d'étude menée sur des groupes restreints. La personne concernée doit cependant être dûment avertie, à l'occasion de l'information générale (art. 16 LRH), que ses données continueront d'être traitées malgré la révocation de son consentement[53]. En application de l'article 10 ORH, certains auteurs, auxquels nous nous rallions, distinguent deux situations en cas de révocation du consentement de la personne source. Selon eux, cette disposition ne régit que les études en cours, et limite donc l'impact du retrait du consentement sur le déroulement de l'étude. En revanche, si les données sont stockées pour des recherches ultérieures, la révocation implique leur effacement si aucune prolongation de la conservation n'est valablement justifiée[54].

Ce positionnement sans nuance surprend et heurte à notre sens le droit à l'autodétermination des sujets de recherche. En effet, l'article 7 LRH ne libelle pas cette exception, qui échappe par conséquent à une interprétation littérale. Les règles générales retiennent que le traitement de données personnelles par une personne privée contre la manifestation de volonté expresse de la personne concernée cause une atteinte à la personnalité dont l'illicéité est présumée (art. 30 al. 1 let. c LPD), à charge pour la personne privée de se prévaloir d'un motif justificatif tel un intérêt prépondérant. Les conditions sont encore plus strictes pour les organes fédéraux qui doivent se fonder sur une base légale, à moins qu'une dérogation existe (autorisation du Conseil fédéral, consentement de la personne concernée ou traitement de données nécessaire à protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers sans pouvoir obtenir préalablement le consentement de la personne concernée ; art. 34 LPD). Au demeurant, la loi relative à la recherche sur l'être humain renforce le droit à l'autodétermination de la personne concernée. Cette dernière pourrait donc penser qu'elle peut retirer son consentement à sa guise. Évidemment, si l'information a effectivement porté sur cette exception à la révocation, la personne concernée pourrait être taxée de mauvaise foi. Néanmoins, selon le contexte dans lequel l'information a été délivrée, nous estimons qu'il serait soutenable qu'elle invoque un vice du consentement initial. Elle supporterait cependant le

néanmoins conserver à l'esprit que le consentement de certaines personnes pourrait être vicié.

53 Message LRH, p. 7314.

54 ERARD, p. 607 ; HFG-RUDIN, art. 32, N 11 à 13.

fardeau de la preuve. À cet égard, elle devrait établir la masse de renseignements qui lui auraient été délivrés dans un court laps de temps, tant sur son état de santé et sur la prise en charge médicale préconisée que sur le projet de recherche, le nombre de projets de recherche pour lesquels sa participation a été sollicitée, la durée et le moment de l'information orale quant aux projets de recherche (à notre sens, l'entretien aura bien moins d'impact s'il a lieu dans le contexte d'une consultation médicale, par exemple d'une consultation préparatoire à une opération). La démonstration de ces faits pourrait conduire une autorité à admettre une dilution de l'information. En nous inspirant de la jurisprudence relative aux clauses insolites[55], nous estimons à cet égard que la simple mention dans un document préformulé de l'exception à l'article 7 LRH concernant les données de santé pourrait être insuffisante selon le contexte, et qu'il pourrait s'avérer indispensable que ladite exception soit mise en évidence pour attirer expressément l'attention de la personne concernée. De plus, celui ou celle qui se charge de l'information orale devrait dans ces cas non seulement évoquer spécifiquement cette exception mais aussi expliquer ses conséquences. L'inexpérience de la personne concernée face à des recherches menées dans un milieu scientifique de pointe, *a fortiori* lorsqu'il s'agit d'un patient déjà fragilisé par son état de santé, justifie de la considérer comme une partie faible et de lui accorder une protection particulière. Par conséquent, la personne concernée pourrait dans certaines situations se prévaloir d'une erreur de base pour invalider son consentement initial.

Il n'est pas question d'appliquer ici la jurisprudence sur la règle de l'insolite en tant que telle, mais de considérer l'argumentation qui a poussé le Tribunal fédéral à la retenir. En l'occurrence et contrairement aux clauses insolites, l'exception à l'article 7 LRH n'est pas stipulée par la chercheuse ou par le chercheur au détriment de la personne concernée mais elle découle de l'interprétation légale. Ainsi, la dérogation à la loi n'est pas due au chercheur ou à la chercheuse mais au système légal lui-même. La personne concernée ne pourrait donc pas se prévaloir du caractère insolite de la clause pour s'opposer au traitement futur des données collectées dans le cadre de la recherche avant la révocation de son consentement.

Ces considérations nous amènent à soutenir que l'article 7 LRH mériterait d'être précisé pour intégrer cette exception de manière explicite. Il s'agirait en outre de la nuancer, en maintenant le principe que l'utilisation des données collectées jusqu'à la révocation du consentement cause une atteinte illicite à la personnalité, à moins que la chercheuse ou le chercheur puisse se prévaloir d'un motif justificatif et notamment d'un intérêt supérieur. Les circonstances du cas d'espèce seraient ainsi examinées concrètement. Dans les situations où le revirement de

55 ATF 119 II 443, c. 1a, SJ 1994 637 ; ATF 135 III 1, c. 2.1, JdT 2011 II 516 ; TF, 4A_186/2018 du 28 octobre 2018, c. 2.

la personne concernée menacerait le projet de recherche, l'autorité devrait reconnaître un intérêt prépondérant. Dans les autres cas, l'intérêt de la personne concernée devrait prévaloir.

C. Conservation

1. Loi sur la protection des données

Aucun article de la loi sur la protection des données n'aborde spécifiquement la conservation de données en vue d'une étude future qui ne porterait pas sur l'être humain. Comme la conservation est un traitement de données, les principes généraux s'appliquent (art. 6 LPD), notamment la proportionnalité (al. 2).

Si les données stockées ne sont pas anonymisées, le consentement explicite de la personne concernée est nécessaire lorsqu'il s'agit de données sensibles (art. 6 al. 7 let. a LPD). En revanche, lorsque les données sont anonymisées ou pseudonymisées, elles échappent à la loi et leur conservation est libre. La vraie question n'est donc pas tellement liée à la conservation mais au processus d'anonymisation ou de codage en vue de la conservation des données à des fins de recherche, car il s'agit d'un traitement soumis à la loi. Lorsque des données sensibles sont en cause, la personne concernée devrait donc donner son consentement explicite à l'anonymisation et au codage en vue du stockage à des fins de recherche qui ne porterait pas sur l'être humain. Lorsque les données personnelles ne sont pas sensibles, la garantie de la transparence du traitement requiert que la personne concernée soit informée lors de la collecte que ses données pourront être anonymisées ou codées afin d'être conservées à des fins de recherche (art. 19 al. 2 let. a et b *cum* art. 6 al. 3 et 4 LPD). Selon notre position, la situation serait donc presque identique à celle que l'article 32 al. 3 LRH retient pour l'anonymisation des données génétiques à des fins de recherche (*infra* D.3). Les régimes se distingueraient comme suit. Dans le dernier cas, le législateur a choisi le système de l'*opt-out*. Cela implique que la personne concernée peut s'opposer à l'anonymisation de ses données à des fins de recherche. Si la loi sur la recherche n'est pas applicable, nous estimons que la personne source peut seulement refuser la collecte initiale de ses données sensibles.

Enfin, le principe de la proportionnalité (art. 6 al. 2 LPD) pourrait s'opposer à l'anonymisation/pseudonymisation générale de toutes données en vue d'une réutilisation dans une potentielle recherche future, sans savoir si elles seront concrètement utiles un jour (« gardons-les au cas où »). À notre sens, aucune base légale ne justifierait ce traitement de données à large échelle par des organes fédéraux pour créer une gigantesque base de données anonymisées ou

pseudonymisées exploitable librement dans des études sortant du champ d'application de la loi relative à la recherche sur l'être humain. Les personnes privées ne pourraient pas invoquer un intérêt prépondérant à un tel traitement généralisé. Cette position se justifie d'autant plus en considérant qu'une anonymisation de fait suffit et que l'appariement des données codées permet de plus en plus souvent de réidentifier la personne source. Ainsi, les risques de réidentification augmentent significativement avec la masse de données anonymes et codées laissée à la libre disposition de la science. Il est même légitime de se demander si les données demeurent anonymes dans cette hypothèse. À notre sens, dès que la personne concernée peut être réidentifiée par la technologie au moyen de croisements de données anonymes ou codées, le caractère anonyme tombe. Cette situation nous place face à un paradoxe. Prises individuellement, les données sont anonymes mais, prises dans leur ensemble, elles ne le sont plus. Si l'ensemble des données était requalifié de données personnelles, il pourrait ne plus y avoir à terme de données anonymes. Cette évolution nuirait à la liberté de la recherche. Il nous apparaît au demeurant disproportionné de requalifier toutes les données puisque la réidentification de la personne concernée suppose l'accès non seulement à toutes les données mais aussi à une technologie de pointe qui peut les croiser. Pour ménager les intérêts en présence, il nous semble que les personnes qui parviennent à réidentifier des tiers au moyen d'un appariement de données anonymisées ou codées devraient être tenues à un secret aussi fort que le secret professionnel. Il s'agirait ainsi de concevoir une nouvelle infraction pénale, qui serait réalisée par toute personne qui utiliserait ou qui dévoilerait des informations sur un tiers après les avoir obtenues au moyen de données anonymisées ou pseudonymisées croisées.

2. Loi sur la recherche

Comme déjà évoqué, l'accès à des données personnelles liées à la santé présente un intérêt indéniable pour le milieu scientifique, qui souhaite par conséquent pouvoir y accéder largement afin de mener des études dont la fiabilité requiert le plus souvent un très grand nombre d'échantillons et de données personnelles correspondantes[56]. Le message précise à cet égard : « *En général, un projet de recherche ne fait pas qu'« utiliser »* […] *les données personnelles liées à la santé disponibles* ; *il les met aussi à la disposition d'autres projets de recherche. Cela implique la conservation de matériel biologique ou de données personnelles liées à la santé, par exemple dans des biobanques, des registres médicaux ou des bases de données.* »[57] Nous verrons que la réutilisation de données est d'ailleurs largement admise (*infra* D).

56 Message LRH, p. 7347.
57 Message LRH, p. 7347.

La conservation de données personnelles liées à la santé comporte un risque que des tiers s'en emparent et les traitent de manière illicite. Il est donc nécessaire d'exiger de celles et ceux qui conservent ces données de prendre les mesures nécessaires à endiguer le risque de piratage. Ainsi, quiconque conserve des données personnelles liées à la santé à des fins de recherche relative à l'être humain est chargé de les protéger de toute utilisation illégale en prenant d'une part les mesures techniques et organisationnelles appropriées et en respectant d'autre part les exigences techniques liées aux conditions d'exploitation (art. 43 al. 1 LRH). Ainsi, les recommandations en matière de sécurité des données doivent être appliquées[58]. L'ordonnance relative à la recherche sur l'être humain précise que cela implique les mesures propres à permettre l'emploi des données aux seules personnes qui en ont besoin pour accomplir leurs tâches, qu'elles doivent empêcher la publication, la modification, la suppression et la copie des données sans autorisation ou par inadvertance et qu'elles sont contraintes de documenter l'ensemble des processus de traitement déterminants pour garantir la traçabilité des données (art. 5 ORH). Le responsable du traitement doit s'assurer les services d'un personnel qualifié qui soit capable d'assurer la qualité de la conservation des données et la sécurité de la base d'exploitation en se conformant aux règles de l'art[59].

D. Réutilisation

1. Remarque liminaire

Les progrès technologiques ont considérablement accru l'intérêt scientifique de pouvoir réutiliser des données déjà collectées à l'occasion d'un premier traitement de données lié ou non à une recherche. Le droit des personnes concernées dans ce contexte revêt par conséquent de l'importance en pratique. À cet égard, DUCOR écrivait déjà il y a une dizaine d'années : « *Avec l'avènement des techniques de séquençage génétique massivement parallèle et l'augmentation de la puissance des calculateurs utilisés en bio-informatique, les biobanques et les banques de données notamment génétiques prennent une place croissante dans la recherche sur l'être humain. En conséquence, les projets de recherche réutilisant du matériel biologique et/ou des données personnelles liées à la santé* […] *sont de plus en plus fréquents tant dans le milieu académique que dans l'industrie.* »[60] Partant, les conditions à la réutilisation de données revêtent une grande importance pratique.

58 Message LRH, p. 7347.
59 Message LRH, p. 7347.
60 DUCOR, p. 190.

2. Loi sur la protection des données

La loi sur la protection des données ne régit pas spécifiquement la réutilisation des données personnelles (les données anonymes et codées peuvent être réutilisées librement puisqu'elles ne sont pas couvertes par la loi). Selon la doctrine, ce traitement est admis dans les limites du principe de finalité (art. 6 al. 3 LPD). Par conséquent, la réutilisation ne doit pas être inattendue, inappropriée ou contestable du point de vue de la personne concernée[61]. ERARD/HEUSGHEM/PARISATO recommandent de procéder à un test de compatibilité qui considère toutes les circonstances du cas d'espèce, en particulier qui compare la finalité de la collecte initiale avec celle de la réutilisation, qui examine le contexte de la collecte, qui établit les attentes raisonnables des personnes concernées, qui considère la nature des données traitées, qui évalue les conséquences de la réutilisation pour les personnes sources et qui vérifie si des garanties appropriées existent[62]. Cette approche se conforme à la notion de finalité compatible que la révision de la loi sur la protection des données a introduite (art. 6 al. 3 LPD).

Si la personne concernée ne pouvait pas s'attendre à la réutilisation de ses données personnelles dans le cadre d'un traitement du fait de personnes privées, le responsable du traitement doit se fonder sur un motif justificatif (art. 31 al. 1 LPD) comme un intérêt prépondérant. Dans le contexte qui nous occupe, le législateur reconnaît précisément que l'intérêt prépondérant de la chercheuse ou du chercheur à la réutilisation de données personnelles peut entrer en considération (art. 31 al. 2 let. e LPD). Il a cependant encadré la pratique par des conditions puisque la pesée des intérêts n'a lieu que si le responsable du traitement anonymise les données dès que possible (ch. 1) et ne publie les résultats de ses investigations que sous une forme qui ne permet pas d'identifier les personnes concernées (ch. 3) (*supra* A.).

De plus, la loi confère une protection accrue aux données sensibles puisque leur réutilisation est soumise à une condition supplémentaire. En effet, le maître du fichier ne peut communiquer les données à des tiers qu'après les avoir codées. Dans l'hypothèse où une pseudonymisation serait impossible, il doit prendre les mesures pour garantir que les tiers ne traiteront les données qu'à des fins qui ne se rapporteront pas à des personnes (art. 31 al. 2 let. e ch. 2 LPD). Cette condition renforce donc l'intérêt de la personne concernée, puisqu'elle empêche d'invoquer le seul intérêt de la recherche pour justifier une violation de l'article 30 al. 2 let. c LPD[63].

61 ERARD/HEUSGHEM/PARISATO, N 45 ; Message sur la révision totale de la LPD, p. 6645.
62 ERARD/HEUSGHEM/PARISATO, N 45.
63 Message sur la révision totale de la LPD, p. 6692.

3. Loi relative à la recherche sur l'être humain

L'ordonnance relative à la recherche sur l'être humain définit la réutilisation de données en mentionnant qu'il s'agit de toute opération effectuée à des fins de recherche avec des données déjà collectées, et elle donne une série d'exemples (art. 24). L'expression « *à des fins de recherche* » n'est pas anodine. Elle signifie que les données personnelles collectées pour une recherche sont conservées afin de pouvoir les utiliser dans d'autres projets de recherche encore inconnus. Ainsi, la conservation n'intervient pas pour un projet de recherche déterminé[64], et les données peuvent aussi être conservées pour nourrir une banque de données pour d'autres recherches[65]. La personne concernée donne alors un consentement général, qui réduit la portée du principe de la finalité[66]. La doctrine reconnaît les avantages du consentement général[67] qui « *réside dans la grande latitude qu'il laisse aux chercheurs tout en protégeant l'autonomie et les droits des participants. Cela à condition que le* [consentement général] *soit formulé en accord avec les dispositions légales et appliqué avec les mesures de sécurité adéquates. Il contribue alors à concilier les intérêts des patients et ceux des chercheurs* »[68]. Des expertes du domaine ont analysé certains formulaires d'information délivrés aux patient·es et ont constaté quelques défauts. Elles ont donc formulé certaines critiques et proposé des pistes d'amélioration[69]. Le consentement général est donc discuté, et le Conseil fédéral examine les mesures qui pourraient l'accompagner pour mieux sauvegarder le droit à l'autodétermination des personnes concernées sans entraver inutilement l'accès aux données pour la science[70]. Pour le surplus, nous renvoyons à la contribution de SPRUMONT dans cet ouvrage collectif, qui aborde en détails le consentement général[71].

Lorsque la loi impose le consentement explicite de la personne concernée, il s'agit du système de l'*opt-in*, peu importe que le consentement doive porter sur un projet particulier ou qu'un consentement général suffise[72]. Le système de l'*opt-out* prévaut en revanche lorsque la personne concernée ne doit pas s'opposer au traitement de ses données après avoir été informée[73].

---

64 Message LRH, p. 7336.
65 HFG-RUDIN, Vorbemerkung Art. 32-35, N 7.
66 ERARD/HEUSGHEM/PARISATO, N 40.
67 ERARD/HEUSGHEM/PARISATO, N 40 ; TALANOVA/SPRECHER, p. 1198 ss.
68 TALANOVA/SPRECHER, p. 1198 et références citées.
69 Pour éviter de répéter ce que la doctrine a déjà développé, nous nous permettons de renvoyer à TALANOVA/SPRECHER, p. 1197 ss.
70 Pour les travaux en cours et une vision critique, se référer à ERARD/HEUSGHEM/PARISATO, N 41 ss.
71 Voir dans cet ouvrage, TALANOVA/DOSCH/MARKS SULTAN/SPRUMONT, p. 89 ss.
72 ERARD, p. 607.
73 ERARD, p. 607.

Avant d'examiner les solutions que la loi retient, relevons que l'article 17 LRH dispose que la personne concernée doit être informée dès la collecte des données personnelles liées à la santé que leur réutilisation est envisagée à des fins de recherche et que son consentement doit déjà être recueilli à ce moment. En outre, elle doit être informée qu'elle peut s'y opposer. Une réutilisation à des fins de recherche est envisageable si elle est planifiée ou si elle est très vraisemblable[74]. Si la personne responsable omet cette information, une commission d'éthique saisie d'une demande sur la base de l'article 34 LRH (réutilisation de données personnelles liées à la santé à des fins de recherche dépourvue du consentement éclairé de la personne concernée) ne pourrait pas la rejeter pour ce motif[75].

La loi relative à la recherche sur l'être humain pose des conditions différentes pour la réutilisation de données personnelles liées à la santé selon leur nature (génétiques ou non) et selon leur forme (non codées, codées ou anonymisées). En bref, le tableau se résume comme suit.

- Données génétiques (art. 32 LRH) :
  - non codées (al. 1) : consentement éclairé *ad hoc*[76] ;
  - codées (al. 2) : consentement éclairé général ;
  - anonymisation (al. 3) : non-opposition après information ;
  - anonymisées : non appréhendées par la loi.

- Données personnelles non génétiques liées à la santé (art. 33 LRH) :
  - non codées (al. 1) : consentement éclairé général ;
  - codées (al. 2) : non-opposition après information ;
  - anonymisation : non appréhendée par la loi ;
  - anonymisées : non appréhendées par la loi.

Comme susmentionné, la loi relative à la recherche sur l'être humain retient l'approche absolue, c'est-à-dire que les données pseudonymisées ne sont pas considérées comme étant anonymes pour celles et ceux qui ne détiennent pas la clé mais conservent leur statut de données personnelles liées à la santé (*supra* II.C). Après avoir souligné le lien entre l'importance conférée au droit à l'autodétermination dans la recherche sur l'être humain (art. 118*b* al. 2 let. a Cst.) et l'approche absolue, ERARD plaide en faveur de son application dans ce contexte particulier de recherche. Il prétend à juste titre que l'approche relative évincerait

74 Message LRH, p. 7322.
75 Message LRH, p. 7322 s.
76 Chaque fois qu'il est question de consentement éclairé dans les art. 32 et 33, la loi précise qu'il s'agit de celui de la personne concernée, ou, le cas échéant, de celui de son représentant légal ou l'un de ses proches.

les données codées de la protection de la loi sur la recherche et éluderait ainsi le principe fondamental du consentement éclairé du patient garanti par la Constitution et par la loi (art. 16 et 17 LRH) en cas de réutilisation[77]. Il observe aussi que l'article 26 ORH ne s'oppose pas à cette interprétation, car cette disposition définit uniquement les exigences pour que des données soient réputées pseudonymisées dans le cadre de la législation sur la recherche relative à l'être humain[78]. Avec d'autres auteurs, il complète en argumentant que les données codées qui seraient exclues de la loi sur la recherche avec l'approche relative échapperaient aux mesures techniques et organisationnelles qui contraignent la conservation des données de recherche (art. 43 LRH)[79]. JOTTERAND soutient quant à lui qu'aucune des deux approches ne doit être retenue en particulier, au motif que la qualification d'une donnée codée dépend des possibilités concrètes de la personne qui l'exploite de rétablir un lien avec la personne source. Si des données supplémentaires pour réidentifier cette dernière existent et que la chercheuse ou le chercheur peut se les procurer, la donnée n'est pas anonyme. À défaut, le caractère anonyme devrait être reconnu[80]. La sécurité et la prévisibilité du droit nous amènent à préférer l'approche d'ERARD, surtout dans un contexte où les données utilisées sont sensibles et toujours en regard des possibilités croissantes de tisser un lien avec la personne source par l'appariement de données.

Les données génétiques recèlent la particularité d'un contenu informatif imprévisible lors de la collecte, dont l'importance est susceptible de se renforcer au gré des avancées du futur concernant leur décryptage[81]. C'est pourquoi la loi régit plus étroitement leur réutilisation que les autres données personnelles liées à la santé[82].

Nous développons ci-dessous les exigences selon la nature des données réutilisées et leur forme.

– Données génétiques non codées

La personne concernée doit donner son consentement éclairé à la réutilisation de données génétiques dans un projet de recherche concret (art. 32 al. 1 LRH). L'article 16 LRH régit par analogie les exigences de l'information pour que le consentement soit éclairé[83]. L'article 28 ORH le complète en mentionnant notamment que la personne concernée doit être avertie de son droit à refuser ou à

77 ERARD, p. 614 s.
78 ERARD, p. 614.
79 ERARD/HEUSGHEM/PARISATO, N 33.
80 JOTTERAND, N 78.
81 DUCOR, p. 190.
82 DUCOR, p. 190.
83 Message LRH, p. 7337.

révoquer son consentement et les conséquences d'une révocation. Elle doit aussi connaître les mesures prises pour assurer la protection de ses données personnelles. Lorsque la personne concernée est incapable de discernement ou est mineure, les articles 22 à 24 LRH trouvent application.

– Données génétiques codées

Le consentement explicite de la personne concernée est requis pour la réutilisation de données génétiques pseudonymisées par une personne qui ne dispose pas de la clé. La personne concernée ne doit pas se prononcer sur un projet de recherche déterminé ; un consentement général, soit le codage de ses données, le stockage et la réutilisation à des fins de recherche, suffit. L'article 29 ORH précise les informations qui doivent être délivrées à la personne concernée. Enfin, les articles 21 à 24 LRH s'appliquent lorsque la personne concernée est privée de la capacité de discernement ou est mineure.

– Anonymisation de données génétiques

Il peut être surprenant que l'anonymisation de données génétiques ne soit pas libre. Le caractère particulièrement sensible de ce type de données justifie cependant cette protection renforcée du droit à l'autodétermination. Effectivement, les progrès de la technique peuvent permettre de rétablir un lien avec une personne en mettant en relation plusieurs jeux de données anonymisées[84].

Selon la loi, les données génétiques peuvent donc être anonymisées et stockées à des fins de recherche si la personne concernée ne s'y est pas opposée après avoir été informée. Les renseignements qui doivent être délivrés à la personne source sont énoncés à l'article 30 ORH, soit l'anonymisation envisagée, le droit de véto de la personne concernée, les conséquences de l'anonymisation sur les résultats concernant la santé de la personne concernée et la possibilité de transmettre les données à des tiers à des fins de recherche.

La protection du droit à l'autodétermination de la personne concernée nous apparaît toutefois relativement faible. À cet égard, le message enseigne que l'information « *peut, par exemple, être faite par le biais de la brochure d'information des patients établie par un hôpital* »[85]. Les exigences sont donc moindres que celles incombant aux médecins pour satisfaire au devoir de l'information médicale, qui contraint les professionnel·les de la santé à veiller que les patient·es comprennent les renseignements qui leur sont donnés. Au demeurant, l'information doit être personnalisée (des renseignements seulement écrits sont insuffisants). Enfin, les médecins supportent le fardeau de la

84 Message LAGH, p. 5325.
85 Message LRH, p. 7337.

preuve de l'information si un patient allègue avec suffisamment de vraisemblance un défaut de consentement faute d'avoir été averti·e correctement.

Il convient d'examiner ces constats à la lumière du droit applicable à la collecte des données génétiques. Au moment de leur collecte, les données génétiques ne sont pas anonymes. Si elles sont d'emblée traitées à des fins de recherche sur les maladies humaines ainsi que sur la structure et le fonctionnement du corps humain, la loi relative à la recherche s'applique. Si tel n'est pas le cas, la loi sur la protection des données régit la collecte. Cette loi commande que la personne concernée consente expressément au traitement de ce type de données puisqu'elles sont sensibles (art. 6 al. 7 let. a LPD), et qu'elle puisse reconnaître la finalité du traitement qui doit être respectée ultérieurement (art. 6 al. 3 LPD). Lors de la collecte des données génétiques, la personne concernée n'a pas forcément conscience que ses données pourraient être anonymisées pour être conservées et réutilisées ultérieurement à des fins de recherche. Dans ce cas, elle pourrait se voir remettre une simple brochure dans un second temps, par exemple quand elle se présente à un entretien pour obtenir les résultats des analyses, afin de l'informer que ses données seront anonymisées et conservées à des fins de recherche sauf avis contraire de sa part. Là encore, l'effet de l'annonce du résultat des analyses génétiques peut éclipser les renseignements en lien avec le traitement futur des données. Nous doutons au demeurant qu'une personne non initiée maîtrise les recoupements qui peuvent être faits entre différentes bases de données génétiques anonymisées et la précision des renseignements que peuvent révéler ces analyses.

Au vu de ce qui précède, nous estimons que l'anonymisation, le stockage et la réutilisation de données génétiques à des fins de recherche sont encadrés par le principe de l'*opt-out*, (art. 32 al. 3 LRH), mais que le problème survient lors de la collecte et de la conservation[86]. Comme le degré d'information au stade de

[86] Voir aussi TALANOVA/SPRECHER, p. 1198 ; ERARD/HEUSGHEM/PARISATO, N 12 qui rapportent que, dans le contexte de la Stratégie Nationale en matière d'*Open Research Data*, le Conseil des États a déposé une motion pour que le Conseil fédéral adopte une loi-cadre régissant les infrastructures spécifiques nécessaires à la réutilisation de données dans des « *domaines stratégiques* » comme la santé et la recherche (Motion 22.3890 du Conseil des États du 22 août 2022). En examinant cette motion qu'il a acceptée, le Conseil fédéral a souligné l'importance et le potentiel d'une réutilisation des données « *à des fins d'utilisation secondaire* » et les a mis en perspective avec les principes généraux de la loi sur la protection des données, notamment de la finalité. Il a relevé que l'utilité que les données pourraient présenter ultérieurement en étant utilisées à d'autres fins est souvent impossible à anticiper lors de la collecte. Sur la base de ce constat, il s'emploiera en particulier à identifier « *les domaines dans lesquels une utilisation secondaire des données serait pertinente et proportionnée, ainsi que les infrastructures et autres exigences préalables qui seraient nécessaires pour exploiter des espaces de données fiables et interopérables* » (avis du Conseil fédéral du 23 novembre 2022) (la motion et l'avis sont disponible sur le site du Parlement, à l'adresse Internet suivante : <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20223890>.

l'anonymisation est minimal, la personne qui récolte les données doit à notre sens déjà attirer l'attention de la personne concernée sur cette possibilité de retraitement à des fins de recherche pour que le consentement soit valable. Par conséquent, la personne concernée qui aurait manqué les informations relatives à l'anonymisation et la réutilisation des données génétiques à des fin de recherche après ce processus ne peut s'en prendre ni à celui ou celle qui a procédé à l'anonymisation des données ni à la personne qui les a réutilisées. Elle pourrait en revanche contester l'attitude de la personne qui a collecté les données génétiques sans avoir recueilli un consentement valable faute d'information.

JUNOD soulève le risque d'une omission de l'étape de l'information avec le système de l'*opt-out*[87].

– Données génétiques anonymisées

Ces données échappent à la loi sur la recherche ; l'article 32 al. 3 LRH régit seulement l'anonymisation des données génétiques à des fin de recherche. Le ou la scientifique qui accède à des données anonymes peut donc les utiliser librement dans une étude. JUNOD nuance en affirmant qu'il ou elle devrait s'abstenir en cas de doute sur la licéité de l'anonymisation des données[88].

– Données personnelles non génétiques liées à la santé codées

Le consentement explicite de la personne concernée est requis. Un consentement général, soit « à des fins de recherche » suffit. La loi renvoie aussi aux articles 16 et 22 à 24 LRH concernant la validité du consentement. Les informations qui doivent être fournies à la personne concernée sont précisées à l'article 32 ORH.

– Données personnelles non génétiques liées à la santé non codées

La personne concernée ne doit pas s'être opposée à la réutilisation après avoir été informée que ses données pourraient être pseudonymisées pour être réutilisées à des fins de recherche. Les renseignements qui doivent être communiqués à la personne concernée figurent à l'article 31 ORH. Le consentement de la personne concernée n'est pas requis.

87 JUNOD, Recherche médicale rétrospective, p. 403.
88 JUNOD, Recherche médicale rétrospective, p. 401.

– Anonymisation des données personnelles non génétiques liées à la santé

La loi ne pose pas de condition à l'anonymisation de données personnelles non génétiques liées à la santé à des fins de recherche. Si les données non pas été collectées dans le cadre d'une étude soumise à la loi spéciale, nous renvoyons à nos considérations précédentes en lien avec la collecte (*supra* B.1). Si la collecte a eu lieu dans le cadre d'un projet de recherche sur l'être humain, la personne source devrait être renseignée sur cette possibilité dans le cadre de l'information générale délivrée lors de la collecte (art. 17 LRH).

– Données personnelles non génétiques liées à la santé anonymisées

La personne concernée n'a pas à être informée et ne peut pas s'opposer à la réutilisation de ces données. Selon le message, « *il n'est guère imaginable que* [ce type de données] *puissent, dans le cadre d'une réutilisation, livrer des conclusions sur le diagnostic, le traitement ou la prévention d'une maladie. C'est pourquoi cette catégorie de données n'a pas fait l'objet d'une interdiction d'anonymisation* »[89].

Exceptionnellement, les données personnelles liées à la santé peuvent être réutilisées même à défaut de consentement explicite ou que l'information relative au droit d'opposition n'a pas été dispensée (*escape clause*[90]) (art. 34 LRH). Trois conditions doivent être remplies cumulativement. D'une part, l'obtention du consentement ou l'information sur le droit d'opposition est impossible ou pose des difficultés disproportionnées ou on ne peut raisonnablement pas l'exiger de la personne concernée (let. a). Deuxièmement, aucun document n'atteste un refus de la personne concernée (let. b). L'intérêt de la science doit enfin primer celui de la personne concernée à décider de la réutilisation de son matériel biologique ou de ses données (let. c). Le législateur a estimé que certaines situations justifient de privilégier les intérêts scientifiques et que, à défaut, la liberté de la recherche serait restreinte de manière disproportionnée.

Selon le message, la première condition est remplie si les personnes nommées sont décédées. Le Conseil fédéral estime en outre qu'il faut évaluer la charge de travail que la prise de contact avec les personnes concernées requiert. S'il est extrêmement difficile de les retrouver, notamment en raison d'un cercle de personnes très étendu ou d'un long délai entre la collecte des données et la remise du projet de recherche, la charge de travail serait disproportionnée. À l'inverse, la charge émotionnelle de la personne concernée qui serait à nouveau confrontée à une situation difficile est insuffisante. Le message précise enfin

89 Message LRH, p. 7338.
90 ERARD, p. 607.

qu'un consentement qui n'aurait pas été recueilli ou qu'une information qui n'aurait pas été délivrée à temps n'excluent pas l'application de l'exception[91].

L'arbitrage des intérêts en présence voulu par la troisième condition suppose d'examiner le cas concret. Son intérêt prime si la recherche laisse espérer des découvertes revêtant un grand intérêt. Tel est le cas s'il est question de données liées à une maladie grave. L'intérêt de la recherche est aussi prépondérant si les enseignements pourraient profiter à un grand nombre d'individus[92]. La doctrine relate que les commissions d'éthique de la recherche ont été assaillies de demandes qui portaient sur des projets réutilisant des données liées au COVID-19 sans le consentement des patients et qui se fondaient sur l'article 34 LRH[93]. La méconnaissance du virus, le nombre de personnes malades et l'urgence de la situation ne réalisaient toutefois pas à elles seules l'intérêt scientifique prépondérant ; l'examen de chaque cas concret demeurait indispensable[94]. Il semblerait d'ailleurs que cette règle qui devrait être interprétée restrictivement est, dans la pratique, appliquée largement par les commissions d'éthique[95].

Certains auteurs plaident en faveur d'un assouplissement du régime actuel de la loi sur la recherche relative à l'être humain. En substance, ils estiment que les intérêts de la personne concernée sont peu menacés dans le cadre de la réutilisation de données dans le cadre d'une recherche, notamment grâce à l'anonymisation et au codage des données qui suppriment le risque d'identification de la personne concernée. Ils estiment que la Suisse doit conserver sa compétitivité dans la recherche scientifique et que l'intérêt scientifique l'emporte par conséquent. Ils suggèrent que la loi soit modifiée pour admettre plus facilement la libre réutilisation de données liées à la santé ou de matériel biologique, si certaines conditions sont remplies (les données de santé et le matériel biologique devraient être anonymisés dès que le but de la recherche le permet ; les données pourraient être transmises à des tiers seulement si la personne concernée n'est pas identifiable ; les personnes concernées seraient informées de la possibilité que leurs données soient réutilisées à des fins de recherche et ne s'y seraient pas opposées ; la recherche aurait été autorisée par une commission d'éthique). Il ne serait donc pas nécessaire de démontrer que l'intérêt de la science prime dans un cas concret ainsi que le requiert l'actuel article 34 let. c LRH[96].

91 Message LRH, p. 7338.
92 Message LRH, p. 7339.
93 TALANOVA/SPRECHER, p. 1197 s.
94 TALANOVA/SPRECHER, p. 1198 et références citées.
95 THOUVENIN *et al*., N 21.
96 THOUVENIN *et al*., toute la contribution (en particulier N 24 ss et 32 ss).

4. Loi sur l'analyse génétique

L'article 12 LAGH règle l'utilisation des échantillons et des données génétiques à une autre fin qu'une analyse. Cette disposition s'applique à la réutilisation des données génétiques dans le cadre d'une recherche qui ne porte pas sur une maladie humaine ou sur la structure et le fonctionnement du corps humain (*supra* II.A).

Les données génétiques non codées et codées ne peuvent être utilisées dans le cadre d'une recherche échappant à la loi sur la recherche que si la personne concernée y a expressément consenti après avoir été suffisamment informée (al. 1). Le message enseigne que l'information doit être circonstanciée quant à l'utilisation à une autre fin prévue. À cet égard, le principe de finalité ne permet qu'un traitement dans un but suffisamment défini et exposé lors de l'entretien d'information, qui doit renseigner la personne sur le lieu et la durée de la réutilisation prévue. La réutilisation peut être unique mais un consentement général est aussi admis. Ainsi, la réutilisation peut avoir une formulation relativement ouverte ou abstraite[97].

Si les données sont anonymisées après l'analyse génétique terminée, le système de l'*opt-out* prévaut (al. 2). Dans son message, le Conseil fédéral expose que les données sortent du champ d'application de la loi sur la protection des données dès qu'elles sont anonymisées. La loi sur l'analyse génétique renforce ainsi la protection des données génétiques puisqu'une anonymisation prévue doit « *être abordée au préalable dans le cadre de l'information* »[98].

E. Transmission

1. Loi sur la protection des données

Lorsque le traitement de données est le fait d'une personne privée, la communication de données sensibles à un tiers constitue une atteinte à la personnalité (art. 30 al. 2 let. c LPD).

Les articles 36 et 37 LPD imposent des règles particulières aux organes fédéraux, car la transmission de données personnelles (y compris sensibles) à des tiers constitue une opération particulièrement délicate[99]. Par conséquent, une base légale est requise. L'article 36 renvoie à l'article 34 al. 1 à 3 LPD (al. 1). En revanche, il instaure ses propres conditions pour déroger à la base légale (al. 2)

97 Message LAGH, p. 5326.
98 Message LAGH, p. 5327.
99 Message LPD, p. 6698.

et la liste est exhaustive[100]. Dans tous les cas, la personne concernée peut s'opposer à la communication de ses données à des tiers par un organe fédéral pour autant qu'elle rende vraisemblable un intérêt digne de protection (art. 37 al. 1 LPD). L'organe fédéral rejette cependant l'opposition (al. 2) lorsqu'il est juridiquement contraint de transmettre les données personnelles (let. a) ou si l'absence de communication risque de compromettre l'accomplissement des tâches de l'organe (let. b).

2. Loi relative à la recherche sur l'être humain

À teneur de l'article 41 LRH, des données personnelles liées à la santé collectées ou utilisées à des fins de recherche peuvent être transmises à d'autres fins uniquement si une base légale le prévoit (let. a) ou si la personne concernée a donné son consentement explicite (let. b). Par conséquent, celui ou celle qui offre ses données personnelles à la recherche ne doit pas craindre qu'elles soient utilisées à d'autres fins sans son consentement, à moins qu'une loi le permette exceptionnellement[101].

IV. Moyens de vérification de la personne objet de la recherche

A. Loi sur la protection des données

La LPD consacre le droit d'accès de la personne concernée (art. 25 LPD), qui peut demander au responsable si des données personnelles sont traitées. Selon le Conseil fédéral, le droit d'accès « *est la clé qui permet à la personne concernée de faire valoir les droits que lui octroie la loi* »[102]. La disposition donne une liste exemplative des renseignements qui doivent être délivrés le cas échéant. Il s'agit de ceux qui sont nécessaires à la revendication des droits inhérents à la protection des données et à la transparence du traitement. Comme la loi ne prévoit pas de disposition spécifique pour l'accès à des données dans le cadre d'une recherche, nous ne le commentons pas et nous bornons à rappeler quelques éléments intéressants pour le sujet de la présente contribution.

La personne concernée peut ainsi consulter ses données personnelles que traite le responsable du traitement pour savoir si l'utilisation est conforme au droit

100 Message sur la révision totale de la LPD, p. 6697.
101 Message LRH, p. 7345.
102 Message sur la révision totale de la LPD, p. 6682.

(principes d'exactitude, de finalité, *etc.*)[103]. Elle a notamment le droit d'être informée de la durée de conservation de ses données personnelles ou, par impossible, des critères pour la fixer (al. 2 let. d). Ces renseignements peuvent être utiles en lien avec la conservation de données à des fins de recherche (*supra* III.C.1). Si la personne suspecte que ses données sont conservées à cette fin, elle peut le demander expressément au responsable du traitement. À notre sens, elle pourrait requérir la destruction de ses données personnelles qui seraient conservées uniquement à des fins de recherche si elle refuse que ses données soient pseudonymisées ou anonymisées et réutilisées dans une recherche future. Au besoin, elle recourra aux actions défensives *(infra* V.C).

La personne concernée peut aussi demander à quels destinataires ou catégorie de destinataires ses données ont été communiquées (al. 2 let. g). Cette possibilité est aussi précieuse en lien avec la conservation des données et la transmission à des fins de recherche.

Un des risques que nous identifions dans le domaine qui nous occupe est la perte de maîtrise de ses données personnelles par la personne concernée. Les données originairement personnelles qui ont été anonymisées ou simplement codées échappent à son contrôle puisque la loi ne les régit plus. Nous avons vu que les progrès de la technologie permettent de plus en plus de relier de telles données à la personne concernée par appariement. Nous avons aussi développé que les opérations qui visent l'anonymisation ou la pseudonymisation des données est un traitement qui devrait donc respecter le principe de la finalité. Par ricochet, la personne concernée aurait dû en être informée au moment de la collecte (art. 19 al. 2 let. b LPD).

Dans le cas où la personne concernée suspecterait que le responsable du traitement ait conservé ses données à des fins de recherche sans l'avoir préalablement renseignée de cette possibilité, elle peut le lui demander. La doctrine mentionne que l'obligation de transparence contraint le responsable du traitement de délivrer des renseignements suffisants aux personnes concernées en raison de son obligation de transparence[104]. À notre sens, la véritable difficulté se loge dans la situation où le responsable du traitement nierait un autre traitement des données mais que la personne source ne la croirait pas. Il faut donc savoir comment celle-ci peut réagir dans un tel cas de figure et quels moyens le droit met à sa disposition (*infra* V).

103 HERTIG PEA, N 291.
104 ERARD/HEUSGHEM/PARISATO, N 50.

B. Loi relative à la recherche sur l'être humain

L'article 8 al. 2 LRH autorise la personne concernée à consulter toutes les données collectées qui la concerne. Dans son message, le Conseil fédéral relevait que cette base légale accordait un droit d'être informée à la personne concernée sur toutes les données collectées à son sujet, et ce par analogie avec l'ancien article 8 LPD qui consacrait le droit d'accès[105]. Puisque la loi sur la protection des données révisée régit désormais le droit d'accès à l'article 25 et que cette disposition n'a pas été fondamentalement changée, nous estimons que l'analogie demeure. La loi spéciale confère une protection accrue à la personne concernée car les restrictions au droit d'accès de l'article 26 LPD ne s'appliquent pas, puisque la disposition spéciale ne prévoit aucune exception au principe du droit à l'information (art. 8 al. 2 LRH).

Le législateur offre une protection particulière aux personnes concernées dans le cadre de la loi sur la recherche relative à l'être humain, puisque tous les projets sont soumis à l'autorisation d'une commission d'éthique, qui la délivre uniquement si les exigences éthiques, juridiques et scientifiques prévues par la loi sont remplies (art. 45 LRH). La compétence de la commission englobe les études qui utilisent des données personnelles liées à la santé à des fins de recherche lorsque l'obtention du consentement ou l'information sur le droit d'opposition manquent (al. 1 let. b). Cernant ce dernier point, DUCOR constate qu'il est parfois difficile de savoir à partir de quel moment une réutilisation de données équivaut à un nouveau projet de recherche. Il estime que la création d'une biobanque ou d'une autre base de données et le stockage ne suffisent pas[106].

La position des personnes sources nous semble donc plus favorable lorsque leurs données sont traitées dans le cadre d'une étude soumise à la loi sur la recherche relative à l'être humain, puisque les commissions d'éthique jouent un rôle de surveillance. En effet, elles doivent non seulement valider les projets de recherche, mais elles vérifient encore que leur réalisation soit conforme aux exigences (art. 51 al. 1 LRH), ce qui implique un suivi de l'étude[107]. Nous doutons que les scientifiques soient malintentionnés, mais la complexité du domaine, due en particulier aux progrès fulgurants, et les risques de perte de maîtrise en cas de négligence, même légère, sont importants.

105 Message LRH, p. 7315.
106 DUCOR, p. 192 s.
107 Message LRH, p. 7352.

V. Mesures judiciaires à l'encontre de personnes privées

A. À titre liminaire

La personne source dispose de moyens d'investigation grâce à la transparence et au droit d'accès qui en découle. Ces principes risqueraient toutefois de demeurer lettre morte à défaut de pouvoir agir en justice pour contraindre la personne responsable à fournir les renseignements demandés en cas de refus de sa part. En l'occurrence, la loi prévoit une action en exécution du droit d'accès (*infra* B).

Il convient ensuite de déterminer comment la personne concernée peut réagir concrètement si elle considère que ses droits sont menacés (*infra* B et C) ou lésés (*infra* D) et si des tiers peuvent agir pour son compte (*infra* E). Quelques considérations sur les coûts de la procédure ponctueront cette rubrique (*infra* F).

Le chapitre 5 de la loi sur la protection des données règle en particulier le traitement de données personnelles par des personnes privées. Les trois dispositions, qui concrétisent la protection de la personnalité (art. 28 CC), sont présentées selon une systématique légale claire. L'article 30 régit les atteintes à la personnalité à l'occasion d'un traitement de données, l'article 31 aborde les motifs justificatifs et l'article 32 expose les mesures à disposition des personnes concernées pour faire valoir leurs prétentions si leurs données personnelles ont été utilisées de manière illicite. L'examen de l'article 32 LPD occupera par conséquent ce chapitre.

La personne concernée peut exiger la rectification de ses données personnelles inexactes, à moins que la loi ne l'interdise ou que les données soient traitées à des fins archivistiques dans un but d'intérêt public (art. 32 al. 1 LPD). Dans la mesure où la qualité d'une étude dépend étroitement de la précision et de l'exactitude des données exploitées, nous n'imaginons pas de situation qui puisse poser un problème en pratique. Si une personne concernée constate une erreur et en informe la personne responsable, cette dernière aura intérêt à la corriger. Par conséquent nous ne développons pas cette mesure.

L'article 32 al. 2 LPD renvoie au Code civil pour les actions en protection de la personnalité (art. 28, 28*a*, et 28*g* à 28*l* CC) et se borne à préciser les mesures que la personne concernée peut demander en justice. Lorsque des données personnelles sont traitées dans le cadre d'une recherche, seules les actions de l'article 28*a* CC sont pertinentes, à l'exclusion des mesures liées au droit de réponse (art. 28*g* à 28*l* CC). Ainsi, nous discutons dans les prochaines sections seulement des actions générales de la protection de la personnalité pour autant qu'elles fassent sens dans le contexte de la recherche. La disposition spéciale de l'art. 32 LPD se distingue de la règle générale de l'article 28*a* CC sur un

point. La première restreint la légitimation active à la personne concernée, tandis que la seconde s'adresse à toute personne lésée. De ce fait, si un traitement illicite de données lèse les proches de la personne concernée, ceux-ci ne pourront pas invoquer l'article 32 LPD et devront agir sur la base de l'article 28*a* CC exclusivement[108].

B. Action en exécution du droit d'accès

Avant la révision totale de la loi sur la protection des données, l'action en exécution du droit d'accès n'était pas citée à l'article 8 aLPD. L'article 15 al. 4 aLPD disposait toutefois : « *Le tribunal statue sur les actions en exécution du droit d'accès selon la procédure simplifiée prévue par le code de procédure civile du 19 décembre 2008* ». Cet alinéa n'a pas été repris dans la loi révisée. La seule trace de l'action réside désormais à l'article 243 al. 2 let. d CPC[109], qui soumet les litiges portant sur le droit d'accès au sens de l'article 25 LPD à la procédure simplifiée[110]. Nous regrettons l'abandon de toute référence à l'action dans le droit de fond. L'ancien texte avait le mérite d'attirer expressément l'attention des responsables du traitement et des personnes concernées à ce sujet. BOHNET rappelle que « *Le législateur détermine qui peut agir en justice et pour quel droit prétendu. En d'autres termes, c'est la loi qui accorde l'action* »[111]. Le législateur définit aussi le type d'action selon l'objet de la demande (actions condamnatoires, formatrices, en constat et actions des organisations)[112]. Au demeurant, « *L'action ne se confond pas avec le droit matériel invoqué et n'est pas plus une émanation de celui-ci. Elle est rattachée à la prétention et existe si la loi reconnaît à celui qui la fait valoir un intérêt digne de protection à voir le juge statuer sur celle-ci* [renvoi]. *En d'autres termes, le droit d'action existe ou n'existe pas* [mises en évidence supprimées] »[113]. La loi sur la protection des données révisée manque donc de clarté sur ce point.

Concernant les éléments procéduraux, l'action confère à toute personne capable de discernement[114] qui n'a pas pu accéder à ses données (ou pas entièrement)[115]

108 Pour tout le paragraphe, se référer à HERTIG PEA, N 324.
109 Code de procédure civile du 19 décembre 2008, RS 272.
110 Seule la rédaction formelle de cet article a été remaniée pour être adaptée à la nouvelle loi sur la protection des données. L'ancien art. 243 al. 2 let. d CPC se référait « *aux litiges portant sur le droit d'accès aux données prévu par la loi fédérale du 19 juin 1992 sur la protection des données* ».
111 CPra Actions-BOHNET, § 1, N 1 ; voir aussi CR CPC-BOHNET, Intro. art. 84-90, N 2.
112 JEANDIN/PEYROT, N 256.
113 CR CPC-BOHNET, intro. art. 84-90, N 10.
114 S'agissant de l'exercice d'un droit strictement personnel, la capacité de discernement suffit à son exercice (HERTIG PEA, N 296).
115 CPra Actions-BOHNET, § 4, N 25.

la possibilité d'agir en justice contre la personne responsable ou sous-traitante. La légitimité active est réservée à la personne concernée, à l'exclusion de tout tiers[116]. L'action est non patrimoniale[117], de nature non pécuniaire et condamnatoire[118]. Elle est soumise à la procédure simplifiée (art. 243 al. 2 let. d CPC) et à la maxime inquisitoire sociale (art. 247 al. 2 let. a CPC)[119]. La partie demanderesse peut cumuler cette action à une action défensive de l'article 32 LPD (*cum* art. 28*a* al. 1 CC). Dans ce cas, le procès est conduit par la procédure ordinaire (art. 219 CPC)[120]. Une tentative de conciliation précède l'action au fond, hormis pour le cas clair (art. 197 et 198 let. a CPC). L'article 20 let. d CPC instaure un for dispositif au domicile ou au siège de l'une des parties. Lorsque l'action est cumulée avec une action réparatrice de l'article 32 LPD, la doctrine se querelle quant à l'application de l'article 36 CPC qui permet à la partie demanderesse d'agir au for du domicile ou du siège du lésé ou du défendeur, ou au for du lieu de l'acte ou encore au for du résultat[121].

Il est particulièrement intéressant de réfléchir aux éléments constitutifs que la partie demanderesse doit alléguer[122], soit l'existence d'une donnée personnelle au sens de la LPD, qui est traitée par une personne privée refusant le droit d'accès dans le délai de 30 jours (art. 25 al. 7 LPD). Selon le Tribunal fédéral, la partie demanderesse ne doit pas établir son intérêt à accéder aux données lorsqu'elle exerce son droit auprès de la personne responsable du traitement. C'est uniquement lorsque cette dernière lui refuse l'accès qu'une pesée des intérêts en présence s'impose. La partie défenderesse peut ainsi opposer l'abus de droit de la personne concernée en démontrant qu'elle utilise le droit d'accès dans un but étranger à la protection des données. Tel serait notamment le cas si la partie demanderesse tentait de nuire à l'autre partie ou de collecter des preuves pour un futur procès qui seraient inaccessibles sinon. Dans ce dernier exemple, notre Haute Cour écrit que la requête constituerait seulement un prétexte à une recherche indéterminée de moyens de preuve (*fishing expedition*). Le libellé de l'article 25 al. 2 LPD a d'ailleurs été modifié à l'occasion de la révision totale de la loi pour tenir compte de cette jurisprudence qui faisait écho à des critiques doctrinales. Ainsi, la personne concernée peut prétendre recevoir

116 HERTIG PEA, N 295.

117 BSK ZPO-MAZAN, art. 243, N 14 ; CR CPC-TAPPY, art. 243, N 15 ; KUKO ZPO-FRAEFEL, art. 243, N 14 ; PC CPC-HEINZMANN, art. 243, N 11.

118 CPra Actions-BOHNET, § 4, N 8.

119 La voie du cas clair peut être choisie si les conditions sont remplies ; dans cette hypothèse, les règles de la procédure sommaire s'appliquent (CPra Actions-BOHNET, § 4, N 10).

120 CPra Actions-BOHNET, § 4, N 12.

121 BOHNET et RAMPINI (CPra Actions-BOHNET, § 4, N 20 ; BSK DSG-RAMPINI, art. 15, N 34) l'admettent alors que MEIER (MEIER, N 1822) le conteste.

122 Pour tout le paragraphe, se référer à CPra Actions-BOHNET, § 4, N 35 ss. Les autres sources consultées sont expressément citées à l'appui du texte.

« *les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la présente loi et pour que la transparence du traitement soit garantie* »[123]. La recherche de moyens de preuve pour une future action réparatrice en raison d'une violation de la loi sur la protection des données n'est en revanche pas abusive[124]. La partie défenderesse doit le cas échéant alléguer et prouver les motifs qui la fondent à refuser ou à limiter le droit d'accès[125].

L'article 25 al. 7 LPD dispose : « *en règle générale, les renseignements sont fournis dans un délai de 30 jours* ». Cette disposition impose-t-elle à la partie demanderesse d'alléguer et de prouver le refus de la partie défenderesse, ou l'absence de réaction de sa part ? En d'autres termes, le délai de 30 jours est-il un élément constitutif de l'action ? Excepté dans les cas d'urgence, où des mesures provisionnelles (voire superprovisionnelles) s'imposent pour bloquer un traitement de données imminent, la personne concernée commencera par faire valoir son droit d'accès directement auprès de la personne responsable. Il serait effectivement disproportionné de saisir la Justice sans s'être heurté à un refus ou à une absence de réaction de la personne responsable. Dans l'hypothèse où la personne concernée agirait directement par la voie judiciaire, la personne responsable serait informée du souhait de la personne concernée dès la notification de la demande. Il lui serait donc libre de s'exécuter. Dans ce cas, son comportement serait sans doute assimilé à un acquiescement, de sorte que les frais judiciaires devraient être à sa charge et elle pourrait être tenue de verser une indemnité de dépens à la partie demanderesse (art. 106 CPC). Le Tribunal pourrait toutefois déroger à cette règle et répartir les frais selon sa libre appréciation en invoquant que la procédure est devenue sans objet ou que les circonstances rendent la répartition en fonction du sort de la cause inéquitable (art. 107 al. 1 let. e et f CPC). Il pourrait aussi mettre les frais causés inutilement à la charge du demandeur (art. 108 CPC). Enfin, l'article 115 CPC permet de mettre les frais judiciaires à la charge de la partie qui a procédé de façon téméraire ou de mauvaise foi, même lorsque la procédure est en principe gratuite comme en l'espèce (art. 113 al. 2 let. g et art. 114 let. g CPC). Le Tribunal dispose donc de plusieurs correctifs qu'il appliquera selon les circonstances du cas d'espèce.

La personne concernée peut requérir des mesures provisionnelles pour garantir son droit d'accès[126]. Elle doit cependant rendre vraisemblable qu'elle est l'objet d'une atteinte ou risque de l'être et que cette atteinte pourrait l'exposer à un préjudice difficilement réparable (art. 261 CPC).

Le fait que seules les personnes concernées puissent se prévaloir de l'article 32 al. 1 LPD n'est pas anodin. Cette base légale prévoit que la personne concernée

123 Message sur la révision totale de la LPD, p. 6683.
124 ATF 141 III 119, c. 7.1.1.
125 ATF 141 III 119, c. 7.2.
126 CPra Actions-BOHNET, § 4, N 16 s.

peut demander en particulier l'interdiction d'un traitement déterminé de données (let. a), l'interdiction d'une communication déterminée de données personnelles à des tiers (let. b) ou encore l'effacement ou la destruction de données personnelles (let. c). En vertu du principe de la proportionnalité, la magistrate ou le magistrat devrait ordonner la mesure la moins contraignante. Si le codage ou l'anonymisation des données personnelles suffit à protéger la personnalité de la partie demanderesse et qu'elle est techniquement possible, seule cette mesure peut résulter du dispositif du jugement. Si aucun autre moyen ne garantit la protection, les données ne peuvent pas être transmises à des tiers ou doivent être supprimées de la base de données de l'étude. Un conflit peut toutefois naître entre un proche de la personne concernée et elle-même si cette dernière accepte le traitement de ses données tel que prévu dans la recherche mais que le tiers estime que sa personnalité propre est ou serait lésée par cette utilisation. En vertu du droit à l'autodétermination, seule la personne concernée peut se prononcer sur l'utilisation de ses données dans le cadre d'une étude déterminée ou à des fins de recherche. Si elle accepte l'utilisation de ses données à cette fin, le tiers n'est pas fondé à demander que les données soient soustraites à l'étude. Du point de vue du tiers, la portée des actions défensives est relativement limitée, et la pratique le réduirait sans doute à agir en réparation de son préjudice (art. 28*a* al. 3 CC).

Est-ce que l'autorité judiciaire pourrait étendre le dispositif du jugement aux données de toutes les personnes concernées par un traitement illicite dans le cadre d'une étude, voire ordonner la destruction de la base de données ? Comme le tribunal examine la situation concrète des parties, le jugement ne déploie pas d'effets directs entre une partie à la procédure et des tiers. En l'occurrence, les autres personnes concernées dont les données sont utilisées dans un projet de recherche ne sont pas dispensées d'agir contre la chercheuse ou le chercheur. Le tribunal n'est pas compétent pour ordonner des mesures visant la protection des données de tiers n'ayant pas participé à la procédure (sauf dans l'hypothèse d'une action sociale que nous examinons brièvement ci-après ; *infra* E). Il ne peut pas non plus condamner la partie défenderesse à détruire la base de données. Notons que le Préposé fédéral à la protection des données personnelles et à la transparence est en revanche compétent pour prendre d'office les mesures qui lui sont dévolues par la loi. En particulier, il est libre d'ouvrir une enquête contre un organe fédéral ou une personne privée si des indices suffisants font penser qu'un traitement de données pourrait être contraire à la protection des données (art. 49 LPD) ; de contraindre l'accès à des informations, à des locaux et à des installations ainsi que l'audition de témoins ou la mise en œuvre d'expertises (art. 50 LPD) ; de prendre des mesures administratives (art. 51 LPD).

C. Actions défensives

1. Considérations communes

Une atteinte à la personnalité ouvre trois actions défensives (art. 28*a* CC) : celle en prévention de l'atteinte (ch. 1), celle en cessation de l'atteinte (ch. 2) et celle en constatation du trouble (ch. 2). Les règles procédurales communes à ces actions sont énoncées ici.

Nous ne revenons pas sur la différence entre le Code civil et la loi sur la protection des données concernant la légitimité active (*supra* A). Comme il s'agit de l'exercice d'un droit strictement personnel au sens de l'article 19 al. 2 CC, les actions défensives peuvent être exercées par une personne mineure ou sous curatelle pour autant qu'elle soit capable de discernement[127].

La légitimité passive échoit à toutes les personnes qui ont traité des données de manière contraire au droit, soit aux auteurs de l'atteinte et aux personnes qui y ont participé[128]. Il peut donc s'agir de la personne responsable mais aussi des personnes auxquelles le traitement des données a été confié ou des sous-traitants[129]. Plusieurs personnes peuvent traiter des données de manière illicite à l'occasion d'une recherche et causer ainsi une atteinte à la personnalité. Dans ces cas, BOHNET souligne que la solidarité ne s'applique pas aux actions défensives et que le comportement requis de chaque partie défenderesse doit être précisé dans la demande[130]. Les défenderesses et les défendeurs forment une consorité passive simple (art. 71 CPC)[131].

La procédure est introduite au for dispositif au domicile ou au siège de l'une des parties (art. 20 let. a CPC)[132]. Dans l'hypothèse d'une pluralité de défendeurs et de défenderesses, la compétence à raison du lieu pour l'un vaut pour les autres, sauf si cette compétence résulte d'une élection de for (art. 15 al. 1 CPC)[133].

Les actions défensives, qui sont de nature non patrimoniale, sont dévolues à la procédure ordinaire (art. 219 et art. 243 *a contrario* CPC)[134]. La demande au fond est précédée d'une tentative de conciliation (art. 197 CPC). Si elle estime que les conditions sont remplies, la partie demanderesse peut opter pour le cas

127 CPra Actions-BOHNET, § 2, N 18.
128 BSK ZGB-MEILI, art. 28, N 37 ; CR CC I-JEANDIN, art. 28, N 89 ; HERTIG PEA, N 334 ; KUKO ZGB-DÖRR, art. 28, N 13.
129 HERTIG PEA, N 334.
130 CPra Actions-BOHNET, § 2, N 22.
131 HERTIG PEA, N 338.
132 CPra Actions-BOHNET, § 2, N 14 ; CR CC I-JEANDIN, art. 28, N 91 ; HERTIG PEA, N 343.
133 CPra Actions-BOHNET, § 2, N 16 ; HERTIG PEA, N 330.
134 HERTIG PEA, N 330.

clair gouverné par la procédure sommaire (art. 257 CPC)[135]. Dans ce cas, la conciliation n'a pas lieu.

La partie demanderesse doit alléguer et prouver que ses données seront, sont ou ont été traitées par la partie défenderesse en violation du droit et l'atteinte à sa personnalité qui en résulte[136]. Du caractère extra-patrimonial des droits de la personnalité découle une protection juridique indépendante d'un préjudice financier ; ainsi, la personne concernée est fondée à réagir judiciairement au traitement illicite de ses données même si son action est dépourvue d'intérêt financier[137]. Elle doit aussi établir que la loi sur la protection des données ou celle relative à la recherche sur l'être humain s'applique. À cet effet, elle est tenue de démontrer les données traitées ainsi que leur type d'une part, et le traitement en cause d'autre part. Le droit d'accès revêt par conséquent une importance considérable. Comme le caractère illicite de l'atteinte est présumé, il incombe ensuite à la partie défenderesse d'établir le motif justificatif dont elle se prévaut[138].

La situation peut évoluer en cours d'instance[139]. Par exemple, une ethnologue dépose une demande de subvention pour réaliser une étude sur les liens entre certaines maladies chroniques et les origines ainsi que les parcours de vie des individus expatriés. Elle pense utiliser les données codées de la patientèle d'une dizaine de cabinets médicaux de Suisse comme échantillon. L'un des patients d'un cabinet découvre fortuitement le projet d'étude. En l'occurrence, il n'est pas d'accord de mettre ses données personnelles à disposition du projet de recherche, mais il se souvient avoir lu quelque part que les données des patient·es du cabinet peuvent être utilisées à des fins de recherche après avoir été soigneusement pseudonymisées. Il ouvre action en prévention de l'atteinte contre l'ethnologue. Cette dernière soutient que l'étude échappe au champ d'application de la loi sur la recherche, au motif qu'elle ne porterait pas sur des maladies humaines ou sur la structure et le fonctionnement du corps humain en tant que tels mais sur l'impact des origines et du parcours de vie de personnes expatriées sur le développement de certaines maladies chroniques. Par conséquent, elle s'estime libre de réutiliser des données codées. À l'obtention des fonds, elle démarre donc son étude malgré la procédure pendante. Si la partie demanderesse s'est contentée de prendre des conclusions en prévention de l'atteinte, elle perd tout intérêt à agir. Cet exemple amène deux remarques[140] :

135 Pour tout le paragraphe : CPra Actions-BOHNET, § 2, N 8 ss.
136 HERTIG PEA, N 362 s.
137 HERTIG PEA, N 366.
138 CPra Actions-BOHNET, § 2, N 28.
139 BSK ZGB-MEILI, art. 28a, N 1 et 6 ; CR CC I-JEANDIN, art. 28a, N 3.
140 En sus des références qui seront citées, voir HERTIG PEA, N 329 et 392.

– Premièrement, la partie demanderesse doit souvent cumuler ses conclusions[141], en demandant principalement l'interdiction de l'atteinte et, subsidiairement dans le cas où celle-ci se serait réalisée, sa cessation et, plus subsidiairement encore, la constatation du trouble[142]. Il nous semble en revanche impossible de prendre directement des conclusions réparatrices en raison de l'ignorance du montant du préjudice lors du dépôt de l'acte.
– Deuxièmement, la partie demanderesse doit pouvoir modifier ses conclusions en cours d'instance pour qu'elles suivent l'évolution de la situation[143]. La doctrine admettait déjà cette solution avant l'unification de la procédure civile qui a, depuis, été consacrée à l'article 227 al. 1 let. a CPC. Comme les actions défensives sont soumises à la procédure ordinaire, il n'y aura pas de difficulté à passer d'une action en prévention de l'atteinte à une action en cessation ou en constat du trouble. Toutefois, l'action en réparation de l'atteinte est soumise à la procédure simplifiée jusqu'à une valeur litigieuse de CHF 30'000.–. Dans ce cas, la partie demanderesse ne peut pas modifier ses conclusions sauf accord de la partie défenderesse, qui pourrait selon les circonstances commettre un abus de droit en refusant. Tel serait le cas si l'évolution de la situation lui était imputable alors qu'elle savait qu'une procédure était pendante. La partie demanderesse doit veiller à alléguer et à prouver les faits nouveaux en lien avec ses nouvelles conclusions en respectant le régime restrictif des *novas* (art. 229 CPC)[144].

Enfin, la partie demanderesse conclura le plus souvent que la décision soit assortie de la menace de la sanction pénale pour insoumission à une décision de l'autorité (art. 292 CP)[145].

2. Action en prévention de l'atteinte

Si le traitement illicite de données à l'occasion d'une recherche n'a pas encore eu lieu, la personne concernée dispose d'une action en prévention de l'atteinte (art. 28*a* al. 1 ch. 1 CC *cum* art. 32 al. 2 let. a et b LPD), qui est de nature condamnatoire (art. 84 CPC)[146].

En sus des éléments constitutifs généraux des actions défensives énoncés ci-dessus (*supra* 1), la partie demanderesse doit rendre vraisemblable l'imminence

141 BSK ZGB-Meili, art. 28a, N 1 ; CR CC I-Jeandin, art. 28a, N 3.
142 CPra Actions-Bohnet, § 2, N 38.
143 CR CC I-Jeandin, art. 28a, N 3.
144 CPra Actions-Bohnet, § 2, N 37.
145 BSK ZGB-Meili, art. 28a, N 2 ; CR CC I-Jeandin, art. 28a, N 8 ; KUKO ZGB-Dörr, art. 28a, N 2 et 3.
146 CPra Actions-Bohnet, § 2, N 8.

de l'atteinte[147]. Cette condition impose une menace sérieuse et concrète d'une atteinte déterminée[148]. La personne concernée ne peut pas se plaindre d'un comportement général, mais elle doit décrire précisément le comportement de la personne responsable dont elle requiert l'interdiction[149]. Elle soignera ainsi la rédaction de ses allégués mais aussi de ses conclusions. L'imminence de l'atteinte s'apprécie au moment du jugement. Si le tribunal admet la demande, il interdit le traitement des données projeté dans l'étude. Le tribunal peut aussi ordonner des mesures d'exécution (*supra* 1).

La partie demanderesse ne peut pas agir en prévention de l'atteinte pour s'opposer à toute recherche de manière abstraite. En revanche, elle peut parfois contrer au traitement de ses données qui les conditionne à réutilisation à des fins de recherche. Si le traitement des données n'est pas soumis à la loi sur la recherche relative à l'être humain, le législateur a reconnu l'intérêt scientifique de pouvoir anonymiser ou pseudonymiser les données collectées à des fins de recherches (art. 31 al. 2 let. e LPD ; *supra* III.D.2). Comme la loi sur la recherche encadre davantage la réutilisation de certaines données, la personne concernée peut dans ce cas s'opposer au traitement qui permettrait de dédier ses données à la recherche. En particulier, l'utilisation de données génétiques codées à des fins de recherche suppose le consentement général de la personne concernée et l'anonymisation de données génétiques à des fins de recherche n'est admise que si la personne concernée ne s'y est pas opposée après avoir été informée (art. 32 LRH ; *supra* III.D.3). De même, un consentement général de la personne concernée est requis pour la réutilisation de données personnelles non génétiques liées à la santé qui ne sont pas codées et celle de données pseudonymisée est soumise au principe de l'*opt-out* (art. 33 LRH ; *supra* III.D.3). Dans ces hypothèses, la personne concernée pourrait établir un défaut de consentement pour l'utilisation de ses données à des fins de recherche et agir par la voie de l'action préventive.

3. Action en cessation de l'atteinte

Lorsque l'utilisation des données est effectuée lors d'une étude concrète ou que les données sont traitées à des fins de recherche de manière illicite et que l'atteinte est en cours, la personne concernée peut agir en cessation (art. 28*a* al. 1 ch. 2 CC *cum* art. 32 al. 2 LPD). L'action est de nature

147 Une preuve stricte n'est donc pas attendue (HERTIG PEA, N 391).
148 BSK ZGB-MEILI, art. 28a, N 2 ; CR CC I-JEANDIN, art. 28a, N 4.
149 CR CC I-JEANDIN, art. 28a, N 4.

condamnatoire (art. 84 CPC)[150]. L'autorité judiciaire ordonne les mesures propres à mettre un terme à l'atteinte.

L'atteinte doit perdurer au moment du jugement. Si elle était pendante lors du procès mais qu'elle est terminée lorsque le juge statue, la partie demanderesse doit être déboutée de ses conclusions. L'élément déterminant est le comportement de l'auteur et pas les effets de l'atteinte sur la partie demanderesse. L'atteinte se termine ainsi au moment même où la chercheuse ou le chercheur arrête le traitement de données litigieux, et ce indépendamment de la persistance du trouble pour la partie demanderesse[151].

Outre les éléments constitutifs généraux des actions défensives, la partie demanderesse doit alléguer et prouver l'existence de l'atteinte. La partie adverse doit avancer et démontrer les motifs justificatifs.

4. Action en constatation du trouble

Il s'agit d'une action en constatation de droit[152], qui est utile lorsque l'atteinte est terminée mais que le trouble subsiste[153].

En plus des éléments constitutifs généraux propres aux actions défensives (*supra* 1), la partie demanderesse doit démontrer le lien de causalité entre l'atteinte et le trouble d'une part et la persistance de ce dernier d'autre part[154]. Cette seconde condition propre à l'action se matérialise principalement dans deux situations. La première suppose que des tiers aient eu connaissance de l'atteinte[155]. Tel pourrait par exemple le cas si des scientifiques avaient eu connaissance de données personnelles liées à la santé d'une personne identifiée en raison d'une mauvaise codification. La seconde est plus intéressante pour le domaine qui nous occupe, car elle porte sur un risque de récidive dépourvu d'imminence[156]. L'action en prévention de l'atteinte est donc écartée. En l'occurrence, l'intérêt scientifique à la conservation des données pour une réutilisation à des fins de recherche est notoire. L'action en constatation du trouble revêt ainsi de l'importance en pratique.

150 CPra Actions-Bohnet, § 2, N 8.
151 Pour tout le paragraphe, se référer à BSK ZGB-Meili, art. 28a, N 4, CR CC I-Jeandin, art. 28a, N 9 ; KUKO ZGB-Dörr, art. 28a, N 3.
152 CPra Actions-Bohnet, § 2, N 8.
153 BSK ZGB-Meili, art. 28a, N 6 ; CR CC I-Jeandin, art. 28a, N 10 ; KUKO ZGB-Dörr, art. 28a, N 4.
154 BSK ZGB-Meili, art. 28a, N 8 ; CR CC I-Jeandin, art. 28a, N 11 ; Hertig Pea, N 414.
155 CR CC I-Jeandin, art. 28a, N 11.
156 CR CC I-Jeandin, art. 28a, N 12.

D. Actions réparatrices

1. Régime général

La personne lésée peut agir en réparation du préjudice subi (art. 28*a* al. 3 CC). L'action est de nature pécuniaire et condamnatoire (art. 84 CPC)[157]. Contrairement aux actions défensives, elle ne poursuit pas la protection de la personnalité en agissant directement sur l'atteinte mais elle tend à replacer la personne lésée dans la situation qui serait la sienne si l'atteinte à sa personnalité, causée en l'occurrence par un traitement illicite de données dans le cadre de la recherche, n'était pas survenue[158].

Les actions réparatrices du Code des obligations sont ouvertes (art. 28*a* al. 3 CO[159]), soit l'action en dommages et intérêts (art. 41 ss CO), l'action en réparation du tort moral (art. 49 CO) et l'action en remise du gain selon les règles de la gestion d'affaires (art. 423 CO). Dépourvues de particularité en lien avec le sujet de la présente contribution, nous renonçons à les développer. L'action en remise du gain est mentionnée pour mémoire. En pratique, il nous semble cependant improbable qu'elle aboutisse dans la mesure où la partie demanderesse devrait établir un lien de causalité entre l'utilisation abusive de ses données et le gain. Comme la qualité d'une recherche dépend aussi de la masse des données, les scientifiques récoltent le plus souvent beaucoup de données. Ainsi, lorsque le résultat de la recherche n'aurait pas été différent si les données litigieuses n'avaient pas été traitées, le lien de causalité fait défaut. La question peut en revanche être pertinente dans les domaines où les données sont rares (p. ex. personne d'une certaine race atteinte d'une maladie orpheline).

Outre les conditions de l'article 28*a* CC[160], la partie demanderesse doit avancer et établir les conditions propres à l'action réparatrice qu'elle introduit. La procédure applicable dépend de la valeur litigieuse (art. 219 et 243 CPC) et l'instance est introduite par une requête en conciliation. Une personne mineure ou sous curatelle mais capable de discernement doit agir directement, en son nom et pour son compte lorsqu'elle revendique une compensation morale. Elle exerce effectivement un droit strictement personnel. À l'inverse, les actions en dommage et intérêts et en remise du gain consacrant des droits pécuniaires

157 CPra Actions-Bohnet, § 2, N 8.

158 BSK ZGB-Meili, art. 28a, N 16 ; CR CC I-Jeandin, art. 28a, N 19.

159 Loi fédérale complétant le Code civil suisse du 30 mars 1911 (Livre Cinquième : Droit des obligations), RS 220.

160 La partie demanderesse doit ainsi prouver avoir subi une atteinte à sa personnalité en raison d'un traitement illicite de données. Si elle fonde ses prétentions sur la loi sur la protection des données, elle doit en outre démontrer que le traitement a porté sur des données personnelles. Si elle invoque la loi relative à la recherche sur l'être humain, elle doit établir elle doit aussi prouver les conditions qui lui sont inhérentes.

requièrent l'exercice des droits civils pour être menées, de sorte que l'intervention de la représentante ou du représentant légal est requise.

2. *Régime spécial de la LRH*

Si une étude est couverte par la loi sur la recherche relative à l'être humain, la personne qui initie le projet de recherche répond des dommages que les sujets de recherche subissent en relation avec l'étude en cause, indépendamment de la commission d'une faute (art. 19 al. 1 LRH). La loi érige donc une responsabilité causale. L'article 60 CO régit la prescription (al. 2). Le Code des obligations ou les lois qui règlent la responsabilité des collectivités publiques s'appliquent pour le surplus (al. 3). On appliquera donc le premier lorsque la relation entre la personne concernée et la chercheuse ou le chercheur repose sur le droit privé et les secondes si leur rapport relève du droit public[161].

Dans son message, le Conseil fédéral précise que l'article 19 LRH instaure une responsabilité causale pour plusieurs raisons. Le sujet de recherche prend des risques dans l'intérêt de la communauté, sans recevoir de rémunération en contrepartie. Par conséquent, il serait inéquitable et contraire à l'éthique que celles et ceux qui prennent des risques pour des motifs essentiellement ou principalement altruistes doivent assumer les préjudices qui peuvent en découler. La responsabilité causale s'applique aussi aux préjudices financiers consécutifs à une atteinte au droit de la personnalité, comme le traitement illicite de données dans le cadre d'une recherche sur l'être humain[162].

Tous les préjudices qui, selon le libellé du texte légal, sont « *en relation avec le projet* » sont couverts. La partie demanderesse doit par conséquent établir un lien de causalité naturelle et adéquate entre le préjudice et la participation à l'étude. L'ensemble des « *actions conformes ou non conformes des personnes impliquées dans le projet, en particulier les instigateurs, les médecins et les professionnels qui les assistent, relèvent également de la responsabilité de la personne qui dirige le projet* »[163].

Un point d'attention mérite d'être souligné en particulier, car il ne ressort pas clairement du texte légal. Le Conseil fédéral exclut des articles 19 et 20 LRH les projets de recherche rétrospective, c'est-à-dire qui réutilisent du matériel et des données déjà existantes (art. 32 ss LRH ; *supra* III.D.3). Il estime qu'une responsabilité causale ne se justifie pas, car ces études ne présentent pas de

161 Message LRH, p. 7325.
162 Message LRH, p. 7324.
163 Message LRH, p. 7324.

risques financiers particuliers et qu'elles ne sont pas susceptibles de causer des préjudices[164].

Afin de renforcer la protection des sujets de recherche, l'article 20 LRH prévoit un régime de sûretés pour endiguer les risques inhérents à l'insolvabilité de la personne responsable[165]. Ainsi, la responsabilité doit être garantie par une assurance ou sous une forme équivalente, sauf celle de la Confédération, de ses établissements et de ses corporations de droit public.

E. Action sociale

Le Tribunal fédéral a reconnu la qualité pour agir aux organisations si certaines conditions sont remplies[166]. L'unification de la procédure civile a codifié cette jurisprudence à l'article 89 CPC. Cela concerne les associations et les autres organisations, comme les fondations, qui revêtent une importance régionale ou nationale[167]. Leurs statuts doivent les habiliter à défendre, en leur propre nom, les intérêts d'un groupe de personnes déterminé pour les atteintes à la personnalité que celles-ci subissent (art. 89 al. 1 CPC)[168]. L'action des organisations est toutefois limitée aux actions défensives ; l'organisation ne peut pas agir en réparation de l'atteinte (art. 89 al. 2 CPC)[169].

Étant considéré qu'une étude requiert autant de données que possible, de nombreux individus peuvent être lésés par un projet de recherche déterminé ou par le traitement de leurs données à des fins de recherche. L'action des organisations constitue un moyen efficace pour combattre un éventuel abus. Une personne en particulier peut avoir de nombreuses réticences à agir seule contre la personne responsable et abandonner toute démarche en raison de ses craintes. L'action des organisations rééquilibre les forces dans le cadre d'une procédure. Si les conditions sont réunies, une association de patients pourrait par exemple réagir contre un traitement de données à des fins de recherche susceptible de causer une atteinte à la personnalité aux patients.

L'organisation doit établir les mêmes éléments constitutifs concernant l'atteinte à la personnalité causée par un traitement de données prohibé par le droit. Elle ne peut cependant pas exercer le droit d'accès, puisque ses propres données ne font pas l'objet du traitement litigieux. Il est donc possible que quelques personnes concernées doivent entreprendre une action en exécution du droit

164 Message LRH, p. 7324 s ; JUNOD, Recherche médicale rétrospective, p. 403.
165 Message LRH, p. 7325.
166 ATF 121 III 168, c. 4b, JdT 1996 I 52 ; ATF 114 II 345, c. 3b.
167 CR CC I-JEANDIN, art. 28, N 88.
168 CR CC I-JEANDIN, art. 28, N 88.
169 CR CC I-JEANDIN, art. 28, N 88.

d'accès pour apprécier si les données sont traitées dans le respect de la loi ou pas.

F. Frais de la procédure

Le faible nombre de procédures civiles introduites dans le domaine de la protection des données a interpellé le législateur. L'une des raisons avancées était les risques financiers liés au procès, de sorte que les frais de justice ont été supprimés (art. 113 let. g et 114 let. g CPC)[170]. Il n'est donc plus perçu de frais judiciaires dans les procédures de conciliation et au fond « *pour les litiges relevant de la LPD* » depuis le 1er septembre 2023. Le message relève que la quasi-absence de revendications réduit considérablement l'efficacité de la loi sur la protection des données et qu'il en résulte aussi une jurisprudence insuffisante à la concrétisation des normes, ce qui nuit à la sécurité juridique[171].

Le message ne précise pas les procédures qui sont englobées dans la notion de « *litiges relevant de la LPD* » à laquelle se réfèrent les articles 113 et 114 CPC. Les actions défensives de l'article 28*a* CC sont concernées puisque l'article 32 LPD prévoit que les actions concernant la protection de la personnalité sont notamment régies par cette disposition. Mais qu'en est-il d'une action défensive introduite par un proche de la personne concernée et non par elle ? Nous avons vu que cet individu n'est pas légitimé à agir sur la base de l'article 32 LPD, et qu'il tire ses prétentions exclusivement du Code civil (*supra* A). Dans cette hypothèse, la partie demanderesse invoque une atteinte causée à l'un de ses droits de la personnalité en raison du traitement de données d'autrui, mais l'atteinte n'est pas due au traitement de ses propres données personnelles. Par conséquent, la gratuité ne devrait pas profiter à ces procédures. Cette position nous apparaît cohérente avec la restriction du champ d'application personnel de l'article 32 LPD.

Il est plus compliqué de savoir si l'exemption des frais judiciaires profite aussi aux actions réparatrices. Il convient donc de déterminer si l'objet d'une action en paiement, en réparation du tort moral ou en remise du gain visant la réparation d'une atteinte à la personnalité due à la violation de la loi sur la protection des données relève de cette loi. En l'occurrence, l'article 32 LPD instaure un renvoi dynamique à l'article 28*a* CC. Les actions prévues dans cette disposition sont par conséquent intégrées à la loi sur la protection des données pour autant qu'elle ne les restreigne pas. Or seule la légitimation active a été limitée. L'article 28*a* CC dispose que la partie demanderesse peut requérir du tribunal des mesures propres à protéger sa personnalité (al. 1) et que les actions réparatrices

170 Message sur la révision totale de la LPD, p. 6737.
171 Message sur la révision totale de la LPD, p. 6737 s.

sont réservées (al. 3). Avec cette précision, le législateur a exprimé « *le principe selon lequel la sauvegarde de ses droits par la victime qui use à ces fins de l'une ou l'autre action défensive et / ou mesure de protection prévues à l'art. 28a al. 1 et 2 CC ne saurait en aucune manière la priver de son droit à obtenir réparation, et réciproquement* »[172]. JEANDIN développe que les actions réparatrices n'agissent pas sur l'atteinte en tant que telle mais visent à en corriger les conséquences, causées en l'occurrence par un traitement de données illicite. Au demeurant, les droits de la personnalité sont de nature extra-patrimoniale alors qu'une action réparatrice ne peut pas rétablir la personne lésée dans ses droits mais uniquement lui accorder une réparation financière[173]. Par conséquent, l'article 28*a* CC ne semble pas englober les actions réparatrices dans les actions visant la protection de la personnalité. Le troisième alinéa exprime seulement que des revendications fondées sur les actions défensives ne privent pas la personne lésée d'introduire une procédure en réparation de son préjudice en parallèle ou ultérieurement. Au vu de cette analyse, la gratuité de la procédure ne devrait pas profiter aux actions réparatrices.

Est-ce que la procédure est gratuite lorsque la personne concernée fonde ses prétentions sur la loi sur la recherche relative à l'être humain ? Lorsque la partie demanderesse ouvre une action défensive, l'article 32 LPD s'applique puisqu'aucune disposition de la loi spéciale n'y déroge ou ne la précise. Si elle réclame la réparation de son dommage, la même réflexion développée au paragraphe précédent s'applique.

Enfin, lorsqu'une violation de la loi sur la protection des données ou de la loi sur la recherche relative à l'être humain constitue aussi une infraction pénale (art. 60 ss et art. 62 s LRH), les frais de la procédure sont en principe mis à la charge de la Confédération ou du canton qui a conduit la procédure (art. 423 CPP[174]), à moins que le prévenu soit condamné auquel cas il les supporte (art. 426 CPP). Si la partie plaignante a pris des conclusions civiles, les frais de procédure y afférents peuvent lui être imputés si la procédure est classée ou que le prévenu est acquitté, en cas de retrait desdites conclusions avant la clôture des débats de première instance, ou lorsque les conclusions ont été écartées ou que la partie plaignante a été renvoyée à agir par la voie civile (art. 427 CPP).

172 CR CC I-JEANDIN, art. 28a, N 20.
173 CR CC I-JEANDIN, art. 28a, N 19.
174 Code de procédure pénale suisse (Code de procédure pénale, CPP) du 5 octobre 2007, RS 312.0.

VI. Mesures à l'encontre d'organes fédéraux

Aucune particularité n'est à signaler dans le domaine de la recherche concernant les prétentions de la personne concernée contre un organe fédéral et la procédure pour les revendiquer. Les articles 41 et 42 LPD constituent le siège de la matière.

Le premier alinéa de l'article 41 LPD reprend en substance les actions défensives du Code civil, puisqu'il permet à quiconque dispose d'un intérêt digne de protection d'exiger de l'organe fédéral responsable de s'abstenir de procéder à un traitement illicite de données (let. a), de supprimer les effets d'un traitement illicite (let. b) ou de constater le caractère illicite du traitement (let. c). Le deuxième alinéa précise les demandes que peut émettre la personne concernée, soit la rectification, l'effacement ou la destruction des données litigieuses (let. a)[175]. L'organe fédéral peut limiter le traitement des données en cause au lieu de les effacer ou de les détruire, si des intérêts prépondérants de tiers l'exigent (al. 3 let. b), ce qui serait reconnu si la destruction des données empêchait le tiers d'exercer ses droits en justice[176]. Cette disposition est-elle susceptible de trouver application lorsque la suppression des données compromettrait la recherche ? À notre sens, la réponse est négative en cas de traitement de données illicite à des fins de recherche. En effet, aucune étude n'est concrètement menacée dans cette hypothèse, et il incombe aux chercheuses et aux chercheurs de collecter les données nécessaires à l'avancement de leurs travaux sans violer les droits de la personnalité des personnes concernées. Lorsque la destruction des données compromet une étude déterminée, toutes les circonstances du cas d'espèce doivent intervenir dans l'appréciation. Il s'agira d'examiner notamment si l'étude a déjà démarré ou si elle réside encore au stade de projet, si elle est réellement compromise ou si la destruction des données litigieuses la complique seulement, la gravité des manquements et l'impact du traitement illicite des données pour la personne concernée. Contrairement à l'article 32 LRH, la légitimation active n'est pas limitée à la personne concernée mais elle est reconnue à tout individu qui présente un intérêt digne de protection. La procédure est régie par la loi fédérale sur la procédure administrative[177] (art. 41 al. 6 LRH). Si l'organe fédéral rejette la demande, sa décision est sujette à recours dans les 30 jours (art. 50 PA) auprès de l'autorité supérieure (art. 47 PA).

La personne concernée peut également revendiquer son droit d'accès à l'endroit de l'organe fédéral (art. 25 ss LPD ; *supra* V.B).

175 Les possibilités énoncées à la let. b nous apparaissent peu pertinentes pour le sujet de la présente contribution, de sorte que nous ne les abordons pas.

176 Message LRH, p. 6701.

177 Loi fédérale du 20 décembre 1968 sur la procédure administrative (PA), RS 172.021.

VII. Mesures extrajudiciaires

Comme mentionné, le législateur a relevé à l'occasion de la refonte de la loi sur la protection des données que les personnes concernées revendiquent peu la protection de leurs données, principalement dans le secteur privé[178]. La personne concernée dispose cependant d'alliés de taille dans les préposés à la protection des données et dans les commissions d'éthiques pour la recherche.

En cas de doute sur la manière dont ses données sont traitées dans le cadre d'une étude concrète ou à des fins de recherche, la personne concernée peut saisir le préposé à la protection des données compétent ou la commission d'éthique chargée de la surveillance d'un projet de recherche soumis à la loi relative à la recherche sur l'être humain.

En bref, le préposé fédéral à la protection des données est compétent pour enquêter contre un organe fédéral ou une personne privée si des indices suffisants font penser qu'un traitement de données pourrait heurter la législation (art. 49 al. 1 LPD)[179]. L'article 50 LPD lui accorde le pouvoir d'accéder aux données, d'auditionner des témoins et de mettre en œuvre des expertises. Au terme de son instruction, il ou elle peut ordonner des mesures visant la protection des données traitées (art. 51 LPD). La procédure est conduite selon les règles de la procédure administrative fédérale. Comme ces considérations ne sont pas propres à la recherche, nous renonçons à des développements détaillés et souhaitions uniquement rappeler l'existence de ces mesures qui sont vraisemblablement plus efficaces qu'une procédure judiciaire. En effet, la personne concernée se contente d'annoncer ses suspicions à un organe qui est spécialisé dans le domaine de la protection des données et qui peut prendre toutes les mesures propres à contrôler utilement la manière dont les données sont traitées. La personne concernée ne court donc aucun risque financier (bien que les procédures judiciaires soient désormais gratuites, la personne concernée n'est pas exemptée des honoraires de son avocat). Au demeurant, le préposé dispose de moyens d'investigation bien plus étendus que la personne concernée, qui supporte la charge de la preuve de la plupart des éléments constitutifs en cas de procès. Enfin, les scientifiques ne sont pas des voyous qui méprisent la protection de la personnalité des sujets de recherches. La coopération à l'instruction devrait donc être bonne et les chercheuses et les chercheurs seront sans doute enclins à prendre les mesures nécessaires pour corriger une éventuelle lacune dans la protection des données qui entacherait leur projet d'étude.

Les commissions d'éthiques de la recherche sont compétentes pour délivrer les autorisations à la réalisation d'un projet de recherche déterminé et à la

178 Message sur la révision totale de la LPD, p. 6737.

179 Les droits cantonaux attribuent aussi cette compétence aux préposé·es cantonaux.

réutilisation de données personnelles liées à la santé à des fins de recherche lorsque le consentement de la personne concernée ou que l'information au droit d'opposition font défaut (art. 45 LRH). Dans le cas où la sécurité des personnes concernées est menacée, elles peuvent révoquer ou suspendre l'autorisation ou encore subordonner la poursuite de l'étude à des conditions supplémentaires (art. 48 al. 1 LRH). À cette fin, elles peuvent exiger du titulaire de l'autorisation tous les renseignements et documents utiles (art. 48 al. 2 LRH). Elles vérifient encore si les projets de recherche et si leur réalisation respectent les exigences éthiques, juridiques et scientifiques qui émanent de la loi sur la recherche (art. 51 LRH). Par conséquent, une personne concernée peut aussi dénoncer une situation aux commissions d'éthique qui évalueront l'opportunité de prendre des mesures de surveillance. Une telle situation pourrait par exemple se produire si un patient qui, devant se soumettre à des tests génétiques, ressentait une certaine pression des soignants pour que ses données puissent être codées et réutilisées à des fins de recherche. Il pourrait aussi s'adresser à l'autorité de surveillance des professionnels de la santé qui pourrait rappeler au responsable du traitement son obligation de diligence, voire prononcer une mesure disciplinaire (art. 43 LPMéd[180] ; art. 19 LPSan[181] ; art. 30 LPsy[182]). Là encore, les scientifiques devraient collaborer pour ne pas retarder leurs recherches ou s'exposer à des sanctions.

Enfin, ces mesures extrajudiciaires sont plus rapides qu'une procédure judiciaire, qui pourrait entraîner le blocage d'une recherche durant les années sur lesquelles s'écoule le procès. De tels délais de traitement sont incompatibles avec le besoin de rapidité du milieu scientifique. Les découvertes et l'évolution du progrès qui en découlent conduisent à une obsolescence rapide des projets de recherche qui ne sont pas menés à terme dans des délais compétitifs. Pour toutes les raisons évoquées, nous estimons que les mesures extrajudiciaires sont plus appropriées que les procédures judiciaires, et ce pour toutes les parties.

VIII. Conclusions

Les intérêts antagonistes de la science et du droit à l'autodétermination des personnes concernées dont les données font l'objet d'un projet de recherche recèlent de nombreuses problématiques juridiques passionnantes qui s'enracinent pour la plupart dans l'équilibre délicat que la société doit atteindre dans l'arbitrage de ce conflit. L'éclatement de la matière corse la réflexion des juristes

180 Loi fédérale du 23 juin 2006 sur les professions médicales universitaires (Loi sur les professions médicales, LPMéd), RS 811.11.
181 Loi fédérale du 30 septembre 2016 sur les professions de la santé (LPSan), RS 811.21.
182 Loi fédérale du 18 mars 2011 sur les professions relevant du domaine de la psychologie (Loi sur les professions de la psychologie, LPsy), RS 935.81.

et complique sans doute le travail des chercheuses et des chercheurs. Il est aussi difficile pour la personne concernée de trouver son chemin au milieu de toutes les normes applicables et de comprendre le système juridique alors que les aspects techniques et scientifiques inhérents aux recherches scientifiques de pointe lui sont déjà difficilement accessibles. Dans le domaine de la recherche biomédicale, les sujets des études sont souvent des patient·es en cours de traitement. En sus de toutes les informations qu'ils et elles doivent intégrer en lien avec leur état de santé, ils et elles doivent encore donner de l'énergie à comprendre des descriptions de projets de recherche. Qui plus est, leur attention se portera davantage sur les risques liés à la recherche pour leur santé et sur les contraintes supplémentaires qu'une participation au projet de recherche impliquera. Au moment du consentement, les considérations propres à la protection de leurs données sont vraisemblablement reléguées au second plan. Selon les circonstances, il est donc légitime de s'interroger quant à la validité de leur consentement pour le traitement de leurs données.

Dans le cadre d'un projet de recherche, les données peuvent être traitées de nombreuses manières (collecte, codage, anonymisation, conservation, réutilisation, transmission, *etc*.). Différents principes régissent ces opérations et la réglementation diffère encore selon le type de données traitées et selon le genre de recherche.

Enfin, le droit en vigueur ne régit pas spécialement les procédures en cas de litige. La partie demanderesse est souvent confrontée aux difficultés d'apporter des preuves au procès. Au vu des compétences scientifiques et techniques très élevées de la recherche de pointe, la compréhension d'un projet de recherche et les techniques de traitement de données peuvent être hors de portée d'un individu non initié. À l'inverse, la chercheuse ou le chercheur peut être entravé dans son travail durant les années que dure une procédure, ce qui est absolument incompatible avec les exigences de rapidité en lien avec l'évolution scientifique.

Ces observations nous amènent à soutenir que notre législation n'encadre pas la recherche adéquatement. Avec le développement fulgurant de l'intelligence artificielle, le législateur devrait adopter une seule loi qui régisse intégralement la recherche, y compris celle relative à l'être humain. La loi devrait non seulement couvrir le traitement des données, mais aussi les démarches entreprises sur le corps humain, les personnes décédées, les embryons (y compris *in vitro*) et les fœtus et le matériel biologique. En bref, la loi devrait s'appliquer à l'ensemble de la recherche. Un projet d'une si grande envergure ne nous semble pas irréalisable concrètement, car de nombreux dénominateurs communs relient tous ces sous-domaines de la recherche. En outre, les intérêts en présence sont identiques et les difficultés sont communes. Cette loi devrait améliorer l'information qui est délivrée au moment de la collecte des données. La protection

des personnes concernées nous semble effectivement insuffisante à ce stade. Nous avons exposé que la personne concernée qui serait sollicitée pour participer à un projet de recherche ou pour offrir ses données à des fins de recherche alors qu'elle consulte un soignant en raison d'une atteinte à sa santé est fragilisée. Dans certains cas, elle est noyée sous une vague de renseignements en lien avec une prise en charge thérapeutique et encore d'informations concernant la participation à un projet de recherche, voire plusieurs. La manière dont ses données, qui sont collectées à l'occasion du traitement ou pour une recherche déterminée, seront traitées pour être réutilisées à des fins de recherche ne la préoccupe guère à ce stade selon la gravité de son état. Qui plus est, le patient pourrait craindre une forme de sanction en cas de refus de participation à un projet de recherche. Enfin, une personne qui n'est pas active dans ce domaine ne dispose pas des connaissances suffisantes pour évaluer le risque de réidentification de données pseudonymisées, voire anonymisées, par une analyse croisée de données rendue possible par le *big data*, les technologies et l'intelligence artificielle. La personne concernée devrait donc être convoquée à une séance d'information *ad hoc*, qui ne pourrait pas être organisée en même temps que la séance de renseignements et de consentement en lien avec un traitement médical. Les projets de recherche déterminés, la possibilité de la personne de pouvoir revenir sur son consentement à tout moment, le traitement des données en vue d'une conservation à des fins de recherche (p. ex. anonymisation), les effets d'un consentement général, le principe de l'*opt-out*, les risques de réidentification, devraient notamment lui être expliqués. Une brochure ou un formulaire, indiquant la personne responsable du traitement et les droits de la personne concernée, devrait compléter l'information délivrée oralement.

IX. Bibliographie

A. Littérature

François Bohnet, Actions civiles, Volume I : CC et LP, 2e édition, Bâle 2019 (cité : CPra Actions-Auteur, § X, N Y) ; **François Bohnet/Jacques Haldy/Nicolas Jeandin/Philippe Schweizer/Denis Tappy (éds)**, Code de procédure civile, Commentaire romand, 2e éd., Bâle 2019 (cité : CR CPC-Auteur, art. X, N Y) ; **Andrea Büchler/Dominique Jakob (éds)**, Kurzkommentar ZGB, 2e éd., Bâle 2018 (cité : KUKO ZGB-Auteur, art. X, N Y) ; **Isabelle Chabloz/Patricia Dietschy-Martenet/Michel Heinzmann (éds)**, Petit commentaire CPC, Bâle 2021 (cité : PC CPC-Auteur, art. X, N Y) ; **Rachel Christinat**, Le procès en responsabilité civile médicale, Mise en œuvre en procédures civile et administrative, thèse, Bâle/Neuchâtel 2019 ; **Yves Donzallaz**, Traité de droit médical, Volume II – Le médecin et les soignants, Berne 2021 ; **Philippe Ducor**, Protection de la personnalité des sujets de recherche, *in* : Margareta Baddeley *et al.* (éds), Facettes du droit de la personnalité, Journée de droit civil 2013 en l'honneur de la professeure Dominique Manaï, Genève 2014, p. 167 ss ; **Frédéric Erard**, Les données codées dans le contexte de la recherche : personnelles ou anonymes ?,

PJA 2021, p. 606 ss ; **Frédéric Erard/Mathilde Heusghem/Clément Parisato**, Recherche biomédicale et Open Data, perspectives en droit suisse, Jusletter 30 janvier 2023 ; **Thomas Geiser/Christiana Fountoulakis (éds)**, Zivilgesetzbuch I, Basler Kommentar, 7e éd., Bâle 2022 (cité : BSK ZGB-Auteur, art. X, N Y) ; **Agnès Hertig Pea**, La protection des données personnelles médicales est-elle efficace ? Étude des moyens d'actions en droit suisse, thèse, Bâle/Neuchâtel 2013 ; **Nicolas Jeandin/Aude Peyrot**, Précis de procédure civile, Genève/Zurich/Bâle 2015 ; **Alexandre Jotterand**, Personal Data or Anonymous Data : where to draw the lines (and why)?, Jusletter 15 août 2022 ; **Valérie Junod**, La responsabilité pour les dommages subis lors d'une recherche médicale : des difficultés inattendues, Responsabilité et Assurance 2015, p. 124 ss (cité : Junod, La responsabilité) ; **Valérie Junod**, Recherche médicale rétrospective : dès 2014, les règles changent, Revue Médicale Suisse 2014, p. 399 ss (cité : Junod, Recherche médicale rétrospective) ; **Philippe Meier**, Protection des données : fondements, principes généraux et droit privé, Berne 2010 ; **Paul Oberhammer/Tanja Domej/Ulrich Haas (éds)**, Kurzkommentar ZPO, 3e éd., Bâle 2021 (cité : KUKO ZPO-Auteur, art. X, N Y) ; **Pascal Pichonnaz/Bénédict Foëx (éds)**, Code civil I, Commentaire romand, Bâle 2010 (cité : CR CC-Auteur, art. X, N Y) ; **Karl Spühler/Luca Tenchio/Dominik Infanger (éds)**, Schweizerische Zivilprozessordnung, Basler Kommentar, 3e éd., Bâle 2017 (cité : BSK ZGB-Auteur, art. X, N Y) ; **Bernhard Rütsche**, Humanforschungsgesetz (HFG), Berne 2015 (cité : HFG-Auteur, art. X, N Y) ; **Vladislava Talanova/Franziska Sprecher**, Le consentement général : points à améliorer, Bulletin des médecins suisse 16 septembre 2020, p. 1197 ss ; **Florent Thouvenin/Thomas Gächter/Kento Reutimann/Samuel Mätzler**, Datenschutz in der Humanforschung: ein Forschungsprivileg für die Sekundärnutzung von Personendaten, Jusletter 30 janvier 2023 (cité : Thouvenin *et al*.).

B. Documents officiels

Conseil fédéral, Message concernant la loi fédérale sur l'analyse génétique humaine du 5 juillet 2017, FF 2017 5253 (cité : Message LAGH) ; **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, FF 2017 6565 (cité : Message sur la révision totale de la LPD) ; **Conseil fédéral**, Message sur la loi fédérale relative à la recherche sur l'être humain du 21 octobre 2009, FF 2009 7259 (cité : Message LRH).

Le privilège de la recherche et le rôle des commissions d'éthique de la recherche

VLADISLAVA TALANOVA
MLaw, Assistante-doctorante
Institut de droit de la santé, Université de Neuchâtel

ALEXANDRE DOSCH
Avocat

GÉRALDINE MARKS SULTAN
Dr iur.
Collaboratrice scientifique
Institut de droit de la santé, Université de Neuchâtel

DOMINIQUE SPRUMONT
Prof. Dr. Iur.
Président de la Commission d'éthique de la recherche du canton de Vaud
Institut de droit de la santé, Université de Neuchâtel
Professeur invité, UNISANTE, FBM, Université de Lausanne

Table des matières

I. Préambule

Parler de « privilège de la recherche » dans un ouvrage destiné à des experts de la protection des données et de la recherche impliquant des êtres humains peut porter à confusion et exige quelques éclaircissements.

En effet, pour les uns, issus du monde de la protection des données, cette expression désigne le régime d'exception de l'art. 13 al. 2 let. e aLPD[1] et de l'art. 31 al. 2 let. e LPD[2], autrement dit les aménagements que le législateur a accordé aux scientifiques en termes de protection des données afin de faciliter la recherche. Pour les autres, spécialistes des enjeux éthiques et juridiques de la recherche impliquant des personnes, cette notion désigne au contraire le principe selon lequel la réalisation de recherches avec des êtres humains n'est pas en soi un droit ou une liberté, mais seulement un privilège. Comme le rappelle l'art. 4 LRH[3], l'art. 2 de la Convention du Conseil de l'Europe sur les droits de l'Homme et la Biomédecine[4] ou l'art. 8 de la Déclaration d'Helsinki de l'Association médicale mondiale (AMM)[5], les intérêts des participants priment toujours les intérêts de la science et de la société. Dès lors, ce privilège ne peut s'exercer que si la protection des participants est garantie, en matière de protection des données également, et que leur dignité est respectée.

Dans le premier cas de figure, la recherche est perçue comme un bien commun, un intérêt général qui justifie *a priori* des exceptions aux droits et libertés des personnes qui y participent. Dans l'autre, la liberté scientifique est, *a contrario*

1 Ancienne loi fédérale sur la protection des données (LPD) du 19 juin 1992, RS 235.1.
2 Loi fédérale sur la protection des données (LPD) du 25 septembre 2020, entrée en vigueur le 1er septembre 2023, RS 235.1.
3 Loi fédérale relative à la recherche sur l'être humain (Loi relative à la recherche sur l'être humain, LRH) du 30 septembre 2011, RS 810.30.
4 Convention pour la protection des Droits de l'Homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine (Convention sur les Droits de l'Homme et la biomédecine), conclue le 4 avril 1997, entrée en vigueur pour la Suisse le 1er novembre 2008, RS 0.810.2.
5 Déclaration d'Helsinki de l'AMM – Principes éthiques applicables à la recherche médicale impliquant des êtres humains, Octobre 2013.

et par définition, sujette à restriction au nom de la protection des participants et de leur dignité.

Ignorer ces différences de perspective peut conduire à des résultats paradoxaux sous l'angle de la législation de la recherche impliquant des êtres humains. De récentes publications en la matière en sont une belle illustration. Citons notamment la thèse de doctorat d'Hélène BRUDERER portant sur le traitement des données personnelles liées à la santé à des fins de recherche scientifique qui a été soutenue et publiée en 2023[6] et deux articles qui ont été publiés en janvier 2023 dans la revue Jusletter[7]. Dans le premier, Samuel MÄTZLER présente les régimes de la protection des données applicables à la réutilisation des données à des fins de recherche sous l'angle du droit général de la protection de données – de la LPD – ainsi que sous l'angle de la législation de la recherche – de la LRH –. La seconde contribution de THOUVENIN *et al.* se fonde sur l'analyse de l'article de MÄTZLER et propose l'utilisation du régime général du privilège de recherche de la LPD dans le cadre de la recherche impliquant des êtres humains soumise à la LRH. Ce dernier article constitue le fil rouge de la présente contribution qui passe en revue le régime actuel applicable à la recherche impliquant les êtres humains.

THOUVENIN *et al.* proposent une modification du régime actuel pour la réutilisation de matériel biologique et des données personnelles à des fins de recherche impliquant les êtres humains selon les art. 32 à 34 LRH.

« *Cette réutilisation serait autorisée si les conditions suivantes du privilège de la recherche en matière de protection des données (i, ii et iii) et de la disposition d'exception de la LRH (iv et v) sont remplies :*

(i) Les données personnelles liées à la santé et le matériel biologique sont anonymisés dès que le but de la recherche le permet.

(ii) Les données personnelles liées à la santé et le matériel biologique ne sont communiqués à des tiers que de manière à ce que les personnes concernées ne soient pas identifiables.

(iii) Les résultats de la recherche ne sont publiés que de manière à ce que les personnes concernées ne soient pas identifiables.

(iv) Les personnes concernées ont été informées de l'utilisation des données personnelles les concernant à des fins de recherche et de l'existence de leur droit d'opposition, et elles n'ont pas manifesté d'opposition.

(v) Il existe une autorisation de la commission d'éthique. [...] Afin de réduire la charge de travail de toutes les parties concernées et de retarder le moins possible la recherche, il semble toutefois judicieux de soumettre à l'examen

6 BRUDERER.

7 MÄTZLER ; THOUVENIN/GÄCHTER/REUTIMANN/MÄTZLER.

> *de la commission d'éthique non pas des projets de recherche individuels, mais un « design de recherche » déterminé, dans lequel sont notamment définis le type de données, les responsables et les méthodes utilisées.* »[8] (notre traduction)

Même si elles ne sont pas explicites, deux prémisses semblent indissociables de cette proposition. La première concerne l'application du régime général du privilège de la recherche, au sens de la LPD (et lorsqu'il s'applique du RGPD[9]), dans le domaine de la recherche impliquant des êtres humains, abstraction faite de la LRH et de sa raison d'être. La deuxième sous-entend que l'application de l'art. 34 LRH, qui confère aux commissions d'éthique de la recherche (CERs) la compétence d'autoriser des recherches en l'absence de consentement des participants, est à tel point généralisée qu'il ne s'agit plus d'un régime d'exception et qu'elle devrait ainsi devenir la règle.

L'analyse point par point de la proposition de THOUVENIN et ses collègues demande ainsi de se déterminer au préalable sur la pertinence de ces deux prémisses.

II. Loi relative à la recherche sur l'être humain (LRH) vs Loi sur la protection des données (LPD)

Étendre le concept de « privilège de la recherche » établi dans le domaine de la législation sur la protection des données à celui de la recherche impliquant des êtres humains présuppose que la LPD soit une *lex specialis* par rapport à la LRH.

Alors que la protection des données est un enjeu majeur dans notre société de la communication, il peut paraître raisonnable d'en imposer les principes dans l'ensemble des activités humaines, quelle que soit la législation spécifique applicable. Cette vision est validée par le législateur – fédéral et cantonal – qui, de manière quasi systématique, renvoie à la législation sur la protection des données. Mais le même raisonnement est-il applicable à ses exceptions ? Autrement dit, est-il d'emblée acquis que les circonstances qui justifient une protection diminuée dans le domaine de la protection des données puissent remettre en cause les mesures de protection renforcée consacrées dans un autre domaine ? Pour répondre à cette question sous l'angle de la législation sur la recherche

8 THOUVENIN/GÄCHTER/REUTIMANN/MÄTZLER, p. 13-14.

9 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).

impliquant des êtres humains, il convient d'abord de comprendre sa raison d'être et ses origines.

A. Origines et raisons d'être de la réglementation de la recherche

L'histoire moderne de la réglementation de la recherche débute en 1947 avec l'adoption du Code de Nuremberg lors du procès contre les médecins nazis et l'adoption en 1964 de la Déclaration d'Helsinki par l'Association médicale mondiale. Depuis, les textes éthiques et légaux, internationaux, régionaux et nationaux relatifs à la recherche impliquant les êtres humains se sont multipliés, avec, chaque fois, pour objectif la protection des participants et le respect de leur dignité afin de prévenir les atrocités du passé[10]. Cette réglementation prend racine dans une longue succession d'abus[11]. Les expérimentations durant la Seconde Guerre Mondiale dans les camps de concentration par les médecins nazis en Europe ou japonais en Chine et en Mandchourie, l'affaire *Tuskegee*[12], l'étude de *Willowbrook Children Hospital*[13], ne sont que quelques exemples des atrocités perpétrées au nom de la science à l'encontre de personnes souvent en situation de vulnérabilité. Il en est découlé une prise de conscience de la nécessité de protéger les personnes dans le cadre des recherches et l'émergence de l'éthique de la recherche et de sa réglementation[14].

Dans le contexte de la présente contribution, l'histoire d'Henrietta Lacks et de ses cellules immortelles mérite d'être rappelée[15]. Elle est particulièrement révélatrice des enjeux en matière de réutilisation de données et d'échantillons biologiques à des fins de recherche, alors que certains pourraient être tentés de considérer que de telles études présentent moins de risques, voire aucun pour les participants.

Née en 1920, Henrietta Lacks est décédée en 1951 d'un cancer virulent du col de l'utérus. Elle était afro-américaine, mère de 5 enfants et venait d'un milieu modeste. Peu avant son décès, son médecin traitant a prélevé un échantillon de sa tumeur sans le consentement ni l'information d'Henrietta Lacks ou de sa famille. Les cellules prélevées, devenues célèbres sous le nom d'HeLa, se sont avérées avoir une capacité illimitée de se régénérer, autrement dit immortelles.

---

10 SPRUMONT, p. 252.

11 Pour reprendre l'expression de Carol Levine, « *the basic approach to the ethical conduct of research and approval of investigational drugs was born in scandal and reared in protectionism* » (*cf.* LEVINE, p. 167).

12 REVERBY.

13 ROBINSON/UNRUH.

14 SPRUMONT, p. 244 ss ; REVERBY ; ROBINSON/UNRUH.

15 Pour l'histoire de Henrietta Lacks, voir SKLOOT.

Les cellules HeLa ont ainsi été utilisées dans de nombreuses recherches sur le cancer et ont contribué à la mise au point de vaccins contre la poliomyélite et le virus de papillome humain (HPV), de médicaments contre le VIH, l'hémophilie, la leucémie ou la maladie de Parkinson. Elles ont été irradiées pour mesurer les effets de la bombe atomique et envoyées dans un vaisseau spatial. Les cellules HeLa sont l'une des découvertes plus importantes dans le domaine des sciences du vivant et leurs contributions aux connaissances actuelles sont colossales.

La famille d'Henrietta Lacks n'apprend toutefois l'existence du prélèvement que tout à fait par hasard 26 ans plus tard. En 1980, elle exprime publiquement sa désapprobation sur le fait que les services rendus par leur épouse, mère, grand-mère, sœur, tante, cousine, etc. à la science ne sont pas explicitement reconnus, et accuse les scientifiques de violation de sa vie privée, de manque d'information, d'absence de consentement et d'atteinte à la dignité de leur aïeule et de la leur. Aucune démarche n'est pourtant entreprise à cette époque par les scientifiques et les autorités pour répondre à ces critiques.

L'histoire rebondit en 2013 lorsque la séquence génétique des cellules HeLa est publiée en libre accès pour les scientifiques. La famille réagit à cette publication, notamment car la séquence des cellules HeLa peut exposer des informations non seulement sur Henrietta Lacks, mais également sur ses descendants. L'accès public est alors bloqué et la famille s'engage dans une discussion avec les *National Institutes of Health* (NIH), organe étatique américain qui avait pris le contrôle des cellules HeLa. Une solution est alors trouvée sous la forme d'une participation de deux membres de la famille Lacks dans le comité contrôlant l'accès aux données sur la séquence génétique de HeLa[16]. Enfin, en 2021, certains de ces petits-enfants ont ouvert une action civile à l'encontre de plusieurs compagnies pharmaceutiques pour enrichissement illégitime et usage non consenti des données et des cellules d'Henrietta Lacks. Un premier accord entre la famille Lacks et la société *Thermo Fischer*, qui commercialisait les cellules HeLa, a été conclu le 31 juillet 2023, d'autres actions en justice étant attendues[17].

62 ans se sont écoulés entre le prélèvement et la première reconnaissance des droits de la famille d'Henrietta Lacks. Cette histoire montre les implications qu'un « simple » prélèvement de cellules peut avoir pour la science, mais surtout pour la personne elle-même et ses descendants. Elle souligne la nécessité de garantir que la personne source puisse revendiquer des droits sur ses échantillons et avoir son mot à dire concernant leur utilisation.

Le besoin d'encadrer la recherche n'est pas seulement une exigence en raison des risques encourus par les participants et afin de garantir le respect de leur

16 HUDSON/COLLINS.
17 HOLPUCH.

dignité. En effet, même s'il ne peut y avoir de progrès médical sans recherche[18], toute recherche n'aboutit pas à une innovation. Malgré la place croissante prise par les sciences en médecine dès le XX^e^ siècle, celle-ci se caractérise encore par une grande incertitude[19]. Selon les méthodes d'évaluation, il est estimé que seuls 5 à 10 % des soins médicaux reposent sur des évidences scientifiques de haute qualité[20]. Si la recherche est incontestablement une nécessité, la capacité des chercheurs de produire des résultats pertinents pour la clinique doit être relativisée et cela n'est pas uniquement dû à la complexité des enjeux scientifiques, cliniques et biologiques auxquels ils sont confrontés.

L'optimisme et l'enthousiasme des chercheurs ainsi que d'éventuels conflits d'intérêts (intellectuels autant, voire plus souvent que financiers) obscurcissent aussi leur vision, ce qui se retrouve dans les articles scientifiques, soit dans la présentation des discussions ou l'analyse dans les conclusions qui vont souvent au-delà des stricts résultats[21]. En conséquence, seule une molécule sur dix testée chez l'humain fait l'objet *in fine* d'une autorisation de mise sur le marché. Ainsi, pour mémoire, une analyse des médicaments testés pour traiter la maladie d'Alzheimer entre 2002 et 2012, a mis en évidence un taux d'échec de 99,6 % si l'on exclut les molécules en phase III de développement[22], une étude de 2022 laissant toutefois entrevoir de modestes avancées[23]. Une étude sur le développement de médicaments entre 2010 à 2017 a aussi mis en lumière que 90 % des essais cliniques n'aboutissaient pas. Les raisons sont multiples : une absence d'efficacité clinique (40-50 %), une toxicité non gérable (30 %), de médiocres propriétés médicamenteuses (10-15 %) ou enfin un manque de besoins commerciaux ou une mauvaise planification stratégique (10 %)[24].Une autre publication de 2019 indique un taux de succès des essais cliniques de médicaments variant fortement selon les domaines, de 3,4 % en oncologie à 33,4 % pour les tests de vaccins contre des maladies infectieuses[25].

Un tel constat ne remet pas en cause l'intérêt scientifique et médical de mener des recherches avec des personnes, mais uniquement les bénéfices concrets à attendre de chaque étude en particulier. D'ailleurs, tout échec d'une approche

---

18 Pour reprendre l'expression de Cherif BASSIOUNI : « *Si le progrès médical devait dépendre uniquement du produit secondaire qu'est l'expérience conduite à l'occasion de la thérapeutique, nous nous retrouverions encore – métaphysiquement – à l'époque préhistorique* » (*cf.* BASSIOUNI, p. 274).

19 FOX.

20 FLEMING *et al*. ; HOWICK *et al*..

21 BOUTRON/DUTTON/RAVAUD/ALTMAN.

22 CUMMINGS/MORSTORF/ZHONG.

23 CUMMINGS/LEE/NAHED.

24 SUN/GAO/HU/ZHOU.

25 WONG/SIAH/LO.

scientifique n'aboutit heureusement pas à une impasse, mais peut ouvrir des pistes dans un autre domaine.

Citons, par exemple, le cas du bosentan qui est un médicament développé par *Roche* qui a été initialement évalué chez des patients hypertendus ou présentant une insuffisance cardiaque, deux affections très fréquentes dans la population, et dont la prise en charge médicamenteuse n'est pas optimale. Cette molécule ne s'est pas révélée être un meilleur antihypertenseur que les médicaments déjà commercialisés. De plus, si testé à trop haute dose dans l'insuffisance cardiaque, il pouvait être associé à une toxicité hépatique élevée. Ces résultats ne répondant pas à ses attentes, *Roche* abandonna cette ligne de recherche. Les époux Clozel reprirent toutefois les études mais cette fois pour l'hypertension pulmonaire, une maladie moins fréquente, mais pour laquelle aucun traitement oral n'existait. Leur persévérance a porté ses fruits. En effet, le bosentan produit d'excellents résultats pour cette autre indication[26]. Ce médicament, commercialisé sous le nom de *Tracleer*, a ainsi apporté une vraie plus-value thérapeutique pour les patients tout en générant un marché de plus d'un milliard de dollars[27].

La prudence reste toutefois de mise dans l'évaluation de la balance entre les bénéfices et les risques d'un essai clinique. D'autant plus que les chiffres susmentionnés ne disent rien sur la véritable plus-value thérapeutique que présentent les nouvelles molécules mises sur le marché, celle-ci étant malheureusement souvent plus faible qu'annoncée[28].

Participer à de la recherche ne doit donc pas être d'emblée assimilé au fait de bénéficier du meilleur traitement disponible, les participants recevant un placebo étant fréquemment mieux lotis que ceux traités avec le produit expérimental. Les bénéfices sont toujours hypothétiques et souvent inexistants, alors que si les risques se réalisent, ils sont bien concrets et directs pour les participants. Cela remet en cause le postulat de base sur lequel repose le concept de privilège de la recherche selon la LPD qui sous-entend que la recherche est, par définition, non seulement dans l'intérêt des chercheurs mais aussi des participants.

---

26 Voir KRUM *et al.* ; VAN VELDHUISEN/POOLE-WILSON.

27 SCHMIDT. Les auteurs tiennent à remercier Susanna GERBER et Nicolas SCHAAD, pharmaciens, respectivement vice-présidente et membre de la CER-VD, d'avoir suggéré cet exemple.

28 Voir par exemple COHEN. Une des rares revues pharmaceutiques non financée par l'industrie – Prescrire – publie chaque année un maigre palmarès des nouveaux médicaments présentant une véritable avancée pour les patients, ainsi qu'une liste (beaucoup plus longue) de médicaments sur le marché à déconseiller en raison de leur dangerosité ou de leur inefficacité. À ce propos, l'*Académie suisse des sciences médicales* soutient l'initiative « *Smarter Medicine* » qui met en avant pour chaque discipline les traitements excessifs ou inappropriés (<https://www.smartermedicine.ch/fr/page-daccueil>).

C'est justement le rôle des CERs, abordé plus bas, de s'assurer que les exigences éthiques, juridiques et scientifiques sont remplies afin de garantir la protection des participants et le respect de leur dignité face à l'enthousiasme (malheureusement souvent refroidi) des chercheurs. Au centre de cette démarche, il y a l'évaluation du rapport entre les risques et les bénéfices, ces derniers n'étant jamais garantis. Il convient donc de relativiser les bienfaits de la recherche du point de vue des participants, et de questionner la défense du « privilège de la recherche » sous l'angle de la LPD comme étant par définition un bien commun. Il s'agit en effet de ne pas confondre la notion de liberté scientifique telle que consacrée à l'art. 20 Cst.[29], et qui est à ce titre reconnue comme un intérêt général, avec le bénéfice réel d'un projet en particulier qui peut s'avérer nettement moindre qu'attendu par les chercheurs eux-mêmes et les promoteurs qui les financent.

B. Quelle est la *lex specialis* ?

La législation suisse relative à la recherche impliquant les êtres humains est le fruit de cet historique et repose sur ces fondements scientifiques et éthiques. Le besoin de protection des participants apparaît clairement au centre de cette législation ainsi que le souligne l'art. 118b Cst. : « La Confédération légifère sur la recherche sur l'être humain, *dans la mesure où la protection de la dignité humaine et de la personnalité l'exige.* » (nos italiques). Limiter ces mesures de protection ne peut donc s'envisager sans tenir compte de l'ensemble des enjeux spécifiques que soulève la recherche impliquant des êtres humains.

Une extension par principe de la notion de « privilège de la recherche » selon la LPD au domaine de la recherche impliquant des êtres humains semble exclue *a priori*. La primauté de la LRH sur la LPD s'explique notamment par l'histoire de la réglementation de la recherche, ainsi qu'en raison de la nature même de la recherche avec des personnes dont les bénéfices sont toujours hypothétiques. Il serait dès lors erroné de vouloir appliquer le régime général du privilège de la recherche selon la LPD à l'utilisation de données personnelles liées à la santé dans la recherche. En effet, la Loi fédérale relative à la recherche sur l'être humain (LRH) est une *lex specialis* par rapport à la législation sur la protection des données[30].

---

29 Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101.

30 Dans le même sens, voir dans cet ouvrage ERARD, p. 1 ss ; ERARD, Données codées, p. 613-614 ; Présentation de Julie GERBER intitulée « *Protection des données et recherche* » dans le cadre la journée thématique de la CER-VD du 28 février 2023,

Soulignons encore que la LPD et les lois cantonales sur la protection des données ne s'appliquent de toute manière qu'aux données personnelles, alors que les règles de la LRH visent également l'utilisation et la réutilisation du matériel biologique humain. Le régime du privilège de la recherche selon l'art. 13 al. 2 let. e aLPD et l'art. 31 al. 2 let. e LPD serait donc, dans tous les cas, limité par rapport à la LRH. Ce point remet aussi en cause la priorité défendue par certains de la LPD sur la LRH, même s'ils ne l'abordent pas. Dans tous les cas, le rattachement du matériel biologique à la personne et ses conséquences sous l'angle de la LRH devrait faire l'objet d'une analyse plus approfondie, mais cela dépasse le cadre de la présente contribution[31].

C. Rôle de la Commission d'éthique de la recherche (CER)

La Commission d'éthique de la recherche (CER) est l'autorité responsable pour l'évaluation des projets de recherche selon la LRH.

La Suisse compte sept commissions d'éthique de la recherche chacune compétente pour un ou plusieurs cantons. Par exemple, la juridiction de la Commission vaudoise d'éthique de la recherche (CER-VD) couvre les cantons de Vaud, Valais, Fribourg et Neuchâtel. Ces sept commissions sont regroupées dans l'Association suisse des commissions d'éthique de la recherche (*swissethics*). La mission principale de la CER est la garantie de la protection des participants à la recherche. Cette mission est expressément prévue à l'art. 118*b* al. 2 let. d Cst. et est rappelée à l'art. 51 al. 1 LRH. Dans cette optique, les CERs vérifient la conformité des projets de recherche aux exigences éthiques, juridiques et scientifiques.

Avant l'adoption de la LRH, dans un arrêt du 4 juillet 2003, le Tribunal fédéral avait déjà confirmé que les CERs sont investies d'une mission publique en matière de politique de la santé[32]. Selon le Tribunal fédéral, le rôle des CERs est une tâche de l'État et un organisme privé ne peut l'exercer sans délégation explicite des autorités compétentes. L'affaire concernait une CER privée – la *Freiburger Ethik-Kommission International* (FEKI) – qui évaluait en temps record les projets de la société *VanTx*. En fait, il s'est avéré que la tâche de la FEKI était

disponible à : <https://www.cer-vd.ch/ressources-opendata> et Homburger-memorandum, Swiss Legal Framework for De-identification of Health-Related Data, 2020, p. 8, disponible à : <https://sphn.ch/wp-content/uploads/2021/04/Homburger-memorandum_Swiss-Legal-Framework-for-De-identification-of-Health-Related-Data_20210105.pdf>.

31 A ce propos, mentionnons la thèse de doctorat d'Alexandre DOSCH en cours de finalisation sur le thème « *Le corps humain et ses parties détachées – Statut juridique dans la perspective de la santé personnalisé*e » qui aborde cette question de manière détaillée.

32 TF, 2A.450/2002 du 4 juillet 2003, c. 3.2. Voir aussi JOST.

facilitée par le fait que le chercheur principal de *VanTx* était également le directeur de la FEKI. Ceci explique la rapidité avec laquelle elle rendait ses décisions, mais également l'évaluation superficielle et entachée de conflits d'intérêts des protocoles. Suite à une série d'articles parus dans la presse estonienne, l'Office intercantonal de contrôle des médicaments (OICM), prédécesseur de *Swissmedic*, a été sollicité par les autorités estoniennes pour clarifier la situation. Dans ce contexte, l'OICM a découvert que les études menées par *VanTx* n'étaient pas conformes aux exigences éthiques, juridiques et scientifiques sur plusieurs aspects et notamment en ce qui concerne les modalités de recrutement des participants dans les pays d'Europe centrale et les pays baltes. En conséquence, le canton de Bâle a retiré l'autorisation cantonale de pratiquer à la FEKI qui a recouru en vain contre cette décision auprès du Tribunal fédéral[33].

Au vu de leur mission définie par la LRH en conformité avec le mandant du Constituant et la jurisprudence du Tribunal fédéral, les CERs se doivent en priorité d'assurer la protection des participants à la recherche. Ce faisant, elles appliquent la LRH et ses dispositions d'exécution à la lumière des exigences éthiques et scientifiques. Elles ne sont pas liées dans ce cadre par la notion de « privilège de la recherche » au sens de la LPD dans la mesure où celle-ci est une exception aux principes de l'éthique et de la réglementation de la recherche. Pour le moins, elles doivent s'assurer que cette exception est compatible avec lesdits principes avant de pouvoir considérer sa mise en œuvre dans un cas particulier. Une telle démarche recoupe l'évaluation des conditions d'application de l'art. 34 LRH.

III. Application de l'art. 34 LRH : toujours une exception

L'art. 34 LRH prévoit une procédure d'exception en cas de défaut de consentement de la part des participants. La CER compétente peut, à titre exceptionnel, donner une autorisation pour une réutilisation de données ou de matériel biologique à des fins de recherche sans consentement si les trois conditions cumulatives suivantes sont remplies :

a. l'obtention du consentement ou l'information sur le droit d'opposition est impossible ou pose des difficultés disproportionnées, ou on ne peut raisonnablement l'exiger de la personne concernée ;
b. aucun document n'atteste un refus de la personne concernée ;

[33] TF, 2A.450/2002 du 4 juillet 2003, c. 3.2 ; JOST. Concernant l'impact de l'affaire *VanTx* sur la refonte de la réglementation de la recherche en Suisse, voir aussi SPRUMONT, Droit suisse et progrès médical.

c. l'intérêt de la science prime celui de la personne concernée à décider de la réutilisation de son matériel biologique ou de ses données[34].

THOUVENIN *et al.* affirment que l'utilisation de l'art. 34 LRH est *de facto* devenue la règle et que le caractère exceptionnel de cette disposition a été dépassé par la réalité de la recherche. En outre, ces auteurs allèguent que la disposition est interprétée de manière extensive dans la pratique, alors qu'elle a été de toute évidence conçue pour s'appliquer de manière restrictive[35].

Ce constat se fonde sur les statistiques de 2019 publiées sous mandat de l'OFSP afin d'évaluer l'utilisation de l'art. 34 LRH ainsi que sur les statistiques de *swissethics* publiées en 2021. Celles-ci montrent que sur toutes les recherches avec réutilisation d'échantillons et données effectuées en 2019, les autorisations selon l'art. 34 LRH et celles avec consentement représentaient 60 % pour les premières et 40 % pour les secondes[36]. Ces chiffres soulèveraient un doute sur le caractère exceptionnel de l'application de l'art. 34 LRH.

Or, ces statistiques ne reflètent que partiellement l'attention portée par les CERs aux nombreuses demandes selon l'art. 34 LRH. De plus, les auteurs semblent ignorer la tendance à la baisse du nombre réel d'autorisations fondées sur l'art. 34 LRH observée ces dernières années alors qu'elle est reflétée dans les statistiques citées[37]. Cette tendance à la baisse est d'ailleurs confirmée par les nouvelles statistiques de 2022 tant au niveau national que régional[38].

Depuis l'entrée en vigueur de cette disposition en 2014, le nombre de demandes selon l'art. 34 LRH présente une tendance à la baisse alors que le nombre de demandes mixtes (art. 34 LRH avec une partie avec un consentement) est clairement en hausse[39]. Une des explications réside dans le fait que la LRH favorise la possibilité d'utiliser un consentement général pour la réutilisation d'échantillons et de données à des fins de recherche[40].

Par exemple, au CHUV, au 1er juin 2023, le taux d'acceptation du consentement général pour la réutilisation de données et échantillons biologiques s'élève à 80 %. Cela signifie que 20 % des personnes questionnées n'accepte pas de participer à la recherche[41]. Leur choix doit être respecté et les CERs ne l'ignorent pas. Ce chiffre semble être constant depuis quelques années et est représentatif

34 Art. 34 LRH.
35 THOUVENIN *et al.*, p. 8.
36 THOUVENIN *et al.*, p. 8-9 avec renvoi à DRIESSEN/CHRISTEN/GERVASONI, p. 7-8 et au rapport de *BSS Volkswirtschaftliche Beratung AG* de 2020.
37 BSS Volkswirtschaftliche Beratung AG, p. 2.
38 Selon les statistiques BASEC.
39 DRIESSEN/CHRISTEN/GERVASONI, Tabelle 4, Graphik 2.
40 SPRUMONT/ TALANOVA, p. 248 ss.
41 <https://www.chuv.ch/fr/consentement-general/cg-home/participer/quelques-chiffres>

de la réalité dans d'autres hôpitaux en Suisse et au-delà. Ainsi, au niveau européen, certaines études montrent que le taux d'acceptation varie également entre 80 et 85 %[42].

Le pourcentage de non-acceptation doit être gardé à l'esprit lors du traitement des demandes d'autorisation selon l'art. 34 LRH. En effet, cela signifie que lorsqu'une autorisation est accordée sur la base de cette disposition, un patient sur cinq est potentiellement opposé et n'aurait pas accepté de participer à la recherche s'il avait eu l'occasion de se prononcer. Les CERs sont conscientes de cette réalité et accordent une attention particulière aux demandes selon l'art. 34 LRH. En signe de son engagement dans le domaine, *swissethics* a modifié en 2020 sa manière d'établir les statistiques sur l'application de l'art. 34 LRH afin de mieux saisir les nuances entre les autorisations avec « pur » article 34 LRH et la majorité des cas où il y a un mélange entre consentement spécifique, consentement général et défaut de consentement selon l'art. 34 LRH. Les CERs limitent ces dernières à l'essentiel en restreignant autant que faire se peut le nombre d'autorisations ainsi que le nombre de personnes dont les données et échantillons peuvent être utilisés sans consentement. Pour la CER-VD, la part des projets de réutilisation autorisée exclusivement sur la base de l'art. 34 LRH est ainsi de l'ordre de 25 % depuis 2020 alors qu'ils représentaient près de 80 % des dossiers en 2017. L'octroi d'une autorisation selon l'art. 34 LRH constitue donc bien un acte exceptionnel, même si les demandes y relatives sont assez nombreuses.

La proposition d'ériger en règle l'autorisation pour défaut de consentement selon l'art. 34 LRH, comme proposé par THOUVENIN *et al.,* s'avère ainsi non seulement contraire aux principes du droit et de l'éthique de la recherche, mais aussi à la pratique des CERs. Il n'y a d'ailleurs pas de demandes de la part des chercheurs, en dehors peut-être de ceux qui maîtrisent mal la loi et les exigences éthiques et scientifiques. La priorité devrait plutôt être d'investir dans d'autres solutions susceptibles de contribuer à la baisse des demandes avec défaut de consentement.

La promotion de l'utilisation du consentement général à la recherche constitue dans ce sens une solution efficace pour limiter l'utilisation de l'art. 34 LRH, tout en garantissant les droits des participants et en permettant aux chercheurs d'utiliser les données et échantillons à des fins de recherches futures et indéfinies. Notons toutefois que malgré son utilisation en augmentation dans les hôpitaux et cliniques en Suisse, le formulaire de consentement général dit national

42 RICHTER *et al*.

adopté en 2018 par *Unimedsuisse*[43] et approuvé en 2019 par *swissethics*[44] présente d'importantes faiblesses du point de vue juridique et ne permet pas à lui seul de garantir les droits des personnes dont les données et échantillons sont collectés à des fins de recherche[45].

Soulignons aussi que, par principe, le consentement des participants est la réponse à une promesse[46]. Dans ce sens, il ne suffit pas de s'assurer que le formulaire permet effectivement un choix éclairé de la part des patients sur la base d'une information complète et compréhensible. Encore faut-il que les institutions qui font usage d'un formulaire de consentement général pour la recherche puisse garantir qu'elles sont en mesure de tenir leurs promesses telles que présentées dans ledit formulaire, autrement dit respectent les règles et les principes applicables en la matière. C'est pourquoi l'utilisation d'un formulaire de consentement général est soumise à des conditions strictes – exigées par *swissethics* et *Unimedsuisse* – telles que le respect de normes et standards nationaux et internationaux en matière de banques de données et de biobanques par les institutions[47].

L'encouragement des patients à signer un consentement général pour la recherche ne remet toutefois pas en cause la nécessité, dans les circonstances restrictives prévues par l'art. 34 LRH, que des chercheurs puissent mener des recherches avec défaut de consentement. C'est notamment le cas lorsque les données visées sont anciennes et qu'il est difficile, voire impossible de contacter les personnes concernées, notamment lorsqu'elles sont décédées. Cela vaut également si, pour des raisons scientifiques ou méthodologiques, il convient de disposer des données d'un grand nombre de personnes. Il existe aussi parfois un risque de biais de sélection si seules les données de personnes ayant signé le consentement général pour la recherche sont incluses dans un projet, les personnes avec les moins bons pronostics et les cas les plus graves n'étant pas toujours en mesure de signer le consentement général ou ne souhaitent pas.

---

43 Modèle de consentement général à la recherche 2019/2, disponible à : <https://www.unimedsuisse.ch/fr/projets/consentment-general>.

44 Swissethics, Communication du 22.02.2019 : Publication de la version 2 du consentement général national, disponible à : <https://swissethics.ch/fr/news/2019/02/22/veroeffentlichung-der-version-2-zum-nationalen-generalkonsent>.

45 Voir à ce propos TALANOVA/SPRECHER.

46 Voir la présentation Pablo DIAZ intitulée « *Conditions de partage de données de recherche* » dans le cadre la journée thématique de la CER-VD du 28 février 2023, disponible à : <https://www.cer-vd.ch/ressources-opendata>.

47 Swissethics, Communication du 22.02.2019 : Publication de la version 2 du consentement général national, disponible à : <https://swissethics.ch/fr/news/2019/02/22/veroeffentlichung-der-version-2-zum-nationalen-generalkonsent> ; Working Group General Consent unimedsuisse, Recommandations concerning the application of the General Consent version 2019, Version 1.0, 12.1.2020, disponible à : <https://www.unimedsuisse.ch/fr/projets/consentment-general>.

Dans ce cas, pour des raisons scientifiques et cliniques, il est admis d'accorder une autorisation avec défaut de consentement si les conditions de l'art. 34 LRH sont remplies, mais cela reste une exception.

IV. Anonymisation des données et des échantillons

A. Approche relative v. approche absolue

Le traitement particulier de données à des fins de recherche selon la législation sur la protection des données (art. 22 al. 1 aLPD, art. 31 al. 2 let. e LPD) – désigné comme le « privilège de la recherche » – est soumis à des conditions relatives à l'anonymisation des données. En principe, (1) les données doivent être anonymisées dès que le but de la recherche le permet, (2) les données doivent être communiquées à des tiers uniquement sous une forme ne permettant pas l'identification de la personne et (3) la même exigence s'applique à la publication de résultats de la recherche. THOUVENIN *et al.* reprennent ces conditions dans leur suggestion pour la révision de la législation sur la recherche (points (i), (ii) et (iii)). Cette proposition est une invitation à appliquer le régime général de la protection des données dans le cadre de la recherche impliquant des êtres humains.

Deux visions s'opposent en termes d'anonymisation des données, l'approche relative et l'approche absolue[48], étant entendu que dans ces deux approches l'anonymisation implique que les données perdent leur caractère personnel et ne sont dès lors plus soumises aux exigences de la législation. L'approche relative admise dans le contexte de l'application de la LPD signifie que le caractère personnel des données est apprécié du point de vue du destinataire des données et de l'environnement de partage. En ce qui concerne les données codées, celles-ci sont considérées comme anonymes – donc non personnelles – pour un destinataire qui n'a pas accès à la clé de codage. On parle d'approche relative car la personne qui a fourni les données reste en mesure d'identifier les personnes sources. Leur réidentification est donc possible sans fournir des efforts disproportionnés. Au contraire, selon l'approche absolue, les données codées sont considérées garder leur caractère personnel même lorsque le destinataire n'est pas capable d'identifier la personne, justement car le détenteur de la clé de codage ou les personnes ayant accès aux données sources peuvent réidentifier les personnes sources sans effort disproportionné. En matière de recherche impliquant des êtres humains, c'est l'approche absolue qui prévaut[49]. Cela est

48 Voir ERARD, Données codées pour une analyse détaillée et approfondie des approches adoptées dans le contexte de la protection des données (LPD, RGPD) et de la recherche (LRH).

49 Voir dans cet ouvrage, CHRISTINAT.

confirmé par les art. 32 et 33 LRH qui reconnaissent un droit à l'autodétermination aux participants sur leurs données non codées, mais aussi sur leurs données codées et leur anonymisation[50].

L'approche relative n'est pas soutenable dans le cadre de la recherche impliquant les êtres humains puisqu'elle va à l'encontre du but de la LRH à savoir la protection des droits des participants et de leur dignité. Si l'approche relative était applicable dans le cadre de la recherche impliquant des êtres humains, les données codées partagées avec le chercheur sans la clé de décodage seraient considérées comme anonymes de manière irréversible, ce qui permettrait audit chercheur d'échapper au champ d'application de la LRH en vertu de son art. 2 al. 2, laissant les participants sans la protection accordée par le droit et l'éthique de la recherche.

La législation impliquant les êtres humains – *lex specialis* – aborde l'enjeu de l'anonymisation aux art. 35 LRH et 25 ORH. Le matériel biologique et les données sont considérés comme anonymisés, lorsqu'ils *« ne peuvent pas être mis en relation avec la personne déterminée ou ne peuvent l'être sans engager des efforts démesurés »* (art. 3 let. i LRH). Cela implique la suppression irréversible du lien à la personne source. Le caractère identifiable des différentes informations doit alors être vérifié au cas par cas. Certains groupes ou populations peuvent présenter des caractéristiques propres et, associées aux éléments individuels, une personne peut ainsi être facilement identifiée ou identifiable. De même, des informations liées au contexte peuvent permettre l'identification d'une personne particulière[51].

Au sens de la législation de la recherche impliquant les êtres humains, l'anonymisation des données et de matériel biologique à des fins de recherche est soumise au droit d'opposition de la personne concernée. Alors que le droit d'opposition sera abordé dans la prochaine section, soulignons d'emblée que l'anonymisation n'est pas une mesure unilatérale du chercheur. Sous l'angle de la LPD, il s'agit d'un traitement de données, au même titre que la collecte, la conservation, l'exploitation ou la destruction[52]. En principe, elle requiert ainsi l'accord de la personne concernée, que ce soit sous forme d'un consentement – spécifique ou général – à la recherche ou de l'exercice du droit de non-opposition. Celui-ci est toutefois strictement encadré par la législation suisse et implique une information active de la personne concernée sur l'anonymisation et sur le fait qu'elle peut s'y opposer (art. 32 al. 3, art. 33 al. 2 LRH, art. 30 ORH).

50 ERARD, Données codées, p. 612.
51 FF 2009 7259, p. 7311 ; SHK HFG-RUDIN, art. 35, N 6.
52 Voir notamment ROSENTHAL, Handkommentar DSG, art. 3 let. e, N 63.

B. Concept dépassé ?

Si l'anonymisation protège en principe l'identité de la personne, le niveau de protection des droits des participants qu'elle garantit, sa faisabilité sous l'angle technique et sa pertinence pour la recherche sont aujourd'hui remises en question.

Les mesures de confidentialité ne visent pas uniquement à éviter une utilisation abusive des informations relatives à une personne, mais également à garantir et à protéger les droits des participants. Or, lorsque tout lien entre les données et la personne est rompu de manière définitive, cette dernière perd l'exercice de trois droits fondamentaux en lien avec ses données et échantillons. Premièrement, la personne concernée n'a plus le droit de savoir ce qui est fait avec ses données et son matériel biologique si ceux-ci sont anonymisés de manière irréversible. L'anonymisation met ainsi fin pour la personne concernée à son droit à l'autodétermination informationnelle prévu par la Constitution (art. 13 al. 2 Cst.) et son droit d'accès à ses données accordé par le droit à la protection des données (art. 8 aLPD, art. 25 LPD). Deuxièmement, la personne concernée ne peut plus retirer son consentement si elle change d'avis. Le droit à l'autonomie est donc également limité (art. 10 al. 2 Cst.). Troisièmement, la personne concernée ne peut plus recevoir les résultats de la recherche qui la concerne même si elle le souhaite (art. 8 LRH). En conséquence, l'anonymisation peut aboutir à de nombreuses atteintes à la personnalité de la personne source, dont l'absence de consentement si celui-ci fait défaut[53].

Une anonymisation absolue, autrement dit irréversible et ne permettant une réidentification qu'au prix d'efforts démesurés est devenue extrêmement complexe au XXI^e^ siècle car le risque de réidentification ne peut pas être complètement écarté. En 2013 déjà, une étude a démontré qu'il était possible à partir d'échantillons biologiques anonymisés de réidentifier les personnes sources par regroupement d'informations issues de diverses bases de données gratuitement et librement accessibles sur internet[54]. Pourtant, dans la pratique, des chercheurs continuent d'imaginer que le simple fait d'enlever ou de modifier les identifiants, à savoir le nom, l'adresse, la date de naissance ou le numéro AVS, suffit pour considérer des données comme anonymisées et justifie de ne pas soumettre leurs projets à la CER compétente. Même si une telle démarche représente une mesure de sécurité sous l'angle de la protection des données (limitation des risques en cas d'accès indus, *etc*.), elle ne vaut rien en termes d'anonymisation si, au demeurant, ils conservent l'accès aux données source. Un chercheur qui travaillerait avec les données de ses propres patients sous forme codée ne peut en effet nier le fait qu'il lui est aisé de comparer ces

53 BAERISWYL, p. 16 ; ELGER, p. 2511 ; SHK HFG-RUDIN, art. 32, N 23.
54 GYMSEK *et al*.

données « codées » avec les dossiers des patients afin de savoir à qui elles correspondent, quel que soit le nombre de ceux-ci. Dans les hôpitaux, les services informatiques sont clairement (et heureusement) en mesure de retrouver un patient avec peu d'indications, leur tâche étant encore plus simple lorsque, comme c'est souvent le cas en matière de recherche, ils disposent de dizaines, voire de centaines de paramètres.

Le caractère anonymisé des données doit donc être questionné en cas de recherches effectuées par des cliniciens ou des soignants, en cabinet ou à l'hôpital, qui utilisent les données de leurs patients ou d'autres patients de l'établissement. Dès lors que les chercheurs ont accès aux données sources dans le cadre de la clinique, il leur est simple de réidentifier les données de recherche même en l'absence de code en comparant les données sources avec celles de la recherche.

Un exemple vaut mieux parfois que toutes les théories. Voici ainsi l'histoire exemplaire d'une patiente qui, à son insu et anonymement (?), a été impliquée dans un projet de recherche[55]. A l'âge de 9 ans, Heidi[56] a été opérée dans un hôpital suisse pour des tumeurs hépatiques dont certaines étaient bénignes, d'autres pas. Malheureusement, 5 ans plus tard, en raison d'une grande fatigue, elle consulte ses médecins qui constatent une masse importante dans son foie. Elle doit alors subir une nouvelle opération. Dans l'intervalle, sa mère s'est inquiétée du fait qu'elle partageait des symptômes similaires. Travaillant comme chercheuse dans l'industrie pharmaceutique, elle conduit ses propres investigations et réalise qu'elle souffre du syndrome de Carney. Forts de cette information sur la santé de sa mère, les médecins d'Heidi envoient des échantillons de son sang aux *National Institutes of Health* (NIH) aux États-Unis, pour procéder à une analyse génétique auprès des spécialistes mondiaux de cette maladie rare. Le test confirme qu'elle souffre aussi du syndrome de Carney. Quatre ans plus tard, la veille de ses 18 ans, Heidi est de nouveau opérée mais aux États-Unis cette fois, par des spécialistes des NIH. A cette occasion, elle apprend l'existence d'un programme sur les maladies rares, dont la sienne, et souhaite participer à un des projets qui y est associé. À sa très grande surprise, les chercheurs américains lui indiquent que cela n'est pas possible, car son cas vient juste d'être publié[57]. Elle découvre ainsi que des chercheurs suisses, dont un de ses

55 Les auteurs tiennent à la remercier vivement d'avoir partagé son histoire et autorisé d'en parler. Son courage face à la maladie et aux personnes dont dépend sa survie force le respect. Elle fait partie de ces nombreuses personnes sans lesquelles les chercheurs ne pourraient rien. Comme Henrietta Lacks, elle mérite sans doute mieux qu'une simple note de bas de page dans une contribution scientifique comme signe de reconnaissance.

56 Prénom d'emprunt.

57 Cette réponse illustre une attitude, basée sur une logique académique et de propriété intellectuelle d'exclusivité sur les données et les échantillons, assez répandue chez les

médecins traitants, ont publié un article la concernant, dans lequel sa mère et son frère sont également mentionnés, sans qu'elle, pas plus que sa mère ni son frère, n'aient donné leur consentement, ni même ait été informés[58].

Heidi s'étant reconnue dans l'article et ayant été identifiée par d'autres, interpelle alors les auteurs de la publication. Ceux-ci lui répondent, sans saisir l'absurdité de leur affirmation, en maintenant que celle-ci a été réalisée avec des données anonymisées. Elle s'adresse aussi au service juridique de l'hôpital concerné pour essayer de comprendre. Sa réponse se borne à rappeler le cadre normatif sans aborder le cas concret :

« *In unserer Informationsbrochure weisen wir zudem die Patienten auch darauf hin, dass im Spital X medizinische Forschung betrieben wird. Dabei geht es einerseits um die Auswertung von Ergebnissen und medizinischen Angaben, welche von der Behandlung der Patienten stammen. Diese Daten werden anonymisiert* […]. *Sämtliche Publikationen erfolgen in anonymisierter Form. Solange die Publikation eines medizinischen Sachverhaltes keine Rückschlüsse auf den betroffenen Patienten oder die betroffene Patientin zulasst, ist sie ohne Einverständnis des Patienten oder der Patientin zulässig. Besteht jedoch die Möglichkeit, dass der geschilderte medizinische Sachverhalt einem Patienten oder einer Patient zugeordnet werden könnte, ist eine Einwilligung des Patienten oder der Patientin unumgänglich.*» (extrait du courrier du service juridique) (nos soulignés).

Il est vraisemblable que l'hôpital en question était au bénéfice d'une autorisation générale de lever le secret professionnel en matière de recherche médicale conformément à l'article 321bis CP[59]. L'affirmation selon laquelle le consentement n'est pas nécessairement requis est donc correcte si les conditions légales sont remplies. La première étant l'anonymat, cela semble *a priori* discutable dans le cas d'espèce[60]. En effet, il n'aura échappé à personne le paradoxe pour l'hôpital d'écrire à une de ses propres patientes, identifiée par des chercheurs aux États-Unis comme étant impliquée dans un projet de recherche conduit en son sein, qu'elle était informée que des recherches seraient faites avec ses données anonymisées (*sic*), autrement dit qu'elle ne serait donc pas identifiable.

La posture du service juridique de protéger en premier chef ses employés en évitant de se prononcer sur le fond n'est pas surprenante en soi. D'une part, il s'agit d'une des fonctions des affaires juridiques des hôpitaux d'éviter le

chercheurs qui tendent à ne pas partager « leurs » sujets de recherche. Le cas d'Heidi ne les intéresse plus car d'autres se le sont déjà appropriés.

58 TERRACCIANO *et al*.

59 Code pénal suisse du 21 décembre 1937, RS 311. Voir *infra* section VI.

60 Pour un rappel de ces exigences CourEDH, Arrêt du 13 janvier 2015, *Elberte c. Lettonie*, n° 61243/08 (voir commentaires *infra* section V.A.).

versement d'indemnités en décourageant les actions en responsabilité civile[61] et, d'autre part, le cadre légal était plus vague au moment des faits, la LRH ne devant entrer en vigueur que 10 ans plus tard. Espérons seulement que sa réponse serait différente aujourd'hui suite à la meilleure reconnaissance des droits des patients et à la création, dans beaucoup d'hôpitaux, d'espace d'accueil et de dialogue entre patients et professionnels de la santé[62].

Même si le cas d'Heidi concerne une personne avec une maladie rare et qui est donc plus susceptible d'être identifiée, il n'est pas unique, de nombreuses études fondées sur des données « anonymes » étant publiées dans la littérature scientifique. Pourtant, chacun, y compris un chercheur, peut imaginer ce que l'on peut ressentir en découvrant n'être qu'un « anonyme » pour ses propres médecins et dans son hôpital.

La désidentification des données est un processus rigoureux qui ne se résume pas de manière binaire au codage ou à l'anonymisation. Par design, les données anonymisées ne sont plus identifiables, et ceci de manière irréversible. Par design, les données codées sont identifiables. Si le code d'identification est détruit ou perdu, elles n'en deviennent pas pour autant anonymes et impersonnelles. Autrement dit, toutes les données désidentifiées ne sont pas soit codées, soit anonymisées. Certaines données demeurent personnelles même si elles ne sont pas ou plus codées, qu'elles aient été collectées sans identifiants ou que le code ait été détruit. Seules les données qui ont été désidentifiées de manière irréversible en application des standards reconnus[63], qui demandent de l'expertise et des moyens importants, peuvent être considérées comme anonymisées au sens de la LRH.

Dans le cadre du projet de révision de 2023 des ordonnances d'exécution de la LRH, l'OFSP reconnaît explicitement ce risque incompressible de réidentification des données dites anonymisées[64]. Ce projet de révision prévoit la modification de

---

61 On peut s'interroger sur la véritable liberté d'une jeune patiente de faire valoir ses droits alors qu'elle était à ce point dépendante de l'hôpital. Éthiquement, sa vulnérabilité aurait pu être davantage prise en compte. Plutôt que de faire comme si tout était en règle, il aurait aussi été possible de lui demander d'exprimer son libre choix concernant l'utilisation à des fins de recherche de ses données et de ses échantillons après l'avoir informée de manière complète et transparente sur ses droits et sur le contexte de cette recherche.

62 Comme l'Espace de médiation entre patients, proches et professionnels, créé au CHUV en 2012. Pour un aperçu passionnant de ce service, voir SCHAAD.

63 Voir Groupe de travail « Art. 29 » sur la protection des données, Opinion 05/2014 sur les Techniques d'anonymisation, 10.4.2014 et Norme ISO/IEC 27559:2022 : Sécurité de l'information, cybersécurité et protection de la vie privée – Cadre pour la déidentification de données pour la protection de la vie privée.

64 Office fédéral de la santé publique (OFSP), Révision partielle des ordonnances d'exécution de la loi relative à la recherche sur l'être humain (LRH), Rapport explicatif, Berne, 26 avril 2023, p. 38-39.

l'art. 25 ORH concernant l'anonymisation des données et des échantillons biologiques afin de mieux éclairer l'application de la LRH à la lumière des connaissances et de la pratique actuelles. Selon cette proposition de révision actuellement en consultation, une simple désidentification, autrement dit la modification ou la destruction d'identifiants, ne suffit pas pour admettre que des données sont anonymisées de manière irréversible. Il faut en outre démontrer, en le documentant, que le processus de désidentification respecte les méthodes conformes à l'état actuel de la science et de la technique pour l'anonymisation du matériel biologique et des données. Enfin, il est aussi requis de décrire le risque de réidentification qui subsiste[65]. Les progrès des sciences des données (*data sciences*) et dans le domaine informatique augmentant constamment ce risque, SPHN développe actuellement des outils performants pour le réévaluer régulièrement et éviter qu'il ne se réalise en prenant les mesures de sécurité supplémentaires qui s'imposent[66].

Sur un autre plan, l'anonymisation entraîne une perte de valeur des données et des échantillons pour les chercheurs dans la mesure où il n'est plus possible de les comparer avec d'autres données ou des données futures concernant les mêmes personnes sources. D'un côté, les nouvelles informations personnelles pertinentes ne peuvent plus être rajoutées au dossier du participant et, d'un autre, les nouveaux échantillons pouvant être prélevés afin de procéder au suivi de la maladie ou à l'évolution de l'efficacité du traitement, par exemple, ne peuvent plus être comparés avec les résultats obtenus précédemment. Or, de tels rectifications et ajouts peuvent s'avérer importants pour le bon déroulement du projet de recherche comme dans le cas des cohortes[67]. L'anonymisation est, par ailleurs, interdite dans le cadre d'essais cliniques puisqu'elle rend impossible l'audit et le contrôle des données médicales qui ne peuvent se faire que sur les données sources. Enfin, l'anonymisation a un coût élevé si elle est faite selon les standards reconnus au niveau international.

Pour toutes ces raisons, les CERs encouragent l'utilisation du codage à la place de l'anonymisation lorsque cela est pertinent. Au sens de la législation sur la recherche, le matériel biologique et les données sont considérés comme codés lorsqu'ils « *sont qualifiés d'anonymisés dans l'optique d'une personne qui n'a pas d'accès au code* » (art. 26 ORH). Selon ERARD, cette définition ne remet pas en question l'application de l'approche absolue présentée précédemment, mais témoigne de l'importance du traitement différencié des données anonymes et des données codées[68]. Travailler avec des données codées est généralement

65 Art. 25 al. 2 et 3 P-ORH mis en consultation.

66 SPHN, « Guidance for de-identification of health-related data in compliance with Swiss legal and data protection regulations », disponible à : <https://sphn.ch/network/data-coordination-center/de-identification/>.

67 CNE, p. 44, ch. 121.

68 ERARD, Données codées, p. 614.

plus simple, efficace et moins coûteux, la charge administrative étant souvent inférieure ou équivalente à ce qu'exige une véritable anonymisation, les mesures techniques et organisationnelles de sécurité étant déjà en place dans les hôpitaux et les institutions de recherche pour protéger les données, notamment contre des accès indus. L'anonymisation doit donc être utilisée uniquement lorsque cela est indispensable et justifié tout en tenant compte du fait que l'anonymisation absolue n'est pratiquement plus possible[69].

V. (Non) droit d'opposition

A. Parallèle entre droit d'opposition, consentement général et consentement présumé

Les art. 32 al. 3 et 33 al. 2 LRH instaurent le régime du droit d'opposition pour l'utilisation du matériel biologique et des données à des fins de recherche. Ces dispositions prévoient que, lors de l'anonymisation de matériel biologique et de données génétiques ou encore la réutilisation à des fins de recherche de données personnelles non génétiques liées à la santé codées, une atteinte à l'intégrité de la personne ou à sa vie privée est justifiée si la personne concernée, après avoir été informée[70], renonce à son droit d'opposition[71]. Relevons que l'information préalable doit être fournie soit par écrit, soit par oral[72] et qu'elle est une condition essentielle à l'existence d'un motif justificatif[73]. En cas de renonciation au droit d'opposition, la doctrine parle de consentement tacite[74].

THOUVENIN *et al.* s'appuient sur ces dispositions et proposent leur utilisation plus systématique.

Or, l'utilisation du droit d'opposition dans la recherche impliquant les êtres humains est abandonnée en pratique depuis 2017. Pour rappel, le premier modèle suisse de formulaire de consentement général a été adopté cette année-là par l'Académie suisse des sciences médicales. Ce formulaire faisait explicitement

69 Swissethics, Entwurf für die Revision der Verordnungen HFG, Stellungnahme swissethics, 31. Januar 2023.

70 Pour le contenu de l'information, voir les art. 30 et 32 ORH.

71 SHK HFG-RUDIN, art. 33, N 14 à 15 ; SHK HFG-VAN SPYK, art. 7, N 14.

72 Voir les art. 30 al. 1 et 32 al. 1 ORH.

73 SHK HFG-RUDIN, art. 32, N 26 ; SHK HFG-RUDIN, art. 33, N 14 ; VAN SPYK, p. 112.

74 « *Stillschweigende Einwilligung durch Verzicht auf Widerspruch nach vorgängiger Information* » (SHK HFG-VAN SPYK, art. 7, N 14). Notons que d'autres motifs justificatifs tels que le consentement présumé ou hypothétique ne sont pas prévus par la LRH et ne permettent par conséquent pas de justifier une atteinte à l'intégrité d'une personne ou à sa vie privée dans le cadre d'une recherche : SHK HFG-VAN SPYK, art. 7, N 11.

référence au droit de non-opposition pour l'utilisation de données génétiques sous forme codée et l'anonymisation des échantillons biologiques. Le formulaire prévoyait la possibilité de communiquer son opposition à la recherche directement à son médecin traitant ou à un contact figurant à la fin du document. Le formulaire précisait aussi qu'en cas d'absence de décision, l'utilisation serait considérée comme acceptée[75]. Une évaluation indépendante de la mise en œuvre de ce formulaire mandatée par l'Académie suisse des sciences médicales et réalisée par *Swiss Biobanking Platform* (SBP), a toutefois mis en évidence que ce modèle n'a été utilisé par aucun hôpital universitaire, cette étude étant de plus critique concernant le principe-même du droit d'opposition[76]. De sorte, la nouvelle version du modèle suisse de consentement général pour la recherche adopté en 2018 par *Unimedsuisse*[77] ne comporte plus de mention relative au droit d'opposition. À notre connaissance, cette option ne semble pas non plus être retenue dans les autres formulaires de consentement général actuellement validés par les CERs en Suisse.

Pour conclure sur la question du droit d'opposition, il paraît intéressant d'aborder encore la règle du consentement présumé dans la mesure où elle présente certaines analogies. Cette règle est reconnue en matière de transplantation d'organes. Sa compatibilité avec la liberté personnelle et la dignité humaine a été admise par le Tribunal fédéral à plusieurs reprises[78] et le 15 mai 2022 le peuple suisse a approuvé l'introduction du consentement présumé pour le prélèvement d'organes et de tissus après le décès de la personne dans la législation fédérale sur la transplantation d'organes[79]. *Mutatis mutandis*, il ne serait donc pas exclu d'envisager la mise en œuvre du consentement présumé dans la recherche, mais sous réserve de respecter des conditions précises qui restent à définir.

La Cour européenne des droits de l'homme (CourEDH) s'est déjà penchée sur la question de la validité de la règle de consentement présumé et des modalités d'exercice du droit d'opposition dans le domaine de la recherche[80]. L'affaire

---

75 Modèle de consentement général version 1/2017, p. 1.

76 SWISS BIOBANKING PLATFORM, Evaluation report V1/2017 : National consent, March 2018, p. 4.

77 Modèle de consentement général à la recherche 2019/2, disponible à : <https://www.unimedsuisse.ch/fr/projets/consentment-general>. Voir TALANOVA/SPRECHER pour les faiblesses du modèle de 2019.

78 ATF 98 Ia 508, JdT 1973 I p. 490 ; ATF 112 Ia 350 ; ATF 123 I 112.

79 Initiative populaire « *Pour sauver des vies en favorisant le don d'organes* » et contre-projet indirect du Conseil fédéral et du Parlement. Le peuple a approuvé le contre-projet indirect à 60,2 % des voix. Plus d'informations disponibles à :<https://www.bag.admin.ch/bag/fr/home/medizin-und-forschung/transplantationsmedizin/rechtsetzungsprojekte-in-der-transplantationsmedizin/revision-des-transplantationsgesetzes/indirekter-gegenvorschlag-organspende-initiative.html>.

80 CourEDH, Arrêt du 13 janvier 2015, *Elberte c. Lettonie*, nº 61243/08, par. 14.

concerne M^me^ Dzintra Elberte, née en 1961 et dont le mari décède d'un accident en 2001. À l'époque, son cadavre avait fait l'objet d'une autopsie réalisée par le Centre national médico-légal de Riga. Deux ans plus tard, elle est informée que des prélèvements de tissus ont été faits sur le corps de son mari, à des fins de transplantation ou de recherche, et qu'une enquête est ouverte à l'encontre de ce centre concernant des prélèvements illégaux d'organes et de tissus envoyés à une société pharmaceutique de 1994 à 2003. L'enquête fut classée en 2005, mais M^me^ Elberte s'est battue pour faire reconnaître ses droits et ceux de son époux. Après une longue procédure, elle obtint en 2015 la condamnation de la Lettonie par la CourEDH pour violation des articles 3 et 8 CEDH[81].

Dans ce cadre, la Cour a conclu que les dispositions prévoyant le droit de s'opposer doivent non seulement être claires et précises, mais les conditions juridiques et pratiques de sa mise en œuvre doivent également être garanties[82]. Le cas échéant, les interventions sur le cadavre constituent une violation de l'art. 3 CEDH qui interdit aux États de commettre des actes de torture ou de faire subir des peines ou des traitements inhumains ou dégradants. De sorte, l'utilisation du consentement présumé n'est admissible que lorsqu'il est prévu explicitement par une loi et si une information adéquate est offerte à la population et aux proches dans un cas concret[83]. Ces conclusions semblent s'appliquer tant en matière de transplantation d'organes que dans le domaine de la recherche scientifique[84].

B. Mise en œuvre délicate en l'absence de preuves fiables

Les difficultés pratiques et juridiques de la mise en place et de l'exercice du droit d'opposition sont nombreuses. La première est liée aux moyens de preuve que l'information a bien été fournie, lue et comprise par la ou le véritable destinataire, autrement dit la personne à qui le consentement est demandé.

Dans les procès portant sur la protection de la personnalité, le fardeau de la preuve des faits dont découle l'atteinte incombe au demandeur, en sa qualité de victime, tandis que le défendeur, en tant qu'auteur potentiel de l'atteinte, doit prouver les circonstances qui permettent de conclure à l'existence d'un

81 Voir CourEDH, Arrêt du 13 janvier 2015, *Elberte c. Lettonie*, n° 61243/08.

82 CourEDH, Arrêt du 13 janvier 2015, *Elberte c. Lettonie*, n° 61243/08, par. 114.

83 CourEDH, Arrêt du 13 janvier 2015, *Elberte c. Lettonie*, n° 61243/08, par. 42 ; ATF 123 I 112, c. 9e.

84 Pour une présentation et analyse approfondie de l'arrêt *Elberte c. Lettonie*, voir SPRUMONT/TALANOVA.

motif justificatif[85]. Dans ce cadre, soulignons que le Tribunal fédéral considère que l'envoi par pli simple n'emporte aucune garantie de réception effective[86].

C'est pourquoi RUDIN considère que la personne ou l'entité responsable de la réutilisation serait avisée de conserver tout document attestant que l'information a été donnée et que la personne concernée n'a pas fait usage de son droit d'opposition. Cet auteur conclut que, dans ce sens, la charge administrative liée au droit d'opposition n'est que légèrement moins contraignante que celle relative au consentement[87]. Au vu de cette différence minime, on peut d'ailleurs s'interroger si cela n'est pas finalement plus simple de demander le consentement des personnes concernées plutôt que de jouer avec la règle de la non-opposition avec toutes les incertitudes que cela entraîne.

D'un point de vue procédural, l'article 55 al. 1 CPC[88] rappelle que « *les parties allèguent les faits sur lesquels elles fondent leurs prétentions et produisent les preuves qui s'y rapportent* ». À la lumière de cet article, un fait, tel que la réception d'un courrier, qui ne serait pas avancé ou prouvé n'existe donc pas pour le tribunal compétent[89]. De jurisprudence constante, le Tribunal fédéral a établi que le fardeau de la preuve de la notification d'une décision et de la date de celle-ci incombe en principe à l'autorité qui entend en tirer une conséquence juridique[90]. L'autorité supporte donc les conséquences de l'absence de preuve en ce sens que si la notification ou sa date sont contestées et qu'il existe effectivement un doute à ce sujet, il y a lieu de se fonder sur les déclarations du destinataire de l'envoi[91]. Notons toutefois que la preuve de la notification peut néanmoins résulter d'autres indices ou de l'ensemble des circonstances, par exemple un échange de correspondance ultérieur ou le comportement du destinataire[92].

Relevons que dans le cadre d'une procédure administrative portant sur une décision du Service des contributions de la République et canton de Neuchâtel, notifiée par pli simple, le Tribunal fédéral a aussi relevé que le mode d'envoi choisi par le service cantonal n'offre aucune preuve formelle de notification[93]. Vu ce qui précède, tant d'un point de vue civil, pénal qu'administratif, celui qui invoque l'absence d'opposition doit prouver la réception de l'information et le fait que la personne n'a pas fait d'opposition. La preuve de la réception de

85 Voir notamment ATF 136 III 410, c. 2.3, JdT 2010 I p. 557.
86 TF, 4A_39/2007 du 9 mai 2007, c. 4.
87 SHK HFG-RUDIN, art. 33, N 16.
88 Code de procédure civile du 19 décembre 2008, RS 272.
89 BK ZPO-HURNI, art. 55, N 9.
90 ATF 142 IV 125, c. 4.3 ; voir également ATF 136 V 295, c. 5.9 et les références citées.
91 ATF 142 IV 125, c. 4.3 ; ATF 129 I 8, c. 2.2 ; ATF 124 V 400, c. 2a ; TF, 6B_869/2014 du 18 septembre 2015, c. 1.2.
92 ATF 142 IV 125 c. 4.3 ; ATF 105 III 43, c. 2a.
93 TF, 2C_250/2018 du 26 octobre 2018, c. 3.

l'information préalable à la renonciation au droit de s'opposer ne peut être apportée lorsqu'elle est transmise à la personne concernée par pli simple. En l'état, une telle preuve paraît difficile à apporter.

D'un point de vue éthique, demander le consentement des patients apparaît indubitablement plus respectueux de leur autonomie que de collecter leur non-opposition. Le fait que les hôpitaux universitaires aient investi des moyens importants dans la solution du consentement général pour la recherche dénote clairement leur volonté d'offrir aux patients la possibilité d'exercer leur libre arbitre de manière transparente. Il faut ainsi saluer le fait qu'ils aient renoncé à faire usage du droit de non-opposition pourtant consacré par la LRH. Les problèmes de preuve susmentionnés expliquent peut-être en partie leur choix. Il eût été intéressant que THOUVENIN *et al.* approfondissent cette problématique dans leur proposition. À défaut, sa mise en œuvre semble fortement compromise.

VI. Autorisation de projets de recherche uniquement sur la base du design

Selon l'art. 45 LRH, le rôle des CERs est l'évaluation de chaque projet de recherche et son autorisation s'il respecte les exigences juridiques, éthiques et scientifiques. THOUVENIN *et al.* proposent de soumettre à l'examen de la CER compétente un « design de recherche » déterminé, dans lequel sont notamment définis le type de données, les responsables et les méthodes utilisées.

Cette proposition n'est pas sans rappeler le régime d'autorisation lié à la levée du secret professionnel en matière de recherche sur l'être humain antérieur à l'entrée en vigueur de la LRH en 2014. L'art. 321bis al. 5 aCP[94] stipulait en effet que « [l]*a commission peut octroyer des autorisations générales ou prévoir d'autres simplifications si les intérêts légitimes des intéressés ne sont pas compromis et si les données personnelles sont rendues anonymes dès le début des recherches* ». Cette disposition concernait la Commission d'experts du secret professionnel en matière de recherche médicale et était précisée par l'Ordonnance du 14 juin 1993 concernant les autorisations de lever le secret professionnel en matière de recherche médicale (OALSP)[95]. Ces autorisations générales s'adressaient aux hôpitaux et cliniques afin de faciliter la transmission des données personnelles au sein de l'institution à des fins de recherche (art. 3 al. 1 OALSP) ainsi qu'aux registres médicaux (art. 3 al. 3 OALSP). Pour la première catégorie, l'autorisation s'accompagnait d'un devoir d'annonce des

94 Code pénal suisse du 21 décembre 1937, RS 311.0, RO 1993 1945.
95 RO 1993 1983.

projets de recherche interne et son approbation par une commission d'éthique ou un autre organe était nécessaire[96].

Avec l'entrée en vigueur de la LRH, la possibilité d'octroi d'autorisations générales a toutefois été supprimée. Selon le Conseil fédéral, cette suppression est due au caractère superflu et inutile de ces autorisations au vu de l'obligation de soumettre tout projet de recherche à la CER compétente[97].

Un système semblable à celui fondé sur l'autorisation du design de recherche existe déjà en droit français. Cela vaut la peine de s'y arrêter sous l'angle théorique, mais aussi dans la mesure où les chercheurs suisses collaborent régulièrement avec leurs collègues français. Ils sont alors soumis au même régime pour les données qui viennent de France. Ce système s'applique aux études avec des données et des échantillons biologiques humains qui ne sont pas qualifiées de recherches impliquant la personne humaine et qui sont régies par la Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[98]. En le transposant au droit suisse, ce système pourrait être celui applicable aux recherches avec les données personnelles de santé qui ne seraient pas soumises à la LRH, mais régies uniquement par la LPD.

Ce système vise les méthodologies de références qui sont homologuées et publiées par la Commission nationale de l'informatique et des libertés (CNIL) (art. 73 Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). Si un projet de recherche utilise une méthodologie de référence, une simple déclaration de conformité à la place d'une autorisation de la CNIL suffit (art. 66, 73 et 76 Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

À titre d'exemple, deux méthodologies de références essentielles sont la méthodologie de référence MR-003 « Recherches dans le domaine de la santé sans recueil du consentement » (CNIL – Délibération nº 2018-154 du 3 mai 2018[99]) et la méthodologie de référence MR-004 « Recherches n'impliquant pas la personne humaine, études et évaluations dans le domaine de la santé » (CNIL – Délibération nº 2018-155 du 3 mai 2018[100]). Chacune de ces méthodologies

96 FF 2009 7280.

97 FF 2009 7339 et 7340.

98 Les projets de recherches qui ne sont pas considérés comme impliquant la personne humaine sont énumérés à l'article R.1121-1 du Code de la santé publique français.

99 CNIL, Méthodologie de référence MR-003, « Recherches dans le domaine de la santé sans recueil du consentement », disponible à : <https://www.cnil.fr/fr/declaration/mr-003-recherches-dans-le-domaine-de-la-sante-sans-recueil-du-consentement>.

100 CNIL, Méthodologie de référence MR-004, « Recherches n'impliquant pas la personne humaine, études et évaluations dans le domaine de la santé », disponible à : <https://www.cnil.fr/fr/declaration/mr-004-recherches-nimpliquant-pas-la-personne-humaine-etudes-et-evaluations-dans-le#:~:text=La%20m%C3%A9thodologie%20de%20r%C3%A9f%C3%A9rence%20MR,impliquant%20pas%20la%20personne%20humaine>.

de référence énonce les données personnelles couvertes et exclues, les objectifs admis du traitement de ces données et conditions d'utilisation (information et droit d'opposition), la durée de conservation des données, les destinataires des données et les mesures de sécurité et de maintien de la confidentialité.

On se rapproche ici de la proposition de THOUVENIN *et al.* avec une nuance importante. En effet, il manque actuellement en droit suisse les bases légales et les outils de référence pour évaluer un projet uniquement sous l'angle de son design. En France, cette tâche relève directement de la CNIL. Pour la Suisse, celle-ci aurait peut-être pu être assumée par la Commission d'experts du secret professionnel en matière de recherche médicale selon le droit antérieur, mais il n'est plus applicable. Actuellement les domaines de vérification des projets de recherche par les CERs sont énumérés à l'art. 15 ORH et vont au-delà d'un simple examen de design. En plus de la vérification des objectifs du projet, des conditions d'utilisation, des mesures de sécurité et de confidentialité et d'autres aspects énoncés dans les méthodologies de référence, les CERs sont tenues d'évaluer également, par exemple, la qualité scientifique du projet, les qualifications professionnelles de la direction et la disponibilité de ressources matérielles et financières du projet particulier. En l'état, il manque donc une base légale pour mettre en œuvre cette proposition.

VII. Conclusion

L'extension du principe du « privilège de la recherche » selon la LPD au domaine de la recherche impliquant des êtres humains avec réutilisation de données et d'échantillons est moins évidente qu'il n'y paraît. La démarche demanderait de démontrer en premier lieu la primauté de la LPD sur la LRH ce qui va à l'encontre des fondements historiques et constitutionnels de la législation sur la recherche avec des personnes. Ensuite, elle exigerait un encadrement strict de la procédure d'anonymisation qui, dans le domaine de la recherche, repose sur l'approche absolue et ne se limite pas à une simple désidentification. Les contraintes pour les chercheurs dépasseraient ainsi celles liées à un simple codage. Elle demanderait aussi de régler le processus de mise en œuvre du droit d'opposition des personnes concernées avec la difficulté pour les chercheurs d'en apporter la preuve conformément aux codes de procédure pénal et administratif et de la jurisprudence. Enfin, elle exigerait une redéfinition du rôle des Commissions d'éthique de la recherche en contradiction avec le droit applicable. De tels efforts, aux résultats incertains, sont-ils pour autant nécessaires si l'objectif est de favoriser la recherche impliquant les êtres humains et les bénéfices qui en découlent pour les patients, le système de soins et le système de santé ?

Au-delà de ces enjeux, pour certains de nature plutôt technique et auxquels il serait possible de répondre dans le cadre d'une révision de la LRH et de ses ordonnances d'exécution, ce sont deux approches de la notion d'innovation qui s'opposent. La première se caractérise par une vision idéalisée des bienfaits concrets et immédiats de la recherche pour les participants, la seconde reposant sur une vision plus pragmatique, basée sur des preuves scientifiques, reconnaissant le caractère toujours hypothétique des bénéfices de la recherche alors que les risques pour les participants sont bien réels lorsqu'ils se réalisent. Historiquement, la recherche est marquée par de nombreux abus et les progrès de la médecine sont souvent plus lents et plus modestes qu'espérés. Des études récentes démontrent le taux de succès relatifs des essais cliniques et la nécessité de faire preuve d'humilité en lançant un projet.

Face à cette réalité, renoncer aux principes en faisant baisser le niveau d'exigences en termes de protection des participants et de qualité de la recherche semble contre-productif. La pandémie du COVID-19 a été un formidable laboratoire à ce propos. Les États, les chercheurs et l'industrie ont consenti des investissements considérables pour développer des traitements et des vaccins. Cela ne s'est pas fait au prix d'une diminution des exigences de rigueur scientifique, de sécurité des participants et de la population et de la qualité. Comme l'a rappelé l'Association suisse des CERs (*swissethics*) dans son communiqué du 6 mai 2020 : « *La pression actuellement exercée sur la recherche médicale ne doit pas conduire à de la recherche ou à une expérimentation de médicaments sur l'être humain sans respecter les normes éthiques et la législation en matière de recherche médicale. Une procédure accélérée ne peut être poursuivie au détriment de ces normes éthiques ou en dérogation à la loi*. »[101] Cette déclaration reprend celle de l'Association européenne des CERs (EUREC) : « *This recent mode in medical research also leads to a tremendous challenge for European Research Ethics Committees (RECs). RECs are aware that they must contribute accordingly.* […] *However, all this must be guided by the principle that RECs, even under these specific circumstances, will not compromise the quality of the review; an accelerated procedure cannot be at the expense of safety, notably that of the research participants. The recognized ethical principles of autonomy, beneficence, non-maleficence and justice must always be respected.* » (nos soulignés)[102]

[101] Swissethics, Communication du 06.05.2020 : La mission des commissions d'éthique pendant la pandémie COVID-19, disponible à : <https://swissethics.ch/fr/news/2020/05/06/die-einhaltung-ethischer-und-rechtlicher-standards-bei-den-ethikkommissionen-waehrend-der-covid-19-pandemie>.

[102] EUREC, Position of the European Network of Research Ethics Committees (EUREC) on the Responsibility of Research Ethics Committees during the COVID-19 Pandemic, 27 April 2020.

Le maintien d'un haut niveau de rigueur scientifique et de respect des principes de protection des participants n'a pas été un frein à la recherche. Même si des erreurs ont été commises et beaucoup de points doivent être améliorés, cet évènement dramatique de portée mondiale a mis en évidence la capacité des chercheurs d'apporter rapidement des réponses aux questions soulevées par la maladie et les stratégies pour y faire face. Les réussites n'ont pas été possibles au prix d'un renoncement aux principes, mais dans leur respect et grâce aux ressources importantes mises à disposition et une gouvernance renforcée. Les institutions de recherche se sont mieux organisées à l'interne et dans leur collaboration avec leurs partenaires académiques et industriels afin de se concentrer sur les enjeux scientifiques tout en protégeant les participants et la population.

Plutôt que de renoncer aux principes de l'éthique et du droit de la recherche impliquant des êtres humains sous prétexte de favoriser les chercheurs, ne serait-il pas plus pertinent de réfléchir à comment en améliorer l'efficacité ? La réponse passe par une amélioration de la gouvernance et le renforcement de la logique institutionnelle en complément de l'approche principalement individuelle des chercheurs. De nombreuses directives internationales ont été développées dans les dernières années prônant l'importance croissante des questions d'organisation dans la recherche[103]. Récemment le CIOMS a mis en consultation de nouvelles directives sur les pratiques de bonne gouvernance des institutions dont l'objectif est d'aider les institutions à donner aux chercheurs les moyens de respecter les plus hauts standards éthiques et scientifiques[104]. Un autre exemple est les directives de l'OMS sur les bonnes pratiques pour les essais cliniques mises en consultation en juillet 2023[105] suite à l'adoption par l'Assemblée mondiale de la santé d'une résolution relative au renforcement des essais cliniques pour fournir des preuves de haute qualité sur les interventions sanitaires et améliorer la qualité et la coordination de la recherche[106]. Au niveau national, nous pouvons mentionner les efforts des hôpitaux, en particulier universitaires, en faveur du consentement général pour la recherche ou encore le soutien apporté par l'initiative SPHN pour renforcer la collaboration entre les hôpitaux

103 Voir notamment la Déclaration de Taipei de l'AMM (adoptée en 2016) et les lignes directrices 11 et 12 des Lignes directrices de CIOMS d'éthique pour la recherche en matière de santé impliquant des participants humains (révisées en 2016).

104 CIOMS, International Guidelines on Good Governance Practice for Research Institutions, pour plus d'informations : <https://cioms.ch/working_groups/principles-of-good-governance-for-research-institutions/>.

105 WHO, Guidance for best practices for clinical trials, consultation publique disponible ici : <https://www.who.int/news-room/articles-detail/public-consultation-on-who-guidance-for-best-practices-for-clinical-trials>.

106 Resolution WHA 75.8 : Strengthening clinical trials to provide high-quality evidence on health interventions and to improve research quality and coordination, 27 May 2022.

et les Universités[107]. Dans le domaine des biobanques, *Swiss Biobanking Platform* met en réseau les biobanques de recherche en Suisse et développe des standards afin de soutenir ces infrastructures indispensables pour permettre aux chercheurs de progresser[108].

Défendre la recherche est une noble cause dans laquelle les CERs sont engagées au quotidien. Leur mission vise à garantir la protection des participants et de leur dignité tout en promouvant une recherche de qualité. Celle-ci n'est pas concevable sans la plus grande rigueur scientifique et la mise en œuvre de moyens importants en termes humains, matériels, techniques et technologiques. Le respect du cadre éthique et des droits humains contribue à maintenir un haut niveau d'attention de l'ensemble des intervenants en rappelant aux chercheurs leur privilège de pouvoir faire de la recherche avec des êtres humains. Toute tentative de faire baisser les standards sous prétexte d'accélérer les processus est en contradiction avec les enseignements de l'histoire et de la philosophie des sciences. Elle réduit le concept de progrès humain à celui de simple innovation technologique sans considération pour les droits et la dignité des personnes concernées et l'intérêt commun. Le jeu en vaut-il la chandelle ?

VIII. Bibliographie

A. Doctrine

Bruno BAERISWYL, Anonymisierung von genetischen Daten? (Datenschutz)rechtliche Aspekte der Anonymisierung bei Biobanken, Digma, 2008, p. 14 ss ; **Cherif BASSIOUNI** avec la collaboration de Thomas BAFFES et John T. EVRARD, Le contrôle de l'expérimentation sur l'homme. Travaux du Comité d'experts réunis à l'Institut supérieur de sciences criminelles. Syracuse, mai 1979 et 1980, Revue internationale de droit pénal, Vol. 51, 1980 (cité : BASSIOUNI) ; **Isabelle BOUTRON/Susan DUTTON/Philippe RAVAUD/Douglas G. ALTMAN**, Reporting and interpretation of randomized controlled trials with statistically nonsignificant results for primary outcomes, JAMA, Vol. 303, 2010, p. 2058 ss ; **Hélène BRUDERER**, La réutilisation des données personnelles liées à la santé à des fins de recherche scientifique. Étude de droit suisse avec des perspectives de droit comparé, thèse Genève, Zürich, 2023 ; **BSS VOLKSWIRTSCHAFTLICHE BERATUNG AG**, Befragung der Ethikkommissionen zur Anwendung von Art. 34 HFG: Schlussbericht, Bâle 2020 ; **Alvarez CIPRIANO *et al.***, Art. 1-352 und Art. 400-406 ZPO, Schweizerische Zivilprozessordnung ZPO: Band I: Art. 1-149 ZPO; Band II: Art. 150-352 ZPO und Art. 400-406 ZPO: Berner Kommentar, Berne 2012 (cité : BK ZPO-AUTEUR, art. X, N Y) ; **Deborah COHEN**, Cancer drugs: high price, uncertain value, British Medical Journal, Vol. 359, Published 04 October 2017 ; **Susanne DRIESSEN/Andri CHRISTEN/Pietro GERVASONI**, Humanforschung, Weiterverwendung und informierte

107 À ce propos, dans cet ouvrage ERARD, p. 1 ss. Voir aussi : <https://sphn.ch/>.

108 Pour plus d'informations : https://swissbiobanking.ch/. À propos de la gouvernance des biobanques, mentionnons aussi la thèse de doctorat en droit de Vladislava TALANOVA en cours de finalisation.

Einwilligung, Analyse zur Weiterverwendung von gesundheitsbezogenen Personendaten und biologischem Material sowie Anwendung von Artikel 34 HFG, Jusletter 1. Februar 2021 ; **Bernice Elger**, La protection de la personnalité et des données : l'anonymisation irréversible comme dilemme éthique. Les directives « Biobanques » de l'Académie Suisse des Sciences Médicales, Bulletin des médecins suisse, Vol. 86, N 45 2005, p. 2510 ss ; **Frédéric Erard**, Les données codées dans le contexte de la recherche : personnelles ou anonymes ? AJP/PJA 2021, p. 606 ss (cité : Erard, Données codées) ; **Padhraig S. Fleming/Despina Koletsi/John P.A. Ioannidis/Nikolaos Pandis**, High quality of the evidence for medical and other health-related interventions was uncommon in Cochrane systematic reviews, Journal of clinical epidemiology, Vol. 78, October 2016, p. 34 ss (cité : Fleming *et al.*) ; **Renée Claire Fox**, The Evolution of Medical Uncertainty, Milbank Memorial Fund Quarterly/ Health and Society, Vol. 58, No. 1, 1980, p. 1 ss ; **Jeffrey L Cummings/Travis Morstorf/ Kate Zhongm**, Alzheimer's disease drug-development pipeline: few candidates, frequent failures, Alzheimer's Research & Therapy, Vol. 6(4), 2014, p. 37 ss ; **Jeffrey Cummings/ Garam Lee/ Pouyan Nahed/Mina Esmail Zadeh Nojoo Kambar/Kate ZhonG/ Jorge Fonseca/Kazem Taghva**, Alzheimer's disease drug development pipeline: 2022, Alzheimer's & Dementia: Translational Research & Clinical Interventions, Vol. 8, Issue 1, e12295, 2022 ; **Melissa Gymsek/Amy L. McGuire/David Golan/Eran Halperin/ Yaniv Erlich**, Identifying personal genomes by surname inference, Science, Vol. 339, 18 January 2013, p. 321 ss (cité : Gymsek *et al.*) ; **Amanda Holpuch**, Family of Henrietta Lacks Settles With Biotech Company That Used Her Cells, The New York Time, August 1, 2023, disponible à : <https://www.nytimes.com/2023/08/01/science/henrietta-lacks-cells-lawsuit-settlement.html> ; **Homburger memorandum**, Swiss Legal Framework for De-identification of Health-Related Data, 2020 ; **Jeremy Howick/Despina Koletsi/John P.A. Ioannidis/Claire Madigan/Nikolaos Pandis/Martin Loef/Harald Walach/ Sebastian Sauer/Jos Kleijnen/Jadbinder Seehra/Tess Johnson/Stefan Schmidt**, Most healthcare interventions tested in Cochrane Reviews are not effective according to high quality evidence: a systematic review and meta-analysis, Journal of Clinical Epidemiology, Vol. 148, 2022, p. 160 ss (cité : Howich *et al.*) ; **Kathy L. Hudson/Francis S. Collins**, Family matters, Nature, Vol. 500, 2013, p. 141 ss ; **Alfred Jost**, Commentaire de l'arrêt du 4 juillet 2003 de la II^e^ Cour de droit public du Tribunal fédéral, Freiburger Ethik-Kommission International c. Bâle-Campagne (2A.450/2002), Revue suisse de droit de la santé RSDS/ SZG 1/2003, p. 13 ss ; **Henry Krum/Reuven J. Viskoper/Yves Lacourciere/Michael Budde/Vincent Charlon**, The effect of an endothelin-receptor antagonist, bosentan, on blood pressure in patients with essential hypertension, The New England journal of medicine, Vol. 338, 1998, p. 784 ss (cité : Krum *et al.*) ; **Samuel Mätzler**, Datenschutz in der (Human-)Forschung: Grundlagen und Probleme bei der Sekundärnutzung von Personendaten, in : Jusletter 30 janvier 2023 ; **Carol Levine**, Has AIDS Changed the Ethics of Human Subjects Research? Law, Medicine & Health Care, Vol. 16, Issue 3-4, 1988, p. 167 ss ; **Susan M. Reverby**, «Normal exposure» and inoculation syphilis: A PHS «Tuskegee» Doctor in Guatemala, 1946-1948, The Journal of Policy History, Vol. 23, N 1, 2011, p. 6 ss ; **Gesine Richter/Michael Krawczak/Wolfgang Lieb/Lena Wolff/Stefan Schreiber/ Alena Buyx**, Broad consent for health care-embedded biobanking: understanding and reasons to donate in a large patient sample, Genetics in Medicine, Vol. 20, 2018, p. 76 ss (cité : Richter *et al.*) ; **Walter M. Robinson/Brandon T. Unruh**, The Hepatitis Experiments at the Willowbrook State School, *in* Ezekiel J. Emanuel (ed.), The Oxford Textbook of Clinical Research Ethics, Oxford, 2008, p. 80 ss ; **David Rosenthal/Yvonne Jöhri**, Handkommentar zum Datenschutzgesetz, Zurich 2008 ; **Bernhard Rütsche**, Humanforschungsgesetz (HFG), Stämpflis Handkommentar (SHK), Bern 2015 (cité : SHK HFG-Auteur,

art. X, N Y) ; **Béatrice Schaad (éd.)**, (in)hospitalités hospitalières, Chêne-Bourg, 2023 ; **Charlie Schmidt**, Profile: Jean-Paul Clozel, Nature Biotechnology, Vol. 25, Issue 2, p. 155 ss ; **Rebecca Skloot**, The immortal life of Henrietta lacks, New York, 2010 ; **Dominique Sprumont**, Research Ethics Regulation: Rules versus Responsibility, *in* Ulf Schmidt/ Andreas Frewer/Dominique Sprumont (éds.), Ethical Research, The Declaration of Helsinki, and the Past, Present, and Future of Human Experimentation, New York 2020, p. 241 ss ; **Dominique Sprumont**, Droit suisse et progrès médical : vingt ans d'expérimentation, *in* Olivier Guillod (éd), Le droit de la santé en mouvement, Actes de la 20e Journée de droit de la santé, Neuchâtel : Université de Neuchâtel, Berne 2014, p. 159 ss (cité : Sprumont, Droit suisse et progrès médical) ; **Dominique Sprumont/Vladislava Talanova**, La recherche sans consentement : l'exceptionnelle exception, *in* Evelyne Clerc/ Jean-Philippe Dunand/ Dominique Sprumont (éd.), Alea jacta est : Santé ! Mélanges en l'honneur d'Olivier Guillod, Collection neuchâteloise, Bâle, 2021, p. 235 ss ; **Duxin Sun/Wei Gao/Hongxiang Hu/ Simon Zhou**, Why 90% of clinical drug development fails and how to improve it?, Acta Pharmaceutica Sinica B, Vol. 12, Issue 7, 2022, p. 3049 ss ; **Vladislava Talanova/ Franziska Sprecher**, Le consentement général : points à améliorer, Bulletin des Médecins Suisses, Vol. 101, No. 38, 2020, p. 1197 ss ; **Luigi Maria Terracciano/Luigi Tornillo/ Pierino Avoledo/Dietrich von Schweinitz/Thomas Kühne/Elisabeth Bruder** ; Fibrolamellar Hepatocellular Carcinoma Occurring 5 Years After Hepatocellular Adenoma in a 14-Year-Old Girl: A Case Report With Comparative Genomic Hybridization Analysis. *Arch Pathol Lab Med* 1 February 2004; 128 (2), p. 222–226 ; **Florent Thouvenin/Thomas Gächter/Kento Reutimann/Samuel Mätzler**, Datenschutz in der Humanforschung: ein Forschungsprivileg für die Sekundärnutzung von Personendaten, in: Jusletter 30 janvier 2023 ; **Benedikt van Spyk**, Das Recht auf Selbstbestimmung in der Humanforschung, Zurich/St-Gall 2011 ; **Dirk J. van Veldhuisen/Philip A. Poole-Wilson**, The underreporting of results and possible mechanisms of 'negative' drug trials in patients with chronic heart failure, International Journal of Cardiology, Vol. 80, 2001, p. 19 ss ; **Chi Heem Wong/ Kien Wei Siah/Andrew W Lo**, Estimation of clinical trial success rates and related parameters, Biostatistics, Vol. 20, Issue 2, April 2019, p. 273 ss.

B. Documents officiels

Conseil fédéral, Message sur la loi fédérale relative à la recherche sur l'être humain du 21 octobre 2009, FF 2009 7259 ss ; **Commission nationale d'éthique dans le domaine de la médecine humaine (CNE)**, Les biobanques destinées à la recherche, Prise de position no. 24/2015, Berne Décembre 2015 ; **Office fédéral de la santé publique (OFSP)**, Révision partielle des ordonnances d'exécution de la loi relative à la recherche sur l'être humain (LRH), Rapport explicatif, Berne, 26 avril 2023.

Le traitement de données personnelles à des fins statistiques

SAMAH POSSE*
Chargée d'enseignement, Faculté de droit et Faculté des sciences, Université de Neuchâtel
Chargée de cours, CAS Protection des données, UniDistance

Table des matières

I. Introduction

Les progrès technologiques sont la source d'importantes transformations tant sur les plans économique et scientifique qu'en matière de rapports sociaux. La numérisation de nos sociétés a généré un contexte dans lequel le traitement de données personnelles est omniprésent. À cet égard, la diversification, l'intensification et la mondialisation des traitements soulèvent de nouveaux enjeux[1] en matière de protection de données et des droits fondamentaux.

Dans ce contexte, la statistique en tant que science de la donnée, joue un rôle essentiel, non seulement en raison de son utilité, mais également par le volume des données traitées et l'étendue des domaines qu'elle couvre. Partant, les traitements de données à fin des statistiques méritent une attention particulière.

Les traitements de données dans un but statistique ont gagné en importance autant en ce qui concerne relevant du secteur public comme privé. Leur fonction est plurielle. Ils permettent par exemple aux entreprises d'évaluer, d'optimiser, de prévoir et/ou encore de personnaliser leurs services.

* L'auteure remercie vivement M^me^ Louise Tinguely pour sa précieuse contribution à la recherche bibliographique et pour sa relecture minutieuse.

1 Généralisation d'Internet, réseaux sociaux, *big data*, objets connectés, géolocalisation, intelligence artificielle générative, *etc*.

En matière d'économie numérique et de recherche, l'« intelligence » artificielle (IA) – si tant est qu'on puisse la considérer comme une intelligence (à proprement dite) – qui, par son essor a marqué ces dernières années en contribuant à une utilisation révolutionnaire des données[2], repose essentiellement sur des méthodes mathématiques[3] ; autrement dit des chiffres, des probabilités et surtout des statistiques.

Pour ce qui est du domaine étatique, la statistique fédérale permet notamment à la Confédération d'exercer ses compétences législatives et exécutives, d'évaluer les situations, les besoins et les progrès ou encore de planifier et diriger l'action politique[4]. De telles informations sont cruciales pour définir la politique de la Confédération dans des domaines d'importance nationale, tels que l'aménagement du territoire ou la politique monétaire de la Banque Nationale Suisse (BNS)[5].

En outre, la statistique assure une fonction majeure qui est celle de renseigner de manière objective la population, les cantons, les communes, les milieux scientifiques, les partenaires sociaux et l'économie privée (art. 1er let. b LSF[6] et 18 al. 1 LSF[7])[8]. À cet effet, l'Office fédéral de la statistique (OFS) met à disposition du public sur son site officiel, les données disponibles les plus récentes sur des thèmes aussi divers que la géographie de la Suisse, la population, l'emploi et le revenu, l'économie, les transports, la sécurité sociale, la formation et la science. La demande d'informations statistiques est en forte croissance et émane autant de l'État que des milieux économiques et de la

2 Progrès notamment dans les domaines du développement des médicaments, de la surveillance en temps réel des machines et des processus de production, de la cybersécurité ou encore de la recherche médicale (Voir Groupe de travail interdépartemental « Intelligence artificielle », Rapport « Défis de l'intelligence artificielle », p. 6).

3 Voir Groupe de travail interdépartemental « Intelligence artificielle », Défis de l'intelligence artificielle, p. 6 et 18.

4 Message Cst., FF 1997 I 1, p. 285 ; CR Cst-LARGEY, art. 65, N 8 et références citées ; voir ég. WALTER, p. 78 ss.

5 CR Cst-LARGEY, art. 65, N 8 et références et exemples cités : données relatives à l'utilisation du sol et le défrichement qui constitue une valeur importante pour déterminer la politique publique en matière de surfaces boisées ; indice suisse des prix à la consommation qui est un facteur important pour la mise en place de la politique monétaire de la Banque nationale suisse.

6 Loi fédérale du 9 octobre 1992 sur la statistique fédérale (LSF), RS 431.01.

7 Pour ce faire, l'art. 18 al. 1 LSF prévoit une obligation de publier les bases et les principaux résultats statistiques dans les langues officielles et sous une forme adaptée aux besoins des utilisateurs. En principe, les résultats non publiés doivent également être accessibles sous une forme appropriée.

8 Message LSF, FF 1992 I 353, p. 354 s. ; CR Cst-LARGEY, art. 65, N 4 et 8.

recherche[9]. Tant pour le secteur public que privé, elle requiert notamment une mise à disposition rapide et adéquate de données fiables[10].

Au niveau constitutionnel, l'intérêt à la statistique trouve son ancrage constitutionnel dans l'art. 65 Cst.[11] qui habilite la Confédération à collecter les données statistiques qui lui sont nécessaires pour accomplir ses tâches[12] (« compétence administrative ») (al. 1) et lui accorde la compétence facultative de légiférer sur l'harmonisation et la tenue des registres officiels (compétence législative) (al. 2)[13] ; le but étant de rationaliser l'activité de collecte des données en augmentant l'efficience des activités statistiques de la Confédération tout en réduisant leurs coûts[14].

Si l'intérêt public et privé aux traitements de données à des fins statistiques est certain, il doit être considéré à la lumière des impératifs liés aux droits fondamentaux, plus particulièrement au droit à l'autodétermination informationnelle consacré à l'art. 13 al. 2 Cst.[15] et à l'art. 8 CEDH garantissant le droit au respect à la vie privée.

Le droit à l'autodétermination informationnelle n'est pas absolu. À l'instar de tout droit fondamental, il peut être soumis à restriction aux conditions de l'art. 36 Cst.[16].

Par conséquent, tout l'enjeu est de garantir un juste équilibre entre les droits et les différents intérêts en présence.

Dans le cadre des traitements de données à des fins statistiques, il s'agit de mettre en balance la nécessité de la production des informations statistiques d'une part, et l'intérêt à la protection de la personnalité et des droits fondamentaux des personnes dont les données personnelles sont traitées (voir art. 1er LPD[17]), notamment lorsque des traitements automatisés de données sont utilisés, d'autre part[18]. En d'autres termes, il faut veiller à un juste équilibre entre les intérêts de la personne concernée et ceux du responsable du traitement ou de la société[19].

9 Message LSF, FF 1992 I 353, p. 354.
10 Message LSF, FF 1992 I 353, p. 354.
11 Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101.
12 Voir art. 65 al. 1 Cst. Les données statistiques concernées portent sur l'état et l'évolution de la population, de l'économie, de la société, de la formation, de la recherche, du territoire et de l'environnement en Suisse.
13 PC Cst-AUBERT/MAHON, art. 65, N 3 s. Il s'agit d'une compétence administrative et législative non globale, restreinte aux seuls domaines énumérés.
14 PC Cst-AUBERT/MAHON, art. 65, N 6.
15 Convention de sauvegarde des droits de l'homme et des libertés fondamentales, RS 0.101.
16 PC Cst-AUBERT/MAHON, art. 13, N 17.
17 Loi fédérale sur la protection des données (LPD) du 25 septembre 2020, RS 235.1.
18 Voir Recommandation nº R(97)18 du Comité des Ministres aux États membres.
19 Voir Rapport explicatif Convention 108+, N 48.

L'objectif de cette contribution est d'analyser à la lumière de la LPD révisée le cadre juridique applicable aux traitements de données personnelles réalisés dans un but statistique.

Sans prétendre à l'exhaustivité – compte tenu de l'étendue de la matière et de la multitude des réglementations cantonales –, nous nous limiterons au cadre juridique fédéral et tenterons d'en dégager les grandes lignes et les enjeux qui nous paraissent être les plus importants.

Il sied de souligner que sur le plan matériel, la statistique relève de la recherche scientifique au sens large, dont elle présente une branche spécifique[20]. En ce sens, les scientifiques utilisent fréquemment des méthodes statistiques dans le cadre de leurs activités de recherche[21].

Sur le plan juridique, la réglementation en matière de traitement de données à des fins statistiques, à l'instar de celle à des fins de recherche, relève du cadre juridique privilégié réservé aux traitements de données personnelles à des fins ne se rapportant pas à des personnes au sens des art. 31 al. 2 let. e et 39 LPD, s'inscrivant dans le cadre de la recherche scientifique au sens large (privilège de la recherche). Partant, les critères applicables aux traitements de données dans un but statistique se recoupent sur certains points avec ceux relatifs à la recherche scientifique, tout en se distinguant sur d'autres[22]. En effet, les critères de traitement de données à des fins non personnelles peuvent également être applicables à d'autres types de traitement, pour autant que leurs conditions soient remplies et sous réserve des dispositions spéciales pertinentes.

Pour appréhender la protection des données personnelles dans le cadre de traitements effectués dans un but statistique, il convient de se pencher, dans un premier temps, sur la notion de « traitement de données à des fins statistiques » (II) et rappeler brièvement le cadre juridique général applicable à la protection des données personnelles (III). Dans un second temps, nous présenterons la réglementation spécifique applicable aux traitements de données à des fins de statistiques. Une attention particulière sera portée à la protection des données dans le cadre de la statistique officielle fédérale et en particulier aux questions liées à l'appariement de données (IV). Enfin, nous terminerons par dégager quelques aspects qui, à notre sens, méritent un examen attentif de la part du, respectivement des responsables du traitement (V).

20 Voir à ce sujet, Beck'sche Kompalt-Kommentare DSGVO-Pauly, Art. 89, N 8.
21 Koç, N 30.3 ; Beck'sche Kompalt-Kommentare DSGVO-Pauly, Art. 89, N 8.
22 Koç, N 30.3 ; Beck'sche Kompalt-Kommentare DSGVO-Pauly, Art. 89, N 8.

II. Notion de traitement de données à des fins statistiques

La notion de traitement de données personnelles à des fins statistiques au sens de la LPD implique en règle générale trois éléments : l'existence d'un traitement (A) portant sur des données personnelles (B), lequel est effectué dans un but statistique (C).

Tant la notion de « *traitement* » que celle de « *données personnelles* » en vertu de la LPD doivent être interprétées au sens large du terme[23]. Cette souplesse du point de vue terminologique nous paraît nécessaire compte tenu des défis soulevés par l'évolution fulgurante des technologies. Une telle approche serait plus à même d'appréhender les éventuelles futures situations inédites qui pourraient en résulter[24].

Les notions de « *traitement* » et de « *données personnelles* » telles que définies par la LPD, rejoignent en substance celles de « *traitement* » et de « *donnée à caractère personnel* » prévues par la Convention 108+ et le RGPD[25].

A. Traitement de données

Est considéré comme traitement au sens de la LPD « *toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés* » (art. 5 let. d LPD)[26].

Outre la collecte qui en constitue la première étape, la notion de traitement de données se réfère, en règle générale, aux opérations telles que, « *l'enregistrement,*

---

23 Voir Message aLPD, FF 1988 II 421, p. 455 ; MÉTILLE, Traitement de données, p. 4 et 6 ; CR LPD-MEIER/TSCHUMY, art. 5, N 19 et 74 ; DE TERWANGNE, La nouvelle loi suisse de protection de données dans le contexte international (Convention 108+ et RGPD), p. 57 ; ROSENTHAL/JÖHRI, art. 3 N 2 ; DI TRIA/LUBISHTANI, p. 32 et références citées ; CJUE, arrêt C-434/16 du 20 décembre 2017, *Nowak*, § 34 s. ; TUE, arrêt du 26 avril 2023, *affaire T-557/20 (CRU/CEPD)* ; JOTTERAND, Des données personnelles pseudonymisées transférées à un tiers deviennent-elles anonymes ?

24 Voir également les considérations de COTTIER, p. 30 ss.

25 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). Voir art. 2 let. a Convention 108+ et art. 4 par. 2 RGPD.

26 Voir également Rapport explicatif Convention 108+, N 21 ; Annexe à la Recommandation N° R(97)18 du Comité des Ministres aux États membres, N 1.

la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction[27] *de données* » (voir art. 5 let. d LPD)[28].

En matière de statistique, le traitement de données se rapporte à des opérations plus spécifiques telles que l'adaptation, l'extraction, la consultation, la mise à disposition, l'appariement ou l'interconnexion, la pseudonymisation et l'anonymisation[29] ainsi que la suppression ou l'application d'opérations logiques et/ou arithmétiques à ces données[30].

Bien que la communication de données tombe sous le coup de la notion de « *traitement* » dont elle constitue une forme spécifique, le législateur a tenu à en souligner le caractère particulièrement délicat de l'opération en lui consacrant plusieurs dispositions spécifiques (voir art. 5 let. e et 36 LPD). En effet, la communication de données personnelles exige une attention particulière en ce sens que « *le fait de transmettre des données personnelles ou de les rendre accessibles* » (art. 5 let. e LPD) à des tiers, et ce « *quels que soient les moyens ou les supports utilisés* »[31] génère un certain risque de perte de contrôle sur les données en question[32].

B. Données personnelles

La notion de « *données personnelles* » est définie comme étant « *toutes les informations concernant une personne physique identifiée ou identifiable* » (art. 5 let. b LPD).

À noter que les données des personnes morales ne constituent plus des données personnelles au sens de la LPD révisée (voir art. 2 al. 1 LPD)[33].

---

27 La notion de destruction va plus loin que celle d'effacement car elle requière une élimination irréversible des données. Si lorsque les données reposent sur un support papier, il suffit de brûler ou déchiqueter le document en question, l'opération est plus complexe lorsqu'il s'agit de support informatique (Voir Message LPD 2017, FF 2017 6565, p. 6641 ; CR LPD-MEIER/TSCHUMY, art. 5, N 75).

28 À noter que la liste des opérations entrant en ligne de compte énoncée par la LPD (*cf*. art. 5 let. d LPD) est exemplative et non exhaustive (*cf*. Message LPD 2017, FF 2017 6565, p. 6641).

29 L'anonymisation et la pseudonymisation constituent des opérations relatives à des données personnelles au sens de l'art. 5 let. d LPD dont le résultat est anonyme ou pseudonymisé.

30 *Cf*. art. 2 let. a Convention 108+ et art. 4 par. 2 RGPD ; Annexe à la Recommandation nº R(97)18 du Comité des Ministres aux États membres, N 1. Voir ég. au sujet de la notion de traitement de données, CR LPD-MEIER/TSCHUMY, art. 5, N 1.

31 Voir Annexe à la Recommandation nº R(97)18 du Comité des Ministres aux États membres, N 1.

32 Voir CR LPD-EPINEY, art. 36, N 1.

33 Voir *infra* III.A.1.

Une personne est identifiée lorsque son identité est donnée[34]. Outre l'identité civile ou juridique, le terme « *identifiable* » se rapporte « *à tout élément susceptible d'‹ individualiser ›* » directement ou indirectement « *ou de distinguer (et donc de traiter différemment) une personne [physique] parmi d'autres* »[35].

La notion de données personnelles ne se limite donc pas uniquement aux informations sensibles ou d'ordre intime ou privé. Elle peut concerner toute sorte information, tant objective que subjective – sous forme d'avis ou appréciations – du moment où elle, son contenu, sa finalité ou son effet est lié à une personne[36].

Il peut s'agir notamment d'une référence à un identifiant, tel qu'un nom, un pseudonyme, un numéro d'identification, des données de localisation, un identifiant en ligne, d'une adresse IP[37], de témoins de connexion (« *cookies* ») ou d'un autre identifiant, qui renvoient à une personne donnée ou à un appareil ou un ensemble d'appareils (p. ex. : ordinateur, téléphone portable, appareil photo, console de jeux, *etc*.)[38].

Il peut en outre s'agir de données biométriques ou génétiques ou d'un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (voir art. 4 par. 1 et consid. 30 RGPD)[39].

34 Voir MÉTILLE, Traitement de données, p. 4 ; DI TRIA/LUBISHTANI, p. 33.

35 Rapport explicatif Convention 108+, N 18 ; voir art. 4 par. 1 RGPD.

36 Voir CJUE, arrêt C-434/16 du 20 décembre 2017, *Nowak*, § 34 s. ; TUE, arrêt du 26 avril 2023, *affaire T-557/20 (CRU/CEPD)* ; JOTTERAND, Des données personnelles pseudonymisées transférées à un tiers deviennent-elles anonymes ?

37 Voir ATF 138 II 346, JdT 2013 I 71 ; Rapport explicatif Convention 108+, N 18 ; Voir ég. consid. 30 et art. 4 par. 1 RGPD. Pour une analyse approfondie de la notion de donnée personnelle, CR LPD-MEIER/TSCHUMY, art. 5, N 20 ss et les références citées ; MÉTILLE, Traitement de données, p. 4 ; DI TRIA/LUBISHTANI, p. 34 et références citées.

38 Rapport explicatif Convention 108+, N 18 ; Voir ég. consid. 30 et art. 4 par. 1 RGPD. Pour une analyse approfondie de la notion de donnée personnelle, Voir CR LPD-MEIER/TSCHUMY, art. 5, N 20 ss et les références citées.

39 Rapport explicatif Convention 108+, N 18 ; Voir ég. consid. 30 et art. 4 par. 1 RGPD. Pour une analyse approfondie de la notion de donnée personnelle, voir CR LPD-MEIER/TSCHUMY, art. 5, N 20 ss et les références citées.

Contrairement au RGPD, la LPD ne propose pas de définition des notions de données biométriques[40] ou génétiques[41].

La notion de donnée personnelle est un élément cardinal dans le système de la réglementation en matière de protection de données de la LPD dans la mesure où elle en délimite le champ d'application matériel[42]. En effet, à l'instar de la Convention 108+ et du RGPD, la LPD n'est pas applicable aux données anonymes ou du moins, considérées en tant que telles[43].

Bien qu'en matière de statistique, le traitement ne vise pas spécifiquement ou exclusivement des données personnelles, ces dernières constituent une part importante des données traitées.

Par ailleurs, même si les deux peuvent se recouper, la notion de « *données d'identification* » est à distinguer de celle de données personnelles. En effet, les données d'identification représentent les données personnelles qui permettent l'identification directe de la personne concernée et qui sont nécessaires à la collecte, au contrôle et à l'appariement des données, mais qui ne sont pas utilisées par la suite pour établir des résultats statistiques[44].

C. « À des fins statistiques »

Le terme « *à des fins statistiques* » se réfère ici et détermine la finalité du traitement, de sorte qu'il doit être apprécié conformément à la notion de statistique.

---

40 Voir art. 4 par. 14 RGPD, « *‹ données biométriques ›, les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques* ».

41 Voir art. 4 par. 13 RGPD, « *‹ les données génétiques › les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question* ».

42 Voir art. 2 et 5 let. a LPD, consid. 26 et art. 2 et 5 par. 1 RGPD, art. 1er, 2 let. a et 3 Convention 108+) ; CR LPD-MEIER/TSCHUMY, art. 5, N 18.

43 Voir art. 1er et 5 let. b LPD ; art. 1er Convention 108+ ; art. 1er et consid. 26 RGPD ; Message LPD 2017, FF 2017 6565, p. 6640. En d'autres termes, la LPD ne couvre pas les informations ne concernant pas une personne physique identifiée ou identifiable, ni les données personnelles rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable (voir *infra* IV.A.2.b).

44 Annexe à la Recommandation No R(97)18 du Comité des Ministres aux États membres, N 1.

La statistique peut être définie comme une science des méthodes, d'application universelle[45] visant à analyser et à caractériser des phénomènes collectifs ou de masse dans une population donnée[46]. Elle englobe autant les méthodes et procédés utilisés pour obtenir, traiter, analyser et représenter des données que pour en tirer des affirmations, des déductions ou en faire la base de décisions que les résultats (provisoires ou définitifs) de ce processus, sous forme d'informations chiffrées plus ou moins condensées sur la réalité[47].

Par conséquent, les traitements de données personnelles effectués en vue d'obtenir « les informations quantitatives et qualitatives, agrégées et représentatives, caractérisant un phénomène collectif au sein d'une population considérée » (art. 3 par. 1 Règlement [CE] 223/2009[48]) constituent des traitements de données à des fins de statistiques.

Le but statistique se rapporte ainsi aux enquêtes statistiques ou à la production de résultats statistiques agrégés[49]. En ce sens, il couvre toutes opérations « *de collecte et de traitement de données à caractère personnel* [données personnelles] *nécessaires aux enquêtes statistiques ou à la production de résultats statistiques* »[50].

Par « *résultats statistiques* », il faut entendre « *une information obtenue par le traitement de données à caractère personnel en vue de caractériser un phénomène collectif dans une population considérée* »[51]. À titre d'exemple, en matière de mobilité et de transport, l'OFS met à disposition des résultats statistiques concernant les nouvelles mises en circulation de véhicules routiers en juillet 2023[52]. Ces résultats se présentent sous forme de tableau Excel et ne contiennent pas d'informations sur les personnes.

« *Les fins statistiques impliquent que le résultat du traitement à des fins statistiques ne constitue pas des données à caractère personnel mais des données agrégées, et que ce résultat ou ces données à caractère personnel ne sont pas utilisés à l'appui de mesures ou de décisions concernant une personne physique*

45 Message LSF, FF 1992 I 353, p. 355 ; CR Cst-Largey, art. 65, N 8.
46 Rapport explicatif Convention 108+, N 50 ; Voir Recommandation nº R(97)18 du Comité des Ministres aux États membres.
47 Message LSF, FF 1992 I 353, p. 355; CR Cst-Largey, art. 65, N 4.
48 Règlement (CE) 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes, JO L 87 du 31 mars 2009, p. 164 ss.
49 Rapport explicatif Convention 108+, N 50 ; voir ég. à ce sujet Beck'sche Kompalt-Kommentare DSGVO-Pauly, Art. 89, N 8.
50 Annexe à la Recommandation nº R(97)18 du Comité des Ministres aux États membres, p. 3 ; consid. 162 RGPD ; voir ég. à ce sujet Beck'sche Kompalt-Kommentare DSGVO-Pauly, Art. 89, N 8.
51 Annexe à la Recommandation nº R(97)18 du Comité des Ministres aux États membres, p. 2.
52 <https://www.bfs.admin.ch/bfs/fr/home/actualites/quoi-de-neuf.gnpdetail.2023-0123.html>.

en particulier »[53]. En règle générale, les résultats statistiques agrégés peuvent être utilisés à différentes fins, notamment des fins de recherche scientifique[54].

En principe, selon le consid. 162 du RGPD « *les données* [personnelles] *collectées et traitées à des fins statistiques doivent servir uniquement à ces fins. Elles ne doivent pas être utilisées pour prendre une décision ou mesure relative à la personne concernée ou pour compléter ou corriger des fichiers dont les données à caractère personnel sont traitées pour des finalités non statistiques* »[55].

Cette définition restrictive des traitements ultérieurs de données à des fins statistiques n'englobe pas les traitements à des fins de ciblage marketing ou de profilage[56].

En pratique, lorsqu'un responsable de traitement procède à un traitement de données à des fins de statistiques et qu'il souhaite également effectuer un traitement de données à d'autres finalités – par exemple afin d'établir des profils de ses clients pour mieux les cibler – il doit distinguer entre le traitement à des fins statistiques et les traitements à d'autres finalités. Chaque traitement doit respecter les principes généraux (art. 6 et 8 LPD) ainsi que les prescriptions correspondantes (voir art. 30 et 31 LPD en ce qui concerne les traitements de données par des personnes privées et les art. 33 ss LPD en ce qui concerne autres types de traitement).

Toutefois le traitement à des fins statistiques de données personnelles collectées à d'autres finalités peut être considéré compatible avec la/les finalité(s) pour lesquelles les données ont été initialement collectées, pour autant qu'elles soient accompagnées de garanties appropriées[57] (voir art. 30 al. 2 let. e et 39 LPD) (voir *infra* IV).

III. Cadre juridique général – Protection des données

Les données statistiques relèvent, d'une part du cadre juridique général applicable en matière de protection des données personnelles, et d'autre part, de la réglementation spécifique régissant la statistique.

---

53 Consid. 162 RGPD.

54 Voir Consid. 162 RGPD ; Beck'sche Kompalt-Kommentare DSGVO-PAULY, Art. 89, N 8.

55 Annexe à la Recommandation n° R(97)18 du Comité des Ministres aux États membres, p. 3.

56 TAMBOU, p. 127.

57 Annexe à la Recommandation N° R(97)18 du Comité des Ministres aux États membres, pt. 4.

Le cadre général est en principe applicable à chaque fois que des informations sur des personnes physiques – étant donnée l'exclusion des données personnelles des personnes morales du champ d'application de la nouvelle LPD (voir art. 1er LPD)[58] – sont collectées et/ou traitées et ce, à quelque fin que ce soit, c'est-à-dire administrative, commerciale, de recherche, statistique ou autre. En Suisse, cette réglementation trouve ses sources dans le droit international, dans le droit national, et dans une certaine mesure, dans le droit européen. Nous nous limiterons ici au cadre juridique national.

A. Sources nationales

1. Au niveau fédéral

Comme déjà relevé (voir *supra* I), le droit de la protection des données tire ses sources de l'art. 13 al. 2 Cst. consacrant le droit à l'autodétermination informationnelle ainsi que de l'art. 8 CEDH garantissant le respect au droit à la vie privée. Comme tout droit fondamental, le droit à l'autodétermination informationnelle n'est pas absolu et peut être soumis à restriction aux conditions de l'art. 36 Cst.[59].

Sur le plan fédéral, le droit à l'autodétermination informationnelle est mis en œuvre par la loi fédérale sur la protection des données qui constitue une loi-cadre, concrétisant à la fois la protection de la personnalité et les droits fondamentaux (voir art. 1er et 5 let. a LPD)[60] et son ordonnance d'application (ODPo).

Le dispositif est complété par les différentes dispositions spécifiques en matière de protection des données prévues dans d'autres instruments[61].

De nature transversale, la LPD régit aussi bien les traitements de données personnelles réalisés par les personnes privées que par les organes fédéraux (art. 2 al. 1 let. b LPD). Par conséquent, elle énonce des normes relevant pour certaines du droit privé, régissant les rapports entre particuliers, et des normes de droit public, applicables aux organes fédéraux[62].

58 Voir *infra* III.A.1.
59 PC Cst-AUBERT/MAHON, art. 13, N 17.
60 Voir MÉTILLE, Traitement de données, p. 6.
61 Voir par ex. art. 179 ss CP, art. 269 ss CPP, Loi sur les profils d'ADN, art. 14 ss LBN, art. 44*a* LPGA ; art. 101 LEI, art. 44 al. 1 et 46 al. 1 LRens, art. 44 LN, art. 96 al. 1 et 99 al. 6 LAsi, art. 10 al. 1 Loi fédérale sur la Commission de prévention de la torture, *etc.*
62 CR LPD-EPINEY/SUMBO, N 1.

Il sied de relever que, la Loi révisée exclut désormais de son champ d'application les données des personnes morales, lesquelles demeurent, pour l'essentiel, protégées par les art. 28 ss CC[63] et les autres instruments sectoriels pertinents[64].

Du fait de ces changements, les dispositions du droit fédéral qui donnent aux organes fédéraux le pouvoir de traiter et de communiquer des données personnelles ne seront plus applicables au traitement et à la communication de données de personnes morales[65]. Toutefois, en application du principe de légalité consacré à l'art. 5 al. 1 Cst., toute action de l'État (y compris le traitement ou la communication de données) doit reposer sur une base légale (voir les art. 13 al. 2 et 36 Cst.). Pour répondre à cette exigence le législateur a introduit dans la LOGA un ensemble de dispositions régissant le traitement de données de personnes morales par les organes fédéraux[66].

Pour ce qui est du domaine de la statistique officielle fédérale, par exemple, les dispositions pertinentes ont été modifiées afin de garantir un niveau de protection équivalent pour les personnes physiques et morales[67]. Certains termes sont également adaptés à la nouvelle terminologie de la LPD (*infra* IV.B)[68].

2. Au niveau cantonal

En règle générale, les traitements de données effectués par des organes publics cantonaux ou communaux, tels les universités[69] – et les hôpitaux cantonaux et universitaires, régionaux et communaux sont régis par les législations cantonales en matière de protection de données. Pour l'essentiel, les réglementations cantonales s'inscrivent dans la même logique que celle de la LPD.

63 MÉTILLE, Traitement de données, p. 4.
64 Voir Message LPD 2017, FF 2017 6565, p. 6595.
65 Voir Message LPD 2017, FF 2017 6565, p. 6722.
66 Voir Message LPD 2017, FF 2017 6565, p. 6722 ss.
67 Message LPD 2017, FF 2017 6565, p. 6746.
68 Message LPD 2017, FF 2017 6565, p. 6746.
69 À noter que les Écoles polytechniques fédérales (EPF) ne relèvent pas du droit cantonal, voir art. 36*c* Loi fédérale du 4 octobre 1991 sur les Écoles polytechniques fédérales, RS 414.110.

B. Principes généraux de la protection des données

À l'instar de tout traitement de données, les traitements à des fins de statistiques sont soumis au respect des principes généraux de la protection des données. Pour rappel, il s'agit du :

– principe de licéité (art. 6 al. 1 LPD) ;
– principe de la bonne foi (art. 6 al. 2 LPD, voir ég. art. 5 al. 3 et 9 Cst.) ;
– principe de proportionnalité (art. 5 al. 2 LPD, voir ég. art. 36 al. 3 Cst.) ;
– principe de transparence ou reconnaissabilité (art. 6 al. 3 LPD) ;
– principe de finalité (art. 6 al. 3 LPD) ;
– principe d'exactitude (art. 6 al. 5 LPD) ;
– et du principe de sécurité (art. 8 LPD).

Il sied de souligner que la LPD prévoit des critères plus restrictifs pour les traitements de données par des organes fédéraux. En effet, en sus des exigences liées à la licéité, le traitement de données personnelles par des organes fédéraux est soumis au principe de la légalité (voir art. 34 al. 1 LPD ; *infra* III.C.2)[70]. Partant, il ne suffit pas que le traitement respecte les exigences de licéité telles que développées *infra*, mais encore faut-il qu'il soit expressément prévu dans une loi au sens formel ou matériel[71].

En matière de traitement de données à des fins de statistiques, les principes de transparence, de finalité, de proportionnalité et de sécurité méritent une attention particulière.

La finalité et la reconnaissabilité constituent des principes juridiques spécifiques à la protection des données[72]. Ils s'inscrivent tous deux dans le prolongement du principe de la bonne foi et de la transparence. Ils présentent par ailleurs un lien étroit avec le principe de la proportionnalité ; le caractère proportionné du traitement s'appréciant quant au but visé par le traitement[73].

Selon la lettre de l'art. 6 al. 3 LPD, « [l]*es données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée et doivent être traitées ultérieurement de manière compatible*

70 Pour plus de détails, voir CR LPD-Epiney/Posse, art. 34, N 1 ss.
71 Voir CR LPD-Epiney/Posse, art. 34, N 3.
72 Voir concernant le principe de la finalité, CR LPD-Meier/Tschumy, art. 6, N 47 et références citées. Au niveau de l'UE et du Conseil de l'Europe, voir art. 5 par. 4 let. b Convention 108+, art. 5 par. 1 let. b RGPD et art. 4 par. 1 let. b Directive 2016/680.
73 Voir CR LPD-Meier/Tschumy, art. 6, N 47 et références citées ; Métille, Traitement de données, p. 10.

avec ces finalités ». En dépit de cette formulation peu précise, la reconnaissabilité doit être comprise comme une exigence portant autant sur la collecte des données, que les finalités du traitement[74].

En règle générale, la transparence est réputée remplie lorsque la personne concernée a été dûment informée, lorsque le traitement est prévu par la loi ou lorsqu'il ressort clairement des circonstances du cas d'espèce[75].

Conformément au principe de finalité, les données ne peuvent être traitées à des fins indéterminées[76]. Non seulement, la personne concernée ne doit pas être prise au dépourvu par la façon dont ses données sont traitées ou combinées[77], mais de plus, les données qui ne sont plus nécessaires au regard des finalités du traitement doivent être détruites ou anonymisées en application du principe de la durée de la conservation des données (art. 6 al. 4 LPD) comme mentionné (voir *supra* III.B).

Cette obligation est à apprécier compte tenu de l'ensemble des circonstances et du cycle de vie des données[78]. En effet, dans certains cas, la conservation des données présente encore un intérêt administratif pour le responsable du traitement, pour des questions de traçabilité ou en raison d'une obligation légale[79] ou encore lorsqu'elles doivent faire l'objet d'un archivage (voir LAr[80]).

En règle générale, le principe de la finalité implique la détermination et l'immuabilité du but du traitement[81]. La compatibilité ultérieure peut toutefois être admise « *lorsque la modification du but initial est prévue par la loi, requise par un changement législatif ou légitimée par un autre motif justificatif* »[82]. Nous verrons qu'à cet égard, la LPD institue, à certaines conditions, une dérogation au principe de la finalité en faveur de la statistique, dans le cadre des traitements ne se rapportant pas aux personnes (voir *infra* IV.).

La reconnaissabilité de la collecte et des finalités doit être examinée en tenant compte de toutes les circonstances concrètes du cas d'espèce et à la lumière des

74 Message LPD 2017, FF 2017 6565, p. 6568 ; MÉTILLE, Traitement de données, p. 11 ; ROSENTHAL, N 37.
75 Message LPD 2017, FF 2017 6565, p. 6644 ; MÉTILLE, Traitement de données, p. 11.
76 TAMBOU, p. 123.
77 TAMBOU, p. 123.
78 CNIL, Guide pratique, Les durées de conservation.
79 CNIL, Guide pratique, Les durées de conservation.
80 Loi fédérale du 26 juin 1998 sur l'archivage (LAr), RS 152.1.
81 Pour une analyse plus approfondie, voir CR LPD-MEIER/TSCHUMY, art. 6, N 47 ss. Voir également TAMBOU, p. 124.
82 Message LPD 2017, FF 2017 6565, p. 6646 ; MÉTILLE, Traitement de données, p. 10 ; ROSENTHAL, N 36 ; Préambule Convention 108+. Concernant la compatibilité ultérieure avec la finalité originelle, voir TAMBOU, p. 124 ss.

principes de la bonne foi et de la proportionnalité[83]. Lorsque le traitement répond à plusieurs finalités, chaque finalité doit être indiquée de manière précise et claire[84].

Il convient de souligner que l'utilisation multiple de données, y compris dans le cadre de la statistique présente un risque accru de violation du principe de la finalité. De ce fait, elle exige une distinction claire entre les traitements de données à des fins statistiques et les autres et requiert la mise en place de mesures organisationnelles et techniques appropriées (voir *supra* III.B)[85].

En vertu de l'art. 6 al. 2 LPD, tout traitement doit être conforme au principe de la proportionnalité, autrement dit être apte, nécessaire et s'inscrire dans un rapport de proportionnalité au sens strict avec le but visé[86].

Si le principe de la proportionnalité joue un rôle central dans le système juridique suisse dans son ensemble[87], son importance se trouve accentuée en matière de protection des données du fait de sa réglementation articulée pour l'essentiel autour de principes généraux du droit (art. 6 et 8 LPD)[88]. À cet égard, il sied de rappeler que l'existence d'une base légale, du consentement de la personne concernée ou d'un intérêt public ou privé, ne suffit, en principe, pas à lui seul, à justifier un traitement de données qui porte atteinte aux droits de la personne concernée. Encore faut-il que l'intérêt audit traitement résiste à l'examen de la proportionnalité. En d'autres termes, l'intérêt du responsable du traitement doit être mis en balance avec celui de la personne concernée et, le cas échéant, en tenant compte d'éventuels autres intérêts publics ou privés.

---

83 CR LPD-Meier/Tschumy, art. 6, N 30 ; Message Révision aLPD, FF 2003 1915, p. 1937 ; Baeriswyl/Pärli, Handkomm. DSG-Baeriswyl, art. 4, N 49 ; Epiney/Nüesch, N 3.89 ; BSK DSG/BGÖ-Maurer-Lambrou/Steiner, art. 4, N 16a ; Belser/Epiney/Waldmann-Epiney, § 9, N 39 s.

84 Tambou, p. 123.

85 Voir PFPDT, 30e Rapport d'activités 2022/23, p. 15 et 29e Rapport d'activités, p. 14 concernant le projet pilote *SpiGes* du programme *NaDB* mené sous la direction de l'OFS, dont le but est d'employer la plateforme d'interopérabilité de l'OFS pour recueillir une seule fois les données relatives aux séjours stationnaires en hôpital (principe de la collecte unique des données) afin de pouvoir ensuite les utiliser à des fins aussi bien administratives que statistiques.

86 ATF 147 I 346, c. 5.5, JdT 2021 I 215 ; ATF 138 II 346, c. 9.2 ss, JdT 2013 I 71 (*Google Street View*) ; ATF 133 I 77, c. 5, JdT 2008 I 418 ; ATF 130 II 425, c. 5.2 ss ; Message LPD 2017, FF 2017 6565, p. 6644 ; CR LPD-Meier/Tschumy, art. 6, N 28 ; CR Cst-Dubey, art. 5, N 97 ss ; Métille, Traitement de données, p. 9 ; Rosenthal, N 34 ; Belser/Epiney/Waldmann-Epiney, § 9, N 24.

87 Voir CR Cst-Dubey, art. 5, N 12 s. et N 91 ss ; CR LPD-Meier/Tschumy, art. 6, N 26 et 30.

88 Quant au caractère fondamental de ce principe en matière de protection des données, voir ég., art. 5 par. 4 let. c Convention 108+, art. 5 par. 1 let. c RGPD (minimisation des données) et art. 4 par. 1 let. c Directive 2016/680.

Le principe de proportionnalité implique, en règle générale, une proportionnalité de principe, une proportionnalité matérielle et une proportionnalité temporelle[89].

En matière de protection de données, le respect du principe de proportionnalité incombe tant aux responsables de traitement privés qu'aux organes publics[90]. Partant, l'aptitude, la nécessité et le caractère adéquat d'une mesure sont à apprécier compte tenu de l'ensemble des circonstances du cas d'espèce[91]. Ces critères sont à respecter non seulement en ce qui concerne la nature et les catégories de données traitées mais également pour ce qui est du type, du mode et des moyens de traitements et de la finalité et durée de la conservation des données[92].

En ce sens, les principes de minimisation et d'évitement des données constituent des expressions du principe de la proportionnalité[93].

Le principe de la durée de conservation, dorénavant codifié à l'art. 6 al. 4 LPD, commande l'anonymisation ou bien la destruction des données dès qu'elles ne sont plus nécessaires au regard des finalités du traitement (voir *infra* III.C.5)[94]. L'ajout exprès de cette exigence qui relève, en soi de la proportionnalité temporelle parmi les principes généraux régissant la protection des données, souligne les enjeux liés à la durée de conservation des données occasionnés par les évolutions technologiques et les capacités gigantesques de stockage[95]. Le principe de la durée de conservation implique par conséquent une obligation de fixer un délai de traitement[96] dont la durée ne doit pas être excessive par rapport aux finalités du traitement[97].

---

89 CR LPD-MEIER/TSCHUMY, art. 6, N 30 et références citées.

90 Voir notamment, Message aLPD, FF 1988 II 421, p. 458 ; ATF 138 II 346, c. 9.2, JdT 2013 I 71 ; EPINEY/NÜESCH, N 3.75 ; CR LPD-MEIER/TSCHUMY, art. 6, N 26 ; BELSER/EPINEY/WALDMANN-EPINEY, § 9, N 23.

91 CR Cst-DUBEY, art. 5, N 92 s. et références citées.

92 MÉTILLE, Traitement de données, p. 9 ; MEIER, N 665.

93 MÉTILLE, Traitement de données, p. 9 ; ROSENTHAL, N 34. Concernant les principes d'évitement et de minimisation des données, voir Message LPD 2017, FF 2017 6565, p. 6644 et 6646.

94 Art. 5 par. 4 let. e Convention 108+ ; art. 4, par. 1, let. e Directive (UE) 2016/680 et art. 5 par. 1 let. e RGPD. Voir Message LPD 2017, FF 2017 6565, p. 6646.

95 Message LPD 2017, FF 2017 6565, p. 6645 ; voir ég. MÉTILLE, Traitement de données, p. 9.

96 Voir Message LPD 2017, FF 2017 6565, p. 6646 ; MÉTILLE, Traitement de données, p. 9 ; CR LPD-MEIER/TSCHUMY, art. 6, N 36.

97 Voir CourEDH, *Drelon c. France*, arrêt du 8 septembre 2022, nº 31353/16 et 27758/18, § 82 & 96 ss. Dans le cas d'espèce, la CourEDH a conclu à la violation du principe de la « *limitation de la durée de la conservation des données – minimisation des données* »

À cet égard, la concrétisation du principe de la durée de conservation dans la réglementation spécifique en matière de statistique officielle fédérale nous paraît discutable (voir *infra* IV.B.2).

En vertu du principe de la minimisation des données, seules les données absolument nécessaires au but poursuivi doivent être traitées[98].

Le principe d'évitement, quant à lui, suppose que si « *le but du traitement peut être atteint sans collecte de données nouvelles, cette option doit être privilégiée* »[99].

Dans le cadre des traitements à des fins statistiques, la collecte et le traitement de données personnelles doivent, en règle générale, être limités aux seules données nécessaires aux finalités statistiques poursuivies[100]. « *En particulier, les données d'identification ne doivent être collectées et traitées que si cela est nécessaire* »[101].

Enfin, dans un contexte numérique en pleine évolution, notamment marqué tant par l'augmentation du volume de données traitées que par la récurrence des traitements et la fréquence des cyberattaques contre des systèmes d'informations sensibles[102], le principe de la sécurité constitue la pierre angulaire de la protection des données personnelles. En effet, il représente à la fois un principe juridique fondamental ainsi qu'une préoccupation et un élément technique majeurs de la protection des données[103].

Inscrit à l'art. 8 LPD, le principe de la sécurité fonde l'obligation pour le responsable du traitement et le sous-traitant d'assurer une sécurité adéquate des données personnelles par la mise en place de mesures organisationnelles et

en raison du caractère excessif de la durée de conservation des données personnelles relatives aux résultats des procédures de sélection des candidats au don du sang, dans la mesure où à l'époque des faits (en 2004), l'outil informatique utilisé par l'établissement pour leur traitement prévoyait leur collecte et leur conservation jusqu'en 2278, ce qui a en l'occurrence donné lieu à leur utilisation répétée, de manière à exclure automatiquement un candidat au don de sang, et ce près de 12 ans après leur collecte.

98 Message LPD 2017, FF 2017 6565, p. 6644 ; CR LPD-MEIER/TSCHUMY, art. 6, N 33 ; MÉTILLE, Traitement de données, p. 9.

99 Message LPD 2017, FF 2017 6565, p. 6644 ; CR LPD-MEIER/TSCHUMY, art. 6, N 32 ; MÉTILLE, Traitement de données, p. 9.

100 Annexe Recommandation N° R (97) 18, N 4.

101 Annexe Recommandation N° R (97) 18, N 4.

102 Le dernier exemple en date a touché plusieurs polices cantonales, l'armée, mais aussi les douanes et l'Office fédéral de la police (Fedpol). Voir à ce sujet, LE TEMPS, Une cyberattaque hors norme frappe la Suisse, touchant l'armée et de nombreuses polices, 2 juin 2023, <https://www.letemps.ch/economie/cyber/une-cyberattaque-norme-frappe-suisse-touchant-larmee-nombreuses-polices>.

103 Sur l'importance de ce principe, voir CR LPD-FANTI/STAEGER, art. 8, N 3 s. ; MEIER, N 780.

techniques appropriées (al. 1), à même de prévenir toute violation de la sécurité des données (al. 2).

La portée du principe de la sécurité des données doit être appréciée à la lumière de la notion de violation de sécurité, introduite dans le cadre de la révision à l'art. 5 let. h LPD. En vertu de cette nouvelle disposition, est considérée comme violation de la sécurité des données « *toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données* »[104].

La violation de la sécurité des données ainsi définie est donc indépendante du caractère intentionnel, malveillant ou non licite de l'acte[105] et couvre, de manière générale, tout incident de sécurité ayant pour conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles (voir art. 2 OPDo)[106].

Le principe de la sécurité tel que prévu à l'art. 8 LPD repose sur une approche fondée sur le risque[107], autrement dit, plus le degré de probabilité et de gravité de l'atteinte à la personnalité et aux droits fondamentaux des personnes concernées d'une atteinte à la sécurité des données est élevé, plus le seront les exigences auxquelles doivent répondre les mesures à prendre[108].

Le niveau de sécurité adéquat, s'articule autour de la notion « *de mesures organisationnelles et techniques appropriées* ». L'OPDo[109] tente d'en préciser les critères (voir art. 1er ss). Lesdites mesures doivent être évaluées par rapport au

104 La Convention 108+ (art. 7), le RGPD (art. 4 par. 12) et la Directive 2016/680 (art. 3 par. 11) contiennent une définition correspondante.

105 Message LPD 2017, FF 2017 6565, p. 6642 ; MÉTILLE, Traitement de données, p. 12.

106 Voir ég. Commission Nationale de l'Informatique et des Libertés (CNIL), qui cite en outre comme ex. : la suppression accidentelle de données médicales conservées par un établissement de santé et non sauvegardées par ailleurs ; la perte d'une clé USB non sécurisée contenant une copie de la base clients d'une société ; l'introduction malveillante dans une base de données scolaires et modification des résultats obtenus par les élèves, <https://www.cnil.fr/fr/definition/violation-de-donnees>.

107 Message LPD 2017, FF 2017 6565, p. 6642 ; MÉTILLE, Traitement de données, p. 12. Cette approche rejoint celle de la Convention 108+ (art. 7), du RGPD (art. 32) et la Directive 2016/680 (art. 29) ; voir Message LPD 2017, FF 2017 6565, 6650 et Rapport P-OLPD, p. 10.

108 Voir Message LPD 2017, FF 2017 6565, p. 6642 ; MÉTILLE, Traitement de données, p. 12.

109 Ordonnance sur la protection des données du 31 août 2022, RS 235.11.

risque encouru et avoir pour objectif d'assurer la confidentialité[110], la disponibilité et l'intégrité[111] ainsi que la traçabilité[112] des données traitées (art. 2 OPDo)[113].

Le caractère approprié des mesures est à apprécier en tenant compte, entre autres, de l'état des connaissances, des coûts de mise en œuvre, du type, de la finalité, de la nature, des circonstances et de l'étendue du traitement ainsi que du risque que le traitement des données présente pour la personnalité et les droits fondamentaux des personnes concernées (voir art. 1 OPDo).

La mise en place de mesures techniques et organisationnelles au sens de l'art. 8 LPD et 1er ss OPDo incombe autant au responsable du traitement des données qu'au sous-traitant[114] et ce, chacun à hauteur de sa responsabilité[115]. En outre, pendant toute la durée du traitement, lesdites mesures doivent faire l'objet d'une réévaluation quant au besoin de protection des données personnelles et du risque encouru et adaptées si nécessaire (art. 1 al. 5 OPDo).

Toujours dans le prolongement du principe de la sécurité des données, le responsable du traitement est dorénavant tenu de mettre en place des mesures techniques et organisationnelles appropriées dès la conception du traitement et par défaut, de manière à rendre impossible une violation de la sécurité des données ou du moins, en réduire la probabilité[116]. Il s'agit de l'obligation de *privacy by design and privacy by default* inscrite à l'art. 7 LPD, introduite lors de la révision totale de la LPD en vue d'un alignement sur la Convention 108+ et la réglementation européenne[117].

110 La confidentialité des données exige la mise en place de mesures techniques et organisationnelles visant à assurer le contrôle de l'accès aux données, aux locaux et aux installations et le contrôle d'utilisation (art. 3 al. 1 OPDo).

111 La disponibilité et l'intégrité des données nécessitent la mise en place de mesures des techniques et organisationnelles de contrôle des supports de données, de la mémoire et du transport, la restauration des données et de sécurité du système (art. 3 al. 2 OPDo).

112 La traçabilité est en règle générale assurée par le contrôle de la saisie, de la communication et la détection des violations de sécurité ainsi que la réparation de leurs conséquences (art. 3 al. 2 OPDo).

113 Voir Rapport P-OLPD, p. 16 s. et RGPD consid. 26 ; exemples de mesures : anonymisation, pseudonymisation et chiffrement des données personnelles ; procédure d'identification, d'analyse et d'évaluation des risques et évaluation de l'adéquation des mesures ; formation et conseils aux personnes chargées de la mise en œuvre des mesures. Voir ég. ROSENTHAL, N 54 ss.

114 ROSENTHAL, N 53 ss.

115 Voir concernant la sous-traitance, voir CR LPD-MÉTILLE, art. 9, N 1 ss ; MÉTILLE, Traitement de données, p. 19, ROSENTHAL, N 13 ss.

116 Message LPD 2017, FF 2017 6565, p. 6648 s.

117 Les art. 25 RGPD et 20 Directive 2016/680 contiennent une règle similaire.

L'idée sous-jacente est celle d'adapter la technologie et l'architecture des systèmes d'information à la protection des données en tenant compte des prescriptions légales dès la conception du traitement (art. 7 al. 1 LPD *privacy by design*)[118] et en garantissant, par le biais de préréglages appropriés, que le traitement des données personnelles soit limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement (art. 7 al. 3 LPD *privacy by default*[119])[120].

Les exigences liées à la protection des données dès la conception et par défaut présentent un lien étroit avec les principes d'évitement et de minimisation des données, eux-mêmes découlant du principe plus général de la proportionnalité (voir *supra* III.B)[121].

L'obligation, à certaines conditions, de journalisation, de la tenue d'un registre des activités de traitement (art. 12 LPD)[122], d'un règlement de traitements (voir art. 8 al. 3 LPD et 4 à 6 OPDo)[123], d'effectuer une analyse d'impact relative à la protection des données personnelles (art. 22 LPD)[124] ou encore de la possibilité de se doter d'une certification (art. 13 LPD et OCPD[125])[126], sont à considérer comme des outils et mesures contribuant à la sécurité des données[127]. Le devoir de diligence du responsable du traitement[128] en cas de sous-traitance (art. 9 al. 2 LPD) s'inscrit également dans une perspective de sécurité.

En outre, dépendant du degré du risque que représente le traitement pour la personnalité et les droits fondamentaux, le principe de sécurité peut fonder une obligation d'annonce relative à la violation de la sécurité des données (voir art. 24 LPD)[129].

---

118 Voir à ce sujet, ROSENTHAL, N 47 ss.

119 Voir à ce sujet, ROSENTHAL, N 43 ss.

120 Message LPD 2017, FF 2017 6565, p. 6648 ; pour plus de détails, voir ROSENTHAL, N 43 ss ; CR LPD-FANTI/STAEGER, art. 7, N 1 ss.

121 Voir Message LPD 2017, FF 2017 6565, p. 6644 et 6649.

122 Voir à ce sujet ROSENTHAL, N 142 ss.

123 Les critères applicables au règlement de traitement par les personnes privées sont définis à l'art. 5 OPDo et ceux relatifs au règlement de traitement des organes fédéraux.

124 Voir à ce sujet ROSENTHAL, N 148 ss.

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

126 Voir à ce sujet ROSENTHAL, N 179 s. : il convient tout de même de souligner que si une certification peut contribuer à démonter la bonne foi du responsable du traitement, elle n'implique pas forcément un niveau de sécurité adéquat. Cet élément est à considérer compte tenu de l'ensemble des circonstances concrètes du cas d'espèce. Les mesures doivent être adaptées et adéquates.

127 Voir ROSENTHAL, N 142 ss.

128 Message LPD 2017, FF 2017 6565, p. 6644 et 6651.

129 MÉTILLE, Traitement de données, p. 19 ; voir à ce sujet ROSENTHAL, N 160 ss.

Enfin, il convient de souligner que le manquement intentionnel aux exigences minimales requises en matière de sécurité des données est passible d'une amende pouvant s'élever jusqu'à CHF 250 000.– pour les personnes privées (art. 8 al. 3 et 61 let. d LPD) et de mesures administratives au sens de l'art. 51 LPD pour les organes fédéraux[130].

Compte tenu de l'importance des traitements de données personnelles à des fins statistiques, en particulier dans le cadre de la statistique publique officielle, qui bénéficient d'un cadre juridique privilégié permettant, entre autres, l'utilisation multiple et des possibilités de procéder à des appariements de données personnelles (voir *supra* III.B), la sécurité des données personnelles mérite une attention particulière.

En cas d'utilisation multiple de données, une distinction claire entre les traitements de données à des fins statistiques et les traitements à d'autres fins (ex. administratives) s'impose. Surtout, les mesures organisationnelles et techniques doivent garantir une séparation stricte entre les finalités et être adaptées à chacune d'elles. En outre, les traitements portant sur des données sensibles et dans le cadre desquels les personnes impliquées exercent deux voire plusieurs fonctions, tels que les hôpitaux et assureurs, qui peuvent exercer, à la fois le rôle de fournisseurs et destinataires de données requièrent de procéder à une séparation stricte des catégories de données traitées, sur les plans organisationnel, technique et informatique, et de restreindre les accès à ces catégories distinctes[131].

C. Traitement de données – personnes privées *versus* organes fédéraux

Si le respect des principes généraux applicables incombe à tout responsable de traitement, autrement dit, à « *la personne privée* [physiques ou morales][132], *ou l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles* » (art. 5 let. j LPD), la LPD prévoit des critères spécifiques distincts selon que le traitement de données est effectué par des personnes privées, respectivement par des organes fédéraux.

130 MÉTILLE, Traitement de données, p. 12 ; ROSENTHAL, N 56.

131 Voir PFPDT, 30e Rapport d'activités 2022/23, p. 15, concernant le programme *NaDB* mené sous la direction de l'OFS et son projet pilote *SpiGes* visant à employer la plateforme d'interopérabilité de l'OFS pour recueillir une seule fois les données relatives aux séjours stationnaires en hôpital (principe de la collecte unique des données) afin de pouvoir ensuite les utiliser à des fins aussi bien administratives que statistiques.

132 MÉTILLE, Traitement de données, p. 7.

Dans la pratique, cette approche n'est pas sans soulever des questions juridiques complexes, en particulier dans le cadre des traitements mixtes[133]. En effet, l'activité étatique requiert une collaboration entre autorités publiques – organes fédéraux et/ou autorités cantonales[134] – et/ou avec des tiers privés[135]. Celle-ci s'effectue généralement par la communication, l'échange ou le traitement conjoint de données ou encore le fait de déléguer tout ou partie d'un traitement à des tiers, notamment dans le cadre de la statistique fédérale officielle (ex. art. 4 et 10 LSF et art. 14 à 16 LB)[136].

1. Traitement par des personnes privées

Les règles spécifiques applicables aux traitements de données par des personnes privées sont énoncées au chapitre 5e de la LPD et précisées aux art. 23 s. OPDo[137].

En principe, selon l'art. 30 al. 2 LPD, une atteinte à la personnalité est illicite, notamment lorsque le traitement est réalisé en violation des principes fondamentaux de la LPD (let. a, voir ég. art. 6 et 8 LPD), contre la manifestation expresse de la volonté de la personne concernée (let. b), ou encore lorsque les données sensibles ou de profilage sont communiquées à des tiers (let. c), à moins que la personne concernée n'ait rendu elle-même ses données personnelles accessibles à tout un chacun et ne se soit pas opposée expressément au traitement (art. 30 al. 3 LPD).

L'illicéité peut être levée en présence de l'un des motifs justificatifs prévus par le législateur, à savoir le consentement de la personne concernée, un intérêt privé ou public prépondérant, ou une loi[138] (art. 31 al. 1 LPD).

L'art. 31 al. 2 LPD énumère, à titre d'exemples, six hypothèses de traitement dans le cadre desquelles l'intérêt prépondérant du responsable du traitement privé

133 CR LPD-Epiney/Sumbo, art. 40, N 19 ; CR LPD-Epiney/Posse, art. 33, N 2 ss.

134 CR LPD-Epiney/Posse, art. 33, N 19, p. ex. collaboration entre autorités fédérales dans le cadre de systèmes d'information communs.

135 CR LPD-Epiney/Posse, art. 33, N 2 ; CR LPD-Epiney/Sumbo, art. 40, N 19 ss ; CR LPD-Epiney/Posse, art. 33, N 2.

136 Autres ex. art. 97*a* LACI, art. 105 ss LEI, art. 59 LEp.

137 Pour ce qui est du champ d'application personnel et matériel de l'art. 2 al. 2 LPD, voir Métille, Traitement de données, p. 6 ss.

138 Voir Métille, Traitement de données, p. 37 s.

est, en quelque sorte, présumé[139]. Partant, il incombe à la personne concernée lésée par le traitement d'en renverser la présomption.

Le qualificatif « prépondérant » est à souligner. En effet, la simple existence d'un intérêt du responsable du traitement figurant au catalogue de l'art. 31 al. 2 LPD ne suffit en principe pas à lever l'illicéité de l'atteinte à la personnalité. Faut-il encore qu'à l'issue d'une mise en balance des intérêts dans le cas d'espèce, l'intérêt au traitement des données du responsable du traitement l'emporte sur celui de la personne concernée (voir *supra* III.B)[140].

2. Traitement par des organes fédéraux

Les règles particulières mises aux traitements de données par les organes fédéraux réglés au chapitre 6 de la LPD (art. 33 à 42 LPD), sont d'une exigence plus élevée que celles applicables aux responsables de traitement privés. En effet, en sus des principes généraux et autres prescriptions de la LPD, le traitement de données doit respecter le principe de la légalité ancré à l'art. 34 LPD[141].

Pierre angulaire du dispositif, l'art. 34 LPD consolide dans la LPD plusieurs normes constitutionnelles à la fois[142]. En effet, il précise aussi bien le principe de légalité de l'activité étatique (l'exigence d'une base légale) posé à l'art. 5 Cst., que le droit à l'autodétermination informationnelle consacré à l'art. 13 Cst. et garanti par l'art. 8 CEDH et les conditions de sa restriction (art. 36 Cst.)[143].

En vertu du principe de la légalité, les organes fédéraux ne sont fondés à traiter ou à communiquer des données personnelles que s'il existe une base légale le permettant (art. 34 et 36 LPD).

---

139 Les hypothèses visées par le législateur concernent pour l'essentiel des traitements de données effectués dans le cadre de relations économiques (dans le cadre d'un rapport de concurrence ou en vue de la conclusion/l'exécution d'un contrat ou d'évaluer la solvabilité) (let. a – c) ; en lien avec le droit à l'information et la transparence de l'activité étatique (let. d et f) ; ou à des fins ne rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique moyennant la réalisation de certaines conditions (let. e). (voir *infra* IV.A). Voir à ce sujet CR LPD-Boillat/Werly, art. 31, N 1 et 31 ; Rosenthal, N 20 ; voir ég. Meier, N 1522. Voir quant aux modifications apportées par la révision de 2017, Rosenthal, N 42.

140 CR LPD-Boillat/Werly, art. 31, N 31 ; Rosenthal, N 41.

141 CR LPD-Epiney/Posse, art. 34, N 5 et références citées ; Métille, Traitement de données, p. 39.

142 CR LPD-Epiney/Posse, art. 34, N 3.

143 Voir CR LPD-Epiney/Posse, art. 34, N 2 ; voir CR Cst.-Hertig Randall/Marquis, art. 13, N 64.

Celle-ci peut être prévue dans une loi au sens ou matériel ou formel pour les restrictions les plus importantes[144] et son exigence vaut en principe pour toutes les phases du traitement[145].

En tout état de cause, la base légale doit revêtir une densité normative suffisante, autrement dit présenter le degré de clarté, de précision et de transparence requis[146]. Les critères développés par la CourEDH dans ce domaine sont très restrictifs[147].

Un traitement de données effectué par un organe fédéral est illicite s'il est réalisé en violation d'un ou plusieurs principes, des autres prescriptions de la LPD ou de toute autre norme juridique contraignante (voir *supra* III.C.1) ou lorsqu'il est effectué en l'absence ou en violation d'une base légale (art. 34 LPD) respectivement des exigences constitutionnelles[148].

À noter qu'en vertu du privilège de la recherche scientifique, le traitement de données à des fins de statistiques dans le cadre de la statistique officielle fédérale, bénéficie d'une dérogation aux principes de finalité et de reconnaissabilité et d'une atténuation du principe de la légalité (voir *infra* IV.A.3.a)[149].

IV. Cadre juridique spécifique – Statistique

En sus du cadre juridique général en matière de protection des données, les données personnelles collectées et/ou traitées à des fins statistiques

144 En règle générale, une base légale au sens formel est requise pour le traitement et la communication de données sensibles, en cas de profilage ou lorsque la finalité ou le mode du traitement de données personnelles est susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée (voir art. 36 al. 1 Cst., art. 34 al. 2 et 36 al. 1 LPD). Toutefois l'art. 34 al. 3 aménage une exception à l'exigence d'une base légale formelle. Une base légale au sens matériel peut suffire, pour autant qu'il ne s'agit pas de profilage, que le traitement soit indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel et que sa finalité ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée. Voir CR LPD-Epiney/Posse, art. 34, N 5 et références citées.

145 À noter que l'art. 34 al. 4 prévoit une atténuation au principe de la légalité, lorsque le traitement de données a été autorisé par le Conseil fédéral (let. a), qu'il est basé sur le consentement de la personne concernée, ou qu'il est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers (let. c). Voir CR LPD-Epiney/Posse, art. 34, N 8.

146 CR LPD-Epiney/Posse, art. 34, N 35.

147 Voir à ce sujet, Message LPD 2017, FF 2017 6565, p. 6586 ; CourEDH, *Vetter c. France*, arrêt du 31 août 2005, nº 59842/00 ; CourEDH, *Peck c. UK*, arrêt du 28 janvier 2003, nº 44647/98 ; CourEDH, *Amman c. Suisse*, arrêt du 16 février 2000, nº 27798/95 ; CourEDH, *Vukota-Bojić c. Suisse*, arrêt du 18 octobre 2016, nº 61838/10.

148 CR LPD-Epiney/Posse, art. 34, N 8 ; Métille, Traitement de données, p. 39.

149 CR LPD-Epiney/Posse, art. 39, N 37.

sont régies par les instruments et dispositions spécifiques pertinentes en matière de statistique.

A. Art. 31 al. 2 let. e et art. 39 LPD – *Privilège de la recherche*

Au niveau de la LPD, le traitement de données personnelles à des fins statistiques relève, à certaines conditions, du régime dérogatoire aménagé au profit de la recherche scientifique au sens large (privilège de la recherche), applicable aux traitements ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification et en l'occurrence la statistique[150].

En tant qu'ils constituent une branche particulière de la recherche scientifique, les traitements de données à des fins statistiques relèvent en partie des critères applicables aux traitements de données à des fins ne se rapportant pas aux personnes et sont, pour le reste, réglés par les instruments et autres dispositions spécifiques.

Institués à l'art. 31 al. 2 let. e LPD pour les traitements de données par des personnes privées et à l'art. 39 LPD en ce qui concerne les organes fédéraux, les allégements prévus pour les traitements des données à des fins ne se rapportant pas aux personnes sont soumis à la réalisation des conditions cumulatives respectives énoncées (voir art. 31 al. 2 let. e et art. 39 al. 1 LPD). En principe, ils couvrent toute forme de traitement pour autant que les critères énoncés demeurent remplis[151].

Les privilèges consistent en une dérogation aux principes de finalité et de reconnaissabilité, en ce sens que les données déjà collectées peuvent être utilisées à des fins de recherche, de planification ou de statistique (ou toute autre fin ne se rapportant pas à des personnes)[152] et une atténuation du principe de légalité en ce qui concerne les traitements effectués par les organes fédéraux (art. 39 al. 2 LPD)[153].

Pour rappel, les données anonymisées ne relèvent pas du champ d'application de la LPD, les données anonymes n'étant pas considérées comme des données personnelles (voir *infra* IV.A.2.a).

150 Baeriswyl/Pärli/Blonski, Handkomm. DSG-Baeriswyl, art. 39, N 1 ; Rosenthal/Jöhri, art. 22, N 1 ; voir CR LPD-Epiney/Posse, art. 39, N 1.
151 Meier, N 1702.
152 CR LPD-Epiney/Posse, art. 39, N 37.
153 CR LPD-Epiney/Posse, art. 39, N 37.

Il sied de souligner que, les allégements concernent les conditions du traitement ; ils ne dispensent aucunement le responsable du traitement du respect des principes généraux ni des autres prescriptions de la LPD[154].

Selon le législateur, ce cadre juridique privilégié se justifie à double égard car, d'une part, il tient compte de l'intérêt public et privé des domaines concernés lié aux attentes légitimes de la société en matière d'innovation et de progrès des connaissances[155] ; et d'autre part, ce type de traitements est censé présenter moins de risques pour les droits des individus étant donné que les finalités du traitement ne se rapportent pas à des personnes[156].

À noter que les domaines énumérés par la LPD sont exemplatifs et non exhaustifs[157]. D'autres intérêts, tels que la prévention d'accidents ou de catastrophes naturelles ou la mensuration officielle[158] peuvent bénéficier de ce cadre juridique privilégié pour autant que les critères juridiques énoncés à l'art. 31 al. 2 let. e LPD, respectivement à l'art. 39 LPD soient réunis[159].

Compte tenu de la systématique de la LPD, le traitement de données à des fins statistiques repose sur des bases légales différentes selon que le traitement est effectué par une personne privée (art. 31 al. 2 let. e LPD) ou par un organe fédéral (art. 39 LPD), même si dans l'ensemble, les allégements prévus dans ce cadre restent similaires[160].

Lorsque des données personnelles sont traitées à des fins ne se rapportant pas à des personnes et que le traitement sert par ailleurs une autre finalité, les dérogations ne s'appliquent qu'au seul traitement effectué à des fins ne se rapportant pas à des personnes (art. 35 OPDo). Par conséquent, il faut impérativement opérer une distinction claire entre les traitements de données à des fins statistiques et les traitements à d'autres fins et prévoir une séparation stricte des catégories de données traitées à travers la mise en place de mesures à la fois

154 BAERISWYL/PÄRLI, Handkomm. DSG-BAERISWYL, art. 22, N 10 ss.
155 Voir consid. 113 RGPD.
156 Voir Message aLPD, FF 1988 II 421, p. 479 ; BSK DSG/BGÖ-MAURER-LAMBROU/KUNZ, art. 22, N 1a s. ; ROSENTHAL/JÖHRI, art. 22, N 1 ; CR LPD-EPINEY/POSSE, art. 39, N 4. L'intérêt public est également mis en évidence à l'art. 89 RGPD qui prévoit des garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques (voir N 11 ss). Voir CR LPD-EPINEY/POSSE, art. 39, N 1 ; KOÇ, N 30.1.
157 Voir CR LPD-EPINEY/POSSE, art. 39, N 17 ; BAERISWYL/PÄRLI/BLONSKI, Handkomm. DSG-BAERISWYL, art. 39 N 11 ; ROSENTHAL/JÖHRI, art. 22, N 1.
158 P. ex. dans le cadre de la Loi sur la géoinformation (LGéo).
159 Voir CR LPD-EPINEY/POSSE, art. 39, N 17 ; ROSENTHAL/JÖHRI, art. 22, N 1.
160 Voir CR LPD-EPINEY/POSSE, art. 39, N 5 ; ROSENTHAL/JÖHRI, art. 22, N 1 ; BAERISWYL/PÄRLI, Handkomm. DSG-BAERISWYL, art. 22, N 2 ss.

organisationnelles, techniques et informatiques au sens de l'art. 8 LPD (voir *supra* III.B)[161].

Par ailleurs, autant le traitement de données personnelles que celui à des fins ne se rapportant pas à des personnes, en l'occurrence la statistique, peuvent être soumis à d'autres normes légales spécifiques[162]. Le cas échéant, celles-ci demeurent applicables en vertu du principe de la priorité des dispositions spéciales sur les dispositions générales, c'est notamment le cas en ce qui concerne les dispositions de la Loi sur la statistique fédérale (LSF) et de la Loi sur l'harmonisation de registres (LHR)[163].

1. Traitement à des fins ne se rapportant pas à des personnes

Le premier critère porte sur la finalité du traitement. Pour que l'objectif du traitement des données personnelles soit considéré comme tel, il doit poursuivre une finalité autre que celle d'obtenir une information sur une personne donnée[164].

Le but du traitement doit donc être indépendant de l'identité des individus dont les données sont traitées[165]. En d'autres termes, la référence à des personnes n'est guère importante du point de vue de la finalité du traitement.

Le traitement à des fins ne se rapportant pas à des personnes peut concerner un grand nombre de personnes, ou porter sur un seul individu dont les caractéristiques sont importantes pour la recherche scientifique[166], bien que, de manière générale, la statistique implique un phénomène de masse.

En revanche, de manière générale, les recherches historiques ou généalogiques visant des personnes données, ne remplissent pas ce critère. Partant, elles ne peuvent pas se prévaloir du privilège de la recherche scientifique[167].

161 PFPDT, Rapport, p. 15. Exemple : restriction des accès *etc*.
162 CR LPD-Epiney/Posse, art. 39, N 6 ; Baeriswyl/Pärli/Blonski, Handkomm. DSG-Baeriswyl, art. 39, N 3 s.
163 *Cf*. ATF 128 II 311, c. 8 ; Message aLPD, FF 1988 II 421, p. 452 ; CR LPD-Epiney/Posse, art. 39, N 6 ; Rosenthal, N 40 ; Meier, N 286 ss ; BSK DSG/BGÖ-Maurer-Lambrou/Kunz, art. 22, N 1 ss ; Baeriswyl/Pärli, Handkomm. DSG-Baeriswyl, art. 22, N 5 ; Rosenthal/Jöhri, art. 22, N 3 ss.
164 Voir CR LPD-Epiney/Posse, art. 39, N 18 ; Koç, N 30.1 ss.
165 Voir CR LPD-Epiney/Posse, art. 39, N 18 ; Koç, N 30.1 ss.
166 Meier, N 1701.
167 Meier, N 1703.

Les critères des art. 31 al. 2 let. b et 39 LPD visent les situations dans lesquelles le responsable traite les données déjà en sa possession à des fins ne se rapportant pas à des personnes[168].

Leur portée s'étend aux traitements de données personnelles en vue de la préparation d'avis ou de rapports d'expertise, pour autant qu'ils soient réalisés à d'autres finalités ne se rapportant pas à des personnes[169].

2. Garanties générales incombant au responsable du traitement

Le régime dérogatoire applicable aux traitements de données à des fins ne se rapportant pas à des personnes est subordonné à l'obligation pour le responsable du traitement – personne privée comme organe fédéral – de mettre en place des garanties visant à prévenir les atteintes à la personnalité et aux droits fondamentaux des personnes concernées (voir art. 1er LPD). Elles se rapportent, pour l'essentiel à l'anonymisation, la publication et la communication de données à des tiers.

a) Anonymisation des données

Le responsable du traitement a l'obligation de procéder à l'anonymisation des données personnelles « *dès que la finalité du traitement le permet* »[170]. Le législateur ne donne toutefois pas plus de précision quant au moment auquel elle devrait intervenir, laissant ainsi une certaine marge d'appréciation au responsable du traitement[171].

168 Message aLPD, FF 1988 II 479 ; CR LPD-EPINEY/POSSE, art. 39, N 17 ; BAERISWYL/PÄRLI/BLONSKI, Handkomm. DSG-BAERISWYL, art. 39, N 12 ; ROSENTHAL/JÖHRI, art. 22, N 2.

169 Voir BAERISWYL/PÄRLI/BLONSKI, Handkomm. DSG-BAERISWYL, art. 39, N 11 ; CR LPD-EPINEY/POSSE, art. 39, N 20.

170 P. ex : Dans le cadre de traitement de données effectué pour procéder uniquement au comptage du nombre de passages par le biais d'un tourniquet de passage, les données peuvent être collectées de manière anonymes, ce qui ne serait pas le cas, lorsqu'une certaine traçabilité est nécessaire. En pratique, l'anonymisation implique un risque de perte de données pour les statisticiens.

171 CR LPD-EPINEY/POSSE, art. 39, N 22. La législation spéciale ne prévoit pas plus de précision. Elle reprend la même formulation « *…dès que le but de leur traitement le permet* [tout en mentionnant] *mais au plus tard 30 ans après le relevé des données* ».

Conçue comme une mesure visant à prévenir, ou du moins limiter les éventuelles atteintes aux droits des personnes concernées, l'anonymisation doit intervenir le plus rapidement possible[172]. En principe, lorsque des données sensibles doivent être traitées à des fins statistiques, elles devraient être collectées de manière que la personne concernée ne soit pas identifiable[173] (voir p. ex. art. 119 al. 5 CP relatif à l'interruption de grossesse non punissable)[174]. Lorsqu'il existe un besoin légitime de collecter des données sensibles à des fins statistiques sous une forme identifiable[175], des garanties appropriées doivent être mises en place[176].

En tout état de cause, le moment est à apprécier au cas par cas, en prenant en considération l'ensemble des circonstances du traitement – notamment le cycle de la vie des données – et par rapport à la finalité du traitement[177]. À notre sens, le moment de l'anonymisation doit faire l'objet d'une interprétation restrictive[178] basée sur une approche contextuelle et systémique des principes et autres prescriptions de la LPD. Surtout, il est essentiel de procéder, dans chaque cas d'espèce, à une interprétation des principes fondamentaux de la LPD, les uns à la lumière des autres, en particulier sous l'angle de la proportionnalité – plus précisément de la durée de conservation – et de la sécurité des données et l'obligation de protection des données dès la conception et par défaut qui en découle. À titre d'exemple la protection de données génétiques nécessiteront des garanties autres que celles à mettre en place dans le cadre de système de traçage.

Pour rappel, la LPD, ne s'applique pas ou plus aux données anonymisées, celles-ci n'étant plus considérées comme des données personnelles[179].

En revanche, les données personnelles qui ont fait l'objet d'une pseudonymisation, c'est-à-dire codées ou chiffrées, de manière à ce qu'elle « *ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* » (art. 4

172 CR LPD-Epiney/Posse, art. 39, N 22 ; voir ég. BSK DSG/BGÖ-Maurer-Lambrou/Kunz, art. 22, N 24.

173 Rapport explicatif Convention 108+, N 61.

174 Cette disposition dont la teneur est la suivante : « [à] *des fins statistiques, toute interruption de grossesse doit être annoncée à l'autorité de santé publique compétente ; l'anonymat de la femme concernée est garanti et le secret médical doit être respecté* » porte sur un domaine extrêmement sensible. Dès lors, il importe d'anonymiser, les données dans la mesure du possible, au moment de la collecte.

175 Ex. afin de réaliser des enquêtes répétées ou longitudinales.

176 Rapport explicatif Convention 108+, N 61.

177 Voir CR LPD-Epiney/Posse, art. 39, N 22.

178 CR LPD-Epiney/Posse, art. 39, N 22 ; voir ég. BSK DSG/BGÖ-Maurer-Lambrou/Kunz, art. 22, N 24.

179 VOIR CR LPD-Epiney/Posse, art. 39, N 13.

par. 5 RGPD), sont à considérer comme des informations concernant une personne physique identifiable[180]. La LPD est donc applicable[181].

« *Le caractère identifiable d'une personne est relatif* »[182]. Pour évaluer si des informations supplémentaires sont susceptibles d'individualiser une personne, il convient de prendre en considération l'ensemble des facteurs objectifs, autrement dit « *l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage* »[183], en particulier l'intérêt d'une identification, l'investissement en temps et en coût nécessaires de l'identification tout en tenant compte des technologies disponibles au moment du traitement et de leur évolution[184].

Le caractère identifiable d'une personne au sens de l'art. 5 let. a LPD, s'apprécie du point de vue du détenteur de l'information[185].

Dans tous les cas, le choix de la solution optimale tant en ce qui concerne le moment que les méthodes d'anonymisation ou les mesures supplémentaires appropriées devrait s'opérer au cas par cas, en utilisant éventuellement une combinaison de techniques différentes[186].

Lorsqu'une anonymisation n'est pas possible, car il est indispensable de conserver la forme identifiable ou qu'elle exige des efforts disproportionnés, le responsable de traitement doit prendre des mesures appropriées afin que les personnes concernées ne puissent pas être identifiées (art. 31 al. 2 let. e par. 1 LPD)

---

180 Message LPD 2017, FF 2017 6565, p. 6639 ; voir ég. ROSENTHAL, N 20.

181 KOÇ, N 30.10.

182 CR LPD-MEIER/TSCHUMY, art. 5, N 25.

183 Consid. 26 RGPD.

184 Consid. 26 RGPD.

185 Voir TF, 1C_425/2020 du 28 février 2020, concernant le refus de l'OFS de faire suite à une demande d'accès d'un particulier concernant des données archivées le concernant dans le cadre d'échantillonnage, soutenant qu'elles étaient anonymisées et que dès lors la LPD n'est pas applicable. Dans le cas d'espèce, le TF rappelle que les données archivées du cadre d'échantillonnage contiennent le numéro AVS, lequel permet d'attribuer sans équivoque une information à une personne déterminée. Il s'agit donc de données relatives à une personne identifiable. En l'occurrence, cela vaut du point de vue de l'OFS en tant que détenteur de l'information, puisqu'il est en mesure d'identifier les personnes au moyen d'un répertoire d'adresses plus récent. Voir ég. CJUE, arrêt C-434/16 du 20 décembre 2017, *Nowak*, C, § 34 s. ; TUE, arrêt du 26 avril 2023, *affaire T-557/20 (CRU/CEPD)* ; JOTTERAND, Des données personnelles pseudonymisées transférées à un tiers deviennent-elles anonymes ? CJUE, arrêt C-582/14 du 19 octobre 2016, *Breyer* ; pour plus de détails voir CR LPD-MEIER/TSCHUMY, art. 5, N 25 ; voir concernant l'anonymisation des données médicales JOTTERAND/ERARD, N 39 ; JOTTERAND/ERARD, Personal Data or Anonymous ? ; voir ég. ERARD, p. 608 ; KOÇ, N 30.10 ; WALTER, p. 163.

186 GROUPE 29, Avis 05/2014 sur les techniques d'anonymisation, p. 3.

(p. ex. des règles en matière de secret professionnel, restriction des accès et de la diffusion de données liées aux fins de traitement ne se rapportant pas à des personnes ou autres mesures d'ordre technique et organisationnel visant la sécurité des données). De plus, toute utilisation de l'information obtenue pour la prise de décisions ou de mesures concernant une personne donnée est, en règle générale exclue[187].

b) Mesures relatives à la publication des résultats

De manière générale, la transmission de données par publication contribue à une diffusion plus ou moins large de l'information et peut, de ce fait générer des atteintes particulièrement importantes aux droits des personnes concernées[188] lorsqu'elles sont susceptibles d'être reliées à elles.

Partant, dans le cadre des traitements de données ne se rapportant pas aux personnes, lorsqu'une publication des résultats, intermédiaires ou finaux, du traitement est envisagée, elle ne peut être réalisée que sous une forme ne permettant pas d'identifier les personnes concernées[189].

En d'autres termes, la publication des résultats doit être dénuée de toute référence à des personnes. En ce sens, les rapports issus de la recherche, de la planification et de la statistique qui permettent d'identifier des personnes ne remplissent pas ce critère. Le cas échéant, une publication ne peut intervenir que si elle repose sur une base légale l'autorisant[190].

3. Critères spécifiques

a) Traitement par des personnes privées (art. 31 al. 2 let. e LPD)

aa) Motif justificatif

En principe, dans le cadre des traitements de données par des personnes privées, une atteinte illicite à la personnalité au sens de l'art. 30 LPD est

187 Annexe à la Recommandation nº R(97)18 du Comité des Ministres aux États membres, N 4.4.

188 Message aLPD, FF 1988 II 421, p. 480 ; CR LPD-Epiney/Posse, art. 39, N 32 ; Koç, N 30.15 s.

189 Message aLPD, FF 1988 II 421, p. 480 ; CR LPD-Epiney/Posse, art. 39, N 32.

190 CR LPD-Epiney/Posse, art. 39, N 35 ; Baeriswyl/Pärli/Blonski, Handkomm. DSG-Baeriswyl, art. 39, N 28.

justifiée par le consentement de la personne concernée, par un intérêt privé ou public prépondérant, ou par la loi (ex. art. 15 LB) (art. 31 al. 1 LPD)[191].

Lorsque le traitement repose sur le consentement de la personne concernée, le responsable de traitement doit prévoir un consentement séparé pour les traitements à des fins de statistiques[192].

En l'absence du consentement de la personne concernée ou d'une base légale l'autorisant, le responsable de traitement privé, peut, dans le cadre de traitement de données à des fins ne se rapportant pas à des personnes, se prévaloir d'un motif justificatif spécifique lié au privilège de la recherche en vertu de l'art. 31 al. 2 let. e LPD.

Cette disposition relève des situations où le législateur a opéré sur une pesée préalable des intérêts et présumé l'existence d'un intérêt prépondérant du responsable du traitement lorsque les conditions cumulatives de l'art. 31 al. 2 let. e LPD sont réalisées.

En principe, il n'est pas nécessaire que la motivation du responsable du traitement soit altruiste[193]. Le but peut être purement économique[194], financier ou encore administratif.

Il sied toutefois de relever le caractère primordial du qualificatif « *prépondérant* », qui implique que la simple existence d'un intérêt du responsable au traitement ne suffit en principe pas. Il faut encore que celui-ci résiste à l'examen de la proportionnalité (voir *supra* III.B). Concrètement, cela nécessite une mise en balance de l'intérêt privé du responsable au traitement des données d'une part, avec celui de la personne concernée à ce que ses données ne soient pas traitées et d'éventuels autres intérêts privés ou publics (p. ex. lorsqu'un grand nombre de personnes est touché) d'autre part[195].

bb) Mesures relatives à la communication de données sensibles à des tiers

De manière générale, le responsable du traitement ne peut communiquer des données sensibles à des tiers « *que sous une forme ne permettant pas d'identifier les personnes concernées* » (art. 31 al. 2 let. e LPD).

En principe, autant pour le traitement de données par des personnes privées que par des organes fédéraux, une anonymisation factuelle – c'est-à-dire lorsque

191 Voir KOÇ, N 30.9.
192 Voir BECK, p. 1.
193 MEIER, N 1704 et référence citée.
194 MEIER, N 1701 : p. ex. industrie pharmaceutique, alimentaire *etc*.
195 Voir à ce sujet, ATF 138 II 346.

les données sont transmises sous une forme pseudonymisée et que la clé permettant de réidentifier la personne reste en possession de la personne qui transmet les données – suffit pour remplir cette exigence (voir *supra* IV.A.3.a).

Ce critère fait partie des mesures visant à renforcer la protection des données personnelles sensibles, introduites lors de la révision de la LPD[196].

À défaut, il incombe au responsable du traitement privé de prendre des mesures afin de s'assurer que le tiers destinataire ne traite les données qu'aux seules finalités ne se rapportant pas à des personnes (art. 31 al. 2 let. e par. 1 LPD).

b) Traitement par des organes fédéraux (art. 39 LPD)

Si de manière générale, l'organe fédéral est habilité à communiquer à des personnes privées des données personnelles en application de l'art. 39 LPD, il n'est fondé à le faire « *que sous une forme ne permettant pas d'identifier les personnes concernées* » (voir art. 39 al. 1 let. b) lorsqu'il s'agit de données sensibles, à moins qu'il n'y soit autorisé en vertu d'une base légale correspondante[197].

De plus, le tiers destinataire de ces données ne peut à son tour transmettre les données à des tiers qu'avec le consentement de l'organe fédéral qui les lui a transmises. Ce critère permet à l'organe fédéral de mettre en place des garanties afin de prévenir une potentielle violation du principe de finalité[198]. Dans la pratique, cette exigence requiert l'établissement d'une convention ou d'instructions claires ou décisions adressant les aspects déterminants du traitement[199].

L'organe fédéral au sens de l'art. 39 LPD est l'organe fédéral responsable du traitement en vertu de l'art. 33 LPD[200].

Conformément au principe de légalité, la collecte de données doit reposer sur une base légale et ne peut pas se fonder uniquement sur l'art. 39 LPD[201].

Les privilèges institués par l'art. 39 LPD consistent en une dérogation aux principes de finalité et de reconnaissabilité, en ce sens que les données déjà collectées peuvent être utilisées à des fins de recherche, de planification ou de

196 Message LPD 2017, FF 2017 6565, p. 6626.
197 BAERISWYL/PÄRLI/BLONSKI, Handkomm. DSG-BAERISWYL, art. 39, N 2-3 ; CR LPD-EPINEY/POSSE, art. 39, N 3 ; BSK DSG/BGÖ-MAURER-LAMBROU/KUNZ, art. 22, N 4.
198 CR LPD-EPINEY/POSSE, art. 39, N 3 ; BSK DSG/BGÖ-MAURER-LAMBROU/KUNZ, art. 22, N 27.
199 CR LPD-EPINEY/POSSE, art. 39, N 30 ; BSK DSG/BGÖ-MAURER-LAMBROU/KUNZ, art. 22, N 26.
200 CR LPD-EPINEY/POSSE, art. 39, N 27.
201 Message aLPD, FF 1988 II 421, p. 480 ; CR LPD-EPINEY/POSSE, art. 39, N 37.

statistique (ou toute autre fin ne se rapportant pas à des personnes)[202] et une atténuation – et non pas une dérogation – au principe de finalité[203].

En effet, ils ne dispensent l'organe fédéral que de l'exigence plus restrictive d'une loi au sens formel pour le traitement de données sensibles, de profilage ou susceptibles de porter gravement atteinte aux droits fondamentaux de la personne concernée lorsque les données sont traitées à des fins de recherche, de planification ou de statistique et pour la communication de données personnelles (voir art. 36 al. 1 LPD). En ce sens, une loi au sens matériel demeure toutefois requise[204].

B. Législation spéciale en matière de statistique officielle publique

Dans le domaine de la statistique, les critères de l'art. 39 LPD sont concrétisés et précisés par la législation spéciale pertinente, composée pour l'essentiel des lois fédérales spécifiques et de leurs dispositions d'application[205]. Le dispositif est complété par d'autres normes légales spécifiques prévues dans des instruments sectoriels[206].

Il s'agit pour l'essentiel des réglementations suivantes :

– Loi sur la statistique fédérale (LSF) ;
– Loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes (Loi sur l'harmonisation de registres)[207] ;
– Loi sur le recensement fédéral de la population (Loi sur le recensement)[208] ;
– Loi fédérale sur le numéro d'identification des entreprises (LIDE)[209] ;

202 Message aLPD, FF 1988 II 421, p. 480 ; CR LPD-EPINEY/POSSE, art. 39, N 37.
203 Message aLPD, FF 1988 II 421, p. 480 ; CR LPD-EPINEY/POSSE, art. 39, N 37.
204 BSK BV-EPINEY, art. 36, N 33 ; CR Cst.-DUBEY, art. 36, N 82 ; PC Cst.-AUBERT/MAHON, art. 36, N 8.
205 Voir CR LPD-EPINEY/POSSE, art. 39, N 3.
206 P. ex. art. 14 à 16 LB, art. 119 al. 5 CP.
207 Loi fédérale du 23 juin 2006 sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes (LHR) (Loi sur l'harmonisation de registres), RS 431.02.
208 Loi fédérale du 22 juin 2007 sur le recensement fédéral de la population (Loi sur le recensement), RS 431.112.
209 Loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE), RS 431.03.

– et les ordonnances d'application[210].

1. L'OFS

L'Office fédéral de la statistique (OFS) est le service statistique central de la Confédération. Il fournit des prestations de nature statistique aux unités administratives de la Confédération, ainsi qu'à d'autres utilisateurs de la statistique fédérale et au public.

Entre autres, il collabore étroitement avec les cantons à la tenue d'un Registre des entreprises et des établissements (REE) et d'un Registre fédéral des bâtiments et des logements (RegBL). Il tient un fichier suisse des étudiants avec les hautes écoles.

2. Protection et sécurité des données

Les dispositions pertinentes en matière de protection et de sécurité des données sont prévues aux art. 4 et 14 à 17 LSF[211]. Celles-ci sont applicables en vertu du principe de la priorité des dispositions spéciales sur les dispositions générales. Elles constituent ainsi une *lex specialis* par rapport à l'art. 39 LPD[212]. Les règles de protection et de sécurité des données aménagées par la LSF couvrent l'ensemble des travaux statistiques. Leur respect incombe à tous les services traitant des données personnelles provenant de la statistique fédérale (organes fédéraux, cantons, commune, voir art. 15 et 16 LSF).

En vertu de l'art. 4 LSF relatif aux principes de la collecte des données, l'OFS est habilité à collecter les données administratives de la Confédération, auprès des autorités fédérales, cantonales ou communales ou auprès d'autres personnes morales de droit public.

---

210 Ordonnance du 30 juin 1993 concernant l'organisation de la statistique fédérale, RS 431.011 ; Ordonnance du 30 juin 1993 concernant l'exécution des relevés statistiques fédéraux (Ordonnance sur les relevés statistiques), RS 431.012.1 ; Ordonnance du 26 janvier 2011 sur le numéro d'identification des entreprises (OIDE), RS 431.031 ; Ordonnance du 19 décembre 2008 sur le recensement fédéral de la population (Ordonnance sur le recensement), RS 431.112.1 ; Ordonnance du 9 juin 2017 sur le Registre fédéral des bâtiments et des logements (ORegBL), RS 431.841 ; Ordonnance du 30 juin 1993 sur le Registre des entreprises et des établissements (OREE), RS 431.903.

211 Voir ég. art. 3*a* al. 2 Ordonnance sur les relevés statistiques.

212 Voir ATF 128 II 311, c. 8 ; Message LPD, FF 2017 6631 ; Message aLPD, FF 1988 II 479 ; MEIER, Protection des données, N 286 ; voir ég. BSK DSG/BGÖ-MAURER-LAMBROU/KUNZ, art. 22, N 1 ss et ROSENTHAL/JÖHRI, art. 22, N 5 ss.

La LSF institue une obligation pour les unités administratives et les autres organismes, de communiquer à l'OFS, les bases et les résultats de leurs travaux statistiques et si nécessaire de lui fournir des données provenant de leurs banques de données et de leurs relevés (art. 10 al. 4 et 2 al. 3 LSF).

En principe, la LSF exclut l'utilisation des données collectées ou communiquées à des fins statistiques à d'autres fins, à moins qu'une loi fédérale n'autorise expressément une autre utilisation ou que la personne physique ou morale concernée n'y ait consenti par écrit (art. 14 al. 1 LSF).

Pour ce qui est de la publication, les résultats doivent être présentés sous une forme qui rend impossible toute déduction sur la situation d'une personne physique ou morale, sauf si les données traitées ont été rendues publiques par la personne concernée (art. 18 LSF). Notamment, les résultats des relevés ne peuvent l'être que sous une forme qui exclut toute identification des personnes, des ménages, des entreprises ou des établissements interrogés (art. 10 Ordonnance sur les relevés statistiques).

Les obligations liées à la sécurité des données sont rappelées à l'art. 15 LSF. En substance, la LSF accorde un large pouvoir d'appréciation à l'OFS en ce qui concerne la durée de la conservation des données. L'art. 8*a* reprend les termes peu précis des art. 31 al. 2 let. e par. 1 et 39 al. 1 let. a LPD selon lesquels, l'anonymisation des données doit intervenir « *dès que le but de leur traitement le permet* » en y ajoutant « *mais au plus tard 30 ans après le relevé des données* ».

Cette marge devrait à notre avis être reconsidérée à la lumière de la LPD révisée, en particulier des principes de proportionnalité et de sécurité des données ; le délai de 30 ans étant le maximum autorisé.

En tout état de cause, les principes d'évitement et de minimisation des données – et plus spécifiquement sous l'angle de la durée de conservation des données – conjugués au principe de la sécurité des données et de l'obligation de protection des données dès la conception et protection des données par défaut qui en découle, commande à notre sens, des contrôles périodiques et si nécessaire un certain « *élagage des données* » qui ne sont plus nécessaires au regard des finalités du traitement (art. 6 al. 4 LPD)[213].

3. Secret de fonction et sanction

En vue d'assurer la confidentialité des données, la LSF prescrit le secret de fonction, assorti d'une sanction en cas de violation (art. 23 LSF), à la charge des personnes effectuant des travaux statistiques (y compris dans les

213 Voir *supra* III.B.

cantons et les communes) portant sur les données concernant des personnes physiques ou morales dont elles ont eu connaissance dans l'exercice de leur fonction (art. 14 al. 2 LSF).

En ce sens, l'art. 7 al. 3 de l'Ordonnance sur les relevés statistiques par exemple, institue l'obligation d'établir un contrat pour régler le secret et le devoir de vigilance des organismes et des instituts de sondage.

La violation du secret est passible « *des arrêts ou de l'amende* » (art. 23 LSF).

4. Appariement de données

a) Notion

Selon les constats des autorités compétentes en matière de statistiques, les relevés directs peuvent s'avérer non seulement coûteux pour la Confédération, mais également fastidieux pour les personnes interrogées. Ils suscitent des interrogations ou incompréhensions vis-à-vis des autorités, ce qui a tendance à se répercuter sur la qualité des statistiques[214].

Pour y remédier, la LSF habilite l'OFS, à certaines conditions, à procéder à des appariements de données (art. 14*a* LSF)[215].

L'appariement de données est un traitement qui consiste à relier des données provenant de sources différentes, telles que les données d'enquêtes, données de registres, données administratives ou données de mesures, créant ainsi un nouveau jeu de données[216] sans avoir à effectuer de relevés – autrement dit, sans avoir à procéder à de nouvelles collectes de données (art. 13*h* et 13*i* al. 2 Ordonnance sur les relevés statistiques). En principe, chaque nouvelle exploitation d'un registre ou nouvelle réalisation d'une enquête en fait une nouvelle source de données[217].

Un « *appariement au sens de la statistique publique implique qu'au moins une des sources de données soit élaborée dans le cadre de la* [LSF] *et que l'appariement serve à remplir des tâches statistiques* »[218].

Les appariements visent ainsi la production d'informations nouvelles à partir de données existantes, tout en optimisant les ressources de l'État et allégeant la charge des milieux interrogés, en créant des synergies et en définissant des

214 OFS, Directives sur l'appariement, p. 7.
215 Voir concernant l'appariement de données, Annexe à la Recommandation n° R(97)18 du Comité des Ministres aux États membres, pt. 4.4.
216 Voir OFS, Directives sur l'appariement, p. 5 et 8.
217 Voir OFS, Directives sur l'appariement, p. 5 et 8.
218 Voir OFS, Directives sur l'appariement, p. 7.

sources de données élargies[219]. Ils contribuent ainsi à la concrétisation du principe de la collecte des données dans le cadre de la statistique fédérale consistant à limiter au strict nécessaire les relevés directs[220] (art. 4 LSF)[221].

b) Bases légales

L'art. 14*a* LFS est la base légale qui fonde l'OFS à procéder, dans le cadre de l'exécution de ses tâches, à l'appariement de données à des fins statistiques (art. 14*a* al. 1 LFS).

Cette habilitation d'ordre général est précisée par les dispositions d'exécution (voir art. 14*a* al. 1 *in fine* LSF)[222] qui figurent pour l'essentiel dans l'Ordonnance sur les relevés statistiques[223] et l'Ordonnance sur l'appariement de données[224]. Le dispositif est par ailleurs complété par les Directives de l'OFS sur l'appariement[225].

En outre, la loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes (LHR) prévoit explicitement la possibilité pour l'OFS d'apparier des données à des fins de statistiques tirées du Registre fédéral des bâtiments et des logements (RegBL) et du Registre des entreprises et des établissements (REE) et les conserver durablement (art. 16 al. 4 LHR).

L'appariement de données dans le cadre de la statistique publique est soumis à plusieurs conditions juridiques cumulatives.

c) Compétence

En règle générale, pour ce qui est de la statistique officielle fédérale, l'OFS est l'organe habilité à procéder à l'appariement de données (art. 14*a* al. 2 LSF). La LSF prévoit néanmoins une clause dérogatoire permettant aux services

219 Voir OFS, Directives sur l'appariement, p. 5.

220 Voir art. 4 al. 3 LSF. Le relevé direct (enquête) consiste à collecter à la source des données nouvelles. La collecte est effectuée en questionnant des personnes physiques ou morales, aux seules fins définies par la LSF.

221 La Confédération renonce à organiser des relevés pour la statistique fédérale (relevés directs, relevés indirects).

222 Le Conseil fédéral règle les modalités.

223 Voir en particulier les art. 8*a* et 13*h* ss Ordonnance sur les relevés statistiques. Voir ég., OFS Directives sur l'appariement, p. 7.

224 Ordonnance du Département fédéral de l'intérieur (DFI) concernant l'appariement de données statistiques du 17 décembre 2013 (Ordonnance sur l'appariement de données), RS 431.012.13.

225 OFS, Directives sur l'appariement.

cantonaux et communaux de statistique d'apparier les données de l'OFS avec d'autres données pour exécuter leurs tâches en matière de statistiques avec l'accord écrit et aux conditions édictées par l'OFS (art. 14*a* al. 2 LSF)[226]. Dans ce cadre, les services statistiques cantonaux et communaux impliqués doivent notamment satisfaire aux exigences posées à l'art. 5 de l'Ordonnance sur l'appariement de données lorsqu'ils font appel à des organismes et à des instituts de sondage privés pour exécuter des relevés.

L'OFS peut effectuer des appariements pour son propre compte ou pour celui de tiers et appuie en particulier les projets d'appariement de la Confédération et des cantons (art. 13*k* al. 1 Ordonnance sur les relevés statistiques).

L'OFS a la possibilité de procéder à des appariements pour le compte de tiers sur mandat à des fins ne se rapportant pas à des personnes, dans le cadre d'un contrat de protection des données et selon ses moyens techniques, organisationnels et humains (art. 13*k* al. 1 Ordonnance sur les relevés statistiques).

Enfin, pour des questions de réduction de coûts et de charge de travail « *d'autres tiers (mandants)* » peuvent être associés au processus d'appariement[227]. Le cas échéant, les détails de la collaboration, en particulier en ce qui a trait à la protection des données doivent être clairement définis dans un contrat (art. 13*k* al. 3 Ordonnance sur les relevés statistiques)[228]. Il s'agit d'un rappel des obligations incombant au responsable de traitement en cas de sous-traitance au sens des art. 9 LPD et 7 OPDo (voir en ce sens l'art. 5 Ordonnance sur les relevés statistiques relatif au recours à des organismes et à des instituts de sondage privés).

d) Critères

Les exigences juridiques en matière d'appariement de données se rapportent essentiellement à la finalité du traitement et à l'anonymisation des données personnelles.

En vertu de la réglementation fédérale, l'OFS ne peut recourir à l'appariement de données que dans le cadre de l'exécution de ses tâches, c'est-à-dire uniquement à des fins statistiques et à condition de rendre les données anonymes (art. 14*a* al. 1 LSF). La LSF tout comme la LPD ne précisent pas le moment auquel cette anonymisation devrait intervenir.

226 OFS, Directives sur l'appariement, p. 7.
227 OFS, Directives sur l'appariement, p. 7.
228 OFS, Directives sur l'appariement, p. 7.

Dans le cadre de son habilitation, l'OFS peut apparier aussi bien ses propres données que des données tierces (art. 13*j* al. 2 Ordonnance sur les relevés statistiques).

À l'instar de toute opération de traitement de données, les appariements doivent faire l'objet d'un examen sous l'angle de la proportionnalité, en particulier en ce qui concerne leur nécessité et leur caractère adapté aux travaux statistiques (art. 13*i* al. 2 Ordonnance sur les relevés statistiques) et présenter les caractéristiques et la qualité requises pour un traitement statistique (art. 13*j* al. 1 Ordonnance sur les relevés statistiques)[229].

L'OFS est tenu d'édicter un règlement de traitement qui précise les autres détails de la réalisation des appariements (voir art. 6 Ordonnance sur l'appariement de données et art. 13*b* Ordonnance sur les relevés statistiques). Les prescriptions de l'art. 6 OPDo doivent être respectées (voir art. 5 Ordonnance sur les relevés statistiques).

Lorsque des données personnelles sont traitées à des fins ne se rapportant pas à des personnes, en l'occurrence, la statistique, et que le traitement sert également une autre finalité, en principe l'appariement ne s'applique qu'au seul traitement effectué à des fins ne se rapportant pas à des personnes (voir art. 39 al. 2 LPD et 35 OPDo) (voir *supra* III.B).

Par souci de transparence, les statistiques qui donnent lieu à des appariements de données systématiques doivent être indiquées comme telles en annexe (art. 13*n* Ordonnance sur les relevés statistiques).

e) Exigences particulières relatives aux données sensibles ou permettant d'établir les caractéristiques essentielles d'une personne

Lorsque l'appariement porte sur des données personnelles sensibles ou permettant d'établir les caractéristiques essentielles d'une personne, la LSF prévoit une obligation d'effacer les données appariées « *une fois les travaux statistiques d'exploitation terminés* » (art. 14*a* al. 1 LSF).

Les autres données appariées peuvent être réutilisées pour des travaux statistiques ultérieurs (art. 14*a* al. 1 LSF).

Force est de constater que là encore le législateur ne donne pas plus d'indications sur le moment concret où l'effacement devrait intervenir ni ce qu'il faut entendre par fin des travaux d'exploitation.

229 Voir ég. OFS, Directives sur l'appariement, p. 7.

En termes de protection des données, l'appariement de données constitue une opération particulièrement sensible méritant une diligence accrue des responsables de traitement, en l'occurrence l'OFS et les partenaires associés.

V. Aspects importants

Compte tenu des considérations développées, il nous paraît opportun de présenter un bref récapitulatif des points déterminants à régler dans le cadre des traitements à des fins statistiques. Il sied de[230] :

- décrire dans les grandes lignes la situation initiale ainsi que le contexte du traitement ;
- déterminer la base légale applicable respectivement les bases légales applicables :
  - vérifier sa densité normative en ce qui concerne les organes fédéraux (voir *supra* III.C.2)
  - pour les responsables de traitement privés, vérifier si le traitement peut se fonder sur un des motifs justificatifs (art. 31 LPD, loi, consentement ou intérêt prépondérant)
- définir la finalité du traitement et délimiter son étendue ;
- désigner les autorités et personnes impliquées dans le traitement et déterminer clairement leur rôle (éventuel traitement conjoint ou sous-traitance)[231] ;
- définir les obligations et clarifier les responsabilités respectives par contrat ou convention (protection des données et obligation de garder le secret convention) ou émettre des instructions claires et prévoir éventuellement des peines conventionnelles en cas de non-respect ;
- prévoir un calendrier et fixer la durée de conservation des données personnelles ;
- en cas d'utilisation multiple, établir une distinction claire entre les traitements de données à des fins statistiques et les traitements à d'autres fins ;
- accorder une vigilance accrue aux appariements de données ;
- déterminer les conditions liées à la publication des statistiques/résultats de la recherche ;
- tenir compte des autres aspects spécifiques liés au type/contexte du traitement.

230 Voir ég. à ce sujet les points soulevés par KOÇ, N 30.29.
231 Voir au sujet de la sous-traitance MÉTILLE, Traitement de données, p. 19 ; ROSENTHAL, N 13 ss.

VI. Conclusion

En matière de traitement de données, plusieurs facteurs invitent à la réflexion. En effet, la variété des acteurs, l'ampleur et l'opacité de certains traitements, sans oublier le volume et la disponibilité globaux des données traitées dans le temps et dans l'espace ou encore la valeur économique qu'on leur accorde, invitent à la réflexion.

À noter que l'anonymisation et la réidentification sont des domaines de recherche très dynamiques faisant régulièrement l'objet de nouvelles avancées[232] occasionnant ainsi une dépréciation des outils utilisés. À cela s'ajoute, le fait que des données anonymisées, comme les statistiques, peuvent servir à étoffer des profils existants, surtout à l'échelle d'un pays comme la Suisse, créant ainsi de nouveaux défis en termes de protection des données[233].

Compte tenu de ce qui précède, des données considérées aujourd'hui comme anonymes ne le seront peut-être plus à l'avenir. L'anonymisation – du moins en ce qui concerne l'anonymisation irréversible – nous paraît en effet de plus en plus illusoire.

Quoiqu'il en soit, lorsque les personnes concernées sont identifiables, la LPD est applicable.

Pour appréhender ces défis, la LPD – en tant que loi-cadre énonçant les notions fondamentales et les principes généraux de la protection des données, et donc d'une certaine souplesse – doit être considérée comme un « *instrument juridique vivant* » à interpréter selon une approche systématique du droit, en tenant compte de ses objectifs (art. 1er LPD) et des évolutions technologiques.

Enfin, au regard du contexte actuel, nous sommes d'avis que compte tenu de leur importance, de la technicité de la matière et de l'ampleur qu'il prendront probablement dans le cadre des transformations numériques en cours[234], les traitements de données à des fins de statistiques nécessitent un accompagnement important. Dès lors, il aurait été judicieux d'attribuer des ressources plus importantes au PFPDT pour lui permettre d'accomplir de manière plus effective sa mission notamment d'accompagnement et de conseil aux différents acteurs – organes fédéraux comme personnes privées.

---

232 GROUPE 29, Avis 05/2014 sur les techniques d'anonymisation, p. 3.

233 Voir au sujet des risques de réidentification, GROUPE 29, Avis 05/2014 sur les techniques d'anonymisation, p. 3.

234 Voir Stratégie suisse de cyberadministration 2020–2023, Voir Message de loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (LMETA), disponible à : <https://www.newsd.admin.ch/newsd/message/attachments/70501.pdf>.

VII. Bibliographie

A. Littérature

Jan Philipp Albrecht/Florian Jotzo, Das neue Datenschutzrecht der EU, Baden-Baden 2017 ; **Jean-François Aubert/Pascal Mahon**, Petit Commentaire de la Constitution fédérale de la Condédération Suisse, Zurich/Bâle/Genève 2003 (cité PC Cst-Auteur, Art. X, N Y) ; **Bruno Baeriswyl/Kurt Pärli (éds)**, Datenschutzgesetz (DSG), Stämpflis Handkommentar, Berne 2015 ; **Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (éds)**, Datenschutzgesetz (DSG), Stämpflis Handkommentar, Berne 2023 ; **Charlotte Beck**, Cookies walls : Le consentement jugé invalide si l'alternative payante offre plus de contenu, swissprivacy.law (<https://swissprivacy.law/215>) ; **Eva Maria Belser/Astrid Epiney/Bernard Waldmann**, Datenschutzrecht. Grundlagen und öffentliches Recht, Berne 2011 ; **Philippe Meier/Sylvain Métille (éds)**, Loi sur la protection des données, Commentaire romand, Bâle 2023 (cité : CR LPD-Auteur, art. X, N Y) ; **Bertil Cottier**, L'ère numérique et le principe de légalité – Frictions et possibilités d'adaptation, *in* Astrid Epiney/Déborah Sangsue (éds), L'ère numérique et la protection de la sphère privée – L'impact des principes juridiques « traditionnels » : analyse et perspectives, Zurich 2018, p. 25 ss ; **Cécile de Terwangne**, La nouvelle loi suisse de protection de données dans le contexte international (Convention 108+ et RGPD), *in* Astrid Epiney/Sophia Rovelli (éds), La révision de la Loi fédérale sur la protection des données, Zurich/Bâle/Genève 2022 ; **Cécile de Terwangne**, Les principes relatifs au traitement des données à caractère personnel et à sa licéité, *in* Cécile de Terwangne/Karen Rosier (éds), Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie, Bruxelles 2018 ; **Bernard Ehrenzeller/Benjamin Schindler/Rainer J. Schweizer/Klaus A. Vallender (éds)**, Die schweizerische Bundesverfassung, St. Galler Kommentar, Zurich 2014 (cité : SGK BV-Auteur, Art. X, N Y) ; **Frédéric Erard/Mathilde Heusghem/Clément Parisato**, Recherche biomédicale et Open Data. Perspectives en droit suisse, Jusletter 30 janvier 2023 ; **Livio Di Tria/Kastriot Lushbitani**, Étude empirique du droit d'accès à ses données personnelles, *in* : Sylvain Métille (éd.), Le droit d'accès, Berne 2021, p. 29 ss ; **Alexandre Jotterand**, Des données personnelles pseudonymisées transférées à un tiers deviennent-elles anonymes ?, swissprivacy.law (<https://swissprivacy.law/232/>) ; **Alexandre Jotterand**, Personal Data or Anonymous Data : where to draw the line (and why)?, Jusletter 15 août 2022 ; **Alexandre Jotterand/Frédéric Erard,** Recherche sur l'être humain et données personnelles. Gestion des échanges et répartition des responsabilités, Jusletter 30 août 2021 ; **Karin Koç**, Datenschutz in Statistik und Forschung, *in* Nicolas Passadelis/David Rosenthal/Hanspeter Thür (éds), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung, Bâle 2015 ; **Jürgen Kühling/Benedikt Buchner (éds)**, Datenschutz-Grundverordnung, BDSG, Kommentar, 3e éd., Munich 2020 (cité : Kommentar DSGVO-BDSG-Auteur, Art. X, N Y) ; **Christopher Kuner/Lee A. Bygrave/Christopher Docksey (éds)**, The EU General Data Protection Regulation (GDPR): A Commentary, Oxford 2020 (cité : GDPR Commentary-Auteur, Art. X, N Y) ; **Peter Kuratli**, Die öffentliche Statistik im Recht – Zugleich ein Beitrag zur Bedeutung von statistisch-ethischen Regelwerken, thèse Bâle, Zürich 2017 ; **Vincent Martenet/Jacques Dubey (éds)**, Constitution fédérale I : Préambule-Art. 80, Commentaire romand, Berne 2021 (cité : CR Cst-Auteur, art. X, N Y) ; **Urs Maurer-Lambrou/Gabor-Paul Blechta (éds)**, Datenschutzgesetz, Öffentlichkeitgesetz, Basler Kommentar, Bâle 2014 (cité : BSK DSG-Auteur, Art. X, N Y) ; **Philippe Meier**, Protection des données. Fondements, principes généraux et droit privé, Berne 2011 ;

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 (cité : MÉTILLE, Traitement de données) ; **Sylvain MÉTILLE/Annelise ACKERMANN**, RGPD : application territoriale et extraterritoriale , *in* Astrid Epiney/Sophia Rovelli (éds), Le Règlement général sur la protection des données (RGPD) : portée et premières expériences, Zurich/Bâle/Genève 2020, p. 77 ss ; **Boris P. PAAL/Daniel A. PAULY**, Datenschutzgrundverordnung – Bundesdatenschutzgesetz, Beck'sche Kompakt-Kommentare, 3e éd., Munich 2021 (cité : Beck'sche Kompalt-Kommentare DSGVO-AUTEUR, Art. X, N Y) ; **Bruno PASQUIER/Marilyne PASQUIER**, États locatifs, outil statistique et protection des données, Revue de l'avocat 2020, p. 472 ss ; **Samah POSSE**, Collecte et conservation des données relatives aux pratiques sexuelles d'un donneur de sang potentiel en violation de la CEDH, swissprivacy.law, (<www.swissprivacy.law/207>) ; **David ROSENTHAL/Yvonne JÖHRI**, Handkommentar zum Datenschutzgesetz. Sowie weiteren, ausgewählten Bestimmungen, Zurich/Bâle/Genève 2008 (cité : Handkommentar DSG-AUTEUR, art. X, N Y) ; **DAVID ROSENTHAL/Samira STUDER/Alexandre LOMBARD** (pour la traduction), La nouvelle loi sur la protection des données, Jusletter 16 novembre 2020 (https://jusletter.weblaw.ch/fr/juslissues/2020/1045/das-neue-datenschutz_0e89d89706.html__ONCE, consulté le 30 janvier 2023) (cité : ROSENTHAL) ; **Olivia TAMBOU**, Manuel de droit européen de la protection des données à caractère personnel, Bruxelles 2020 ; **Jean-Philippe WALTER**, La protection de la personnalité lors du traitement de données à des fins statistiques : en particulier, la statistique officielle fédérale et la protection des données personnelles, thèse Fribourg 1988.

B. Documents officiels

Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, Manuel de droit européen en matière de protection des données, Édition 2018, Luxembourg 2019 ; **Conseil de l'Europe**, Projet de rapport explicatif. Convention 108 modernisée (<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000016806b6ec3>) ; **Conseil de l'Europe**, Rapport explicatif. Convention 108 modernisée (<https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726>) ; **Conseil de l'Europe**, Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981 ; **Conseil de l'Europe**, Recommandation No R (97) 18 du Comité des Ministres aux États membres concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques (cité : Recommandation N No R (97) 18) ; **Conseil fédéral**, Message relatif à une nouvelle constitution fédérale du 20 novembre 1996, FF 1997 I 1(cité : Message Cst.) ; **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, FF 2017 6565 (cité : Message LPD 2017) ; **Conseil fédéral**, Message relatif à la révision de la loi fédérale sur la protection des données (LPD) et à l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données, FF 2003 1915 (cité : Message Révision aLPD) ; **Conseil fédéral**, Message concernant la loi fédérale sur la protection des données du 23 mars 1988, FF 1988 II 421 (cité : Message aLPD) ; **Conseil fédéral**, Message concernant la loi sur la statistique fédérale du 30 octobre 1991, FF 1992 I 353 (cité : Message LSF) ; **Commission nationale informatique & libertés**

(CNIL), Guide pratique. Les durées de conservation (<https://www.cnil.fr/sites/cnil/files/atoms/files/guide_durees_de_conservation.pdf>) ; **Groupe de travail « Article 29 » sur la protection des données**, Avis 05/2014 sur les techniques d'anonymisation, adopté le 10 avril 2014, 0829/14/FR, WP216 ; **Groupe de travail interdépartemental « Intelligence artificielle »**, Rapport « Défis de l'intelligence artificielle » au Conseil fédéral, 13 décembre 2019 ; **Office fédéral de la justice (OFJ),** Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales du 21 décembre 2016 (cité : Rapport explicatif LPD) ; **Office fédéral de la justice (OFJ)**, Révision totale de l'ordonnance relative à la loi fédérale sur la protection des données. Rapport explicatif relatif à la procédure de consultation (cité : Rapport P-OLPD) ; **Office fédéral de la statistique (OFS)**, Marco D'Angelo, Directives sur l'appariement., 05.03.2020 ; **Office fédéral de la statistique (OFS),** Nouveau Règlement général de la protection des données (RGPD) de l'Union européenne : Ses effets sur la statistique publique suisse, 2019 (cité : RGPD : Ses effets sur la statistique publique suisse) <https://www.bfs.admin.ch/asset/fr/9146871> ; **Préposé fédéral à la protection des données et à la transparence (PFPDT)**, Le RGPD et ses conséquences sur la Suisse, juillet 2018 (<https://www.edoeb.admin.ch/dam/edoeb/fr/Dokumente/deredoeb/Le%20RGPD%20et%20ses%20conséquences%20sur%20la%20Suisse_FR.pdf.download.pdf/Le%20RGPD%20et%20ses%20conséquences%20sur%20la%20Suisse_FR.pdf>) ; **Préposé fédéral à la protection des données et à la transparence (PFPDT)**, 29e Rapport d'activités 2021/2022 ; **Préposé fédéral à la protection des données et à la transparence (PFPDT)**, 30e Rapport d'activités 2022/23.

La protection des données personnelles et la valorisation des données de recherche

Au sein des institutions de recherche en Suisse

VALENTIN CONRAD
Juriste

TANIA GERMOND*
Avocate

Table des matières

I. Qu'entend-on par valorisation des données de recherche ?

Comme la société dans son ensemble, les institutions suisses de recherche exploitent les outils numériques depuis plusieurs années et la numérisation de leurs activités quotidiennes produit de nombreuses données au format numérique[1].

Mais de quelles données de recherche parle-t-on ? La notion de données n'est pas clairement définie par les différentes parties prenantes[2] ni par un texte légal suisse. Elle se veut donc un terme polysémique regroupant plusieurs genres de données : données brutes générées par un chercheur, les métadonnées[3], données institutionnelles, mais aussi les données personnelles obtenues lors d'un projet de recherche. Deux auteurs définissent les données de recherche comme des

* Nous remercions Prof. Sylvain Métille, M. Enzo Bastian, et M. Quentin Jacquemin pour leur aide précieuse.

1 Dans le monde, le volume de données produit passera probablement de 33 zettabytes (=33 x 1021 bytes) en 2018 à 175 zettabytes en 2025 (*cf.* REINSEL/GANTZ/RYDNING, p. 3-6).

2 Déclaration de Berlin sur le Libre Accès à la Connaissance en Sciences exactes, Sciences de la vie, Sciences humaines et sociales du 22 octobre 2003

3 Les métadonnées sont des informations sur des données. Ce sont des informations structurées ou semi-structurées, qui permettent la création, la gestion et l'utilisation de documents d'activités dans le temps, au sein de divers domaines et entre ces domaines (*cf.* ISO 15489-1:2016).

données qui, selon le contexte spécifique, font l'objet d'un processus de recherche, découlent d'un processus de recherche ou en sont le résultat[4]. L'on peut par ailleurs se référer à l'article 2 du nouveau Règlement sur la gouvernance des données européen[5] qui constitue une nouveauté en la matière dès son entrée en application le 24 septembre 2023 et qui définit la notion de « données » comme « toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels » et qui inclut les données personnelles au sens de l'article 4, point 1 du Règlement général sur la protection des données[6] et les données non personnelles au sens du même Règlement.

L'existence de cet amas de données hétéroclites serait vaine si elles n'étaient pas utilisées. En les consolidant, structurant, documentant, et en les rendant accessibles au public, celles-ci deviennent lisibles et permettent de servir les objectifs fixés par ces institutions, mais aussi par la Suisse dans son ensemble. En effet, la diffusion des données de recherche répond à des enjeux économiques et sociétaux primordiaux.

Pour ces raisons, l'une des missions des institutions suisses de recherche consiste à valoriser les résultats de leurs recherches, à savoir les données de recherche[7]. Même si la question de la valorisation n'est pas nouvelle, dans le contexte de la société de la connaissance et d'une concurrence mondiale du savoir, la question de la valorisation de la recherche devient de plus en plus stratégique.

Cette mission pose des défis aux institutions de recherche et à leurs chercheurs, notamment dans le domaine de la protection des données personnelles. La présente contribution a pour but d'énumérer une casuistique non exhaustive de valorisation de données intrinsèque aux institutions de recherche et les contraintes juridiques qu'elle soulève d'un point de vue de la protection des données.

Avant de développer ces exemples de valorisation, nous souhaitons définir la notion de valorisation.

Au sens commun du terme, selon le Larousse, valoriser signifie « *donner, faire prendre de la valeur à quelque chose* » ou encore « *donner une importance accrue à quelque chose, le mettre en valeur* ». En d'autres termes, la valorisation consiste en « *l'action de donner de la valeur, plus de valeur à quelque chose ou quelqu'un, au fait d'être valorisé* » selon le Larousse. Par valeur, on entend mettre

4 KINDLING/SCHIRMBACHER, p. 127-136.
5 COM/2020/767 final.
6 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 (Règlement général sur la protection des données, RGPD).
7 Art. 2 al. 1 let. f de la loi fédérale sur les écoles polytechniques fédérales du 4 octobre 1991 ; FF 2002 3251, p. 3260.

en valeur au sens de mettre en lumière, diffuser, donner plus d'importance, mais également au sens de donner plus de valeur, sans préciser ici dans quelle unité cette valeur pourrait être mesurée.

Dans le contexte de la recherche scientifique, la valorisation des résultats de la recherche correspond à favoriser le transfert de savoirs et de technologie de la science à l'économie, mais aussi entre chercheurs[8]. Ce transfert débouche sur le développement de nouveaux produits et services ou de nouvelles recherches, pour le plus grand bien de l'ensemble de la société. La valorisation correspond ainsi aux moyens de « *rendre utilisables ou commercialisables les résultats, les connaissances et les compétences de la recherche* »[9]. Elle concerne les relations entre les acteurs de la recherche et le monde économique. La valorisation suppose ainsi une mise en relation du monde de la recherche et du monde socio-économique. Elle n'est pas un processus automatique : elle doit être organisée et faire l'objet d'actions concertées et réfléchies. Cette conception de la valorisation de la recherche comprend la diffusion à titre gratuit, mais également à titre onéreux des résultats de la recherche ainsi que la mise en valeur des chercheurs et de leur institution.

Nous ne traiterons pas dans cet article de la valorisation des biens immatériels dans le cadre de la recherche qui ressortit davantage au domaine de la propriété intellectuelle.

Nous allons aborder quatre principales formes de valorisation des données de recherche : la première résulte de l'attrait pour les données personnelles dans le domaine de l'intelligence artificielle ; la seconde sert des politiques de gouvernance ; la troisième poursuit l'objectif d'une science ouverte ; et la dernière cherche à favoriser l'accessibilité des données de santé pour mettre en œuvre une médecine personnalisée et une santé personnalisée. Cette liste n'est pas exhaustive, mais ces quatre expressions de valorisation nous semblaient les plus importantes sous l'angle de la protection des données personnelles. Nous traiterons dans les sections suivantes de ces quatre formes de valorisation en les détaillant, puis en les confrontant avec le droit suisse de la protection des données personnelles. Nous limiterons notre analyse à la nouvelle loi fédérale sur la protection des données personnelles du 25 septembre 2020 (ci-après « LPD »)[10], même s'il eût été intéressant de considérer aussi certaines lois cantonales[11]. Nous traiterons tout de même très brièvement des dispositions de la Loi fédérale sur la recherche sur l'être humain du 30 septembre 2011 et ses

8 FF 2002 3251, p. 3260.

9 COLLIN-LACHAUD/MICHEL, n. 11.

10 Loi fédérale sur la protection des données (LPD) du 25 septembre 2020, entrée en vigueur le 1er septembre 2023, RS 235.1.

11 Hélas, les projets de loi cantonale vaudoise et genevoise ne sont soit pas encore connus soit pas encore définitifs.

ordonnances (ci-après « LRH »[12]) qui trouveraient à s'appliquer dans la partie consacrée à l'accessibilité des données de santé. Évidemment, cette contribution est destinée à un public déjà averti, car nous évitons volontairement de rappeler certaines définitions qui devraient être plus ou moins connues afin de limiter la longueur de ce texte. L'exercice est également délicat tant le sujet est vaste. Ce travail a donc surtout vocation à susciter le débat et à offrir un panorama subjectif de problématiques qu'un praticien, qui travaille dans le secteur de la recherche, pourrait rencontrer.

II. Une valorisation au travers de l'intelligence artificielle et de la gouvernance institutionnelle

En premier lieu, les données de recherche ont pris de la valeur en raison de leur utilisation dans le domaine de l'intelligence artificielle – elles sont une source indispensable à l'entraînement d'algorithmes, mais aussi grâce à leur utilisation dans la gouvernance des institutions de recherche, constituant ainsi une aide précieuse dans la prise de décision au sein des directions des institutions de recherche. Nous traitons ces deux stratégies dans la même partie, car, selon nous, ces deux stratégies posent des problèmes similaires en matière de réutilisation de données personnelles, comme nous l'expliquerons plus loin.

A. Un besoin accru de données pour développer l'intelligence artificielle

Pour l'Union européenne, l'intelligence artificielle représente le moyen de devenir leader dans l'économie des données et de ses applications. L'Union européenne définirait l'intelligence artificielle comme un logiciel qui est développé au moyen d'une ou plusieurs techniques ou approches et qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit[13]. La Suisse aussi entend utiliser l'intelligence artificielle comme outil essentiel à la productivité économique[14]. Le domaine des écoles polytechniques fédérales a également pour

12 Loi fédérale relative à la recherche sur l'être humain (Loi relative à la recherche sur l'être humain, LRH) du 30 septembre 2011, RS 810.30.

13 COM(2021) 206 final, Art. 3 ch. 1.

14 Stratégie Suisse numérique, Données, contenus numériques et intelligence artificielle : <https://digital.swiss/fr/strategie/strategie-suisse-numerique.html>.

objectif d'accompagner la transition numérique de la société grâce notamment à l'intelligence artificielle[15].

Même si la définition choisie par l'Union Européenne est sujette à caution[16], il semble suffisant de retenir que l'intelligence artificielle désigne une automatisation des fonctions cognitives, pour percevoir, raisonner, apprendre, agir et interagir[17]. Or, l'intelligence artificielle repose et fonctionne sur la base de données et d'algorithmes[18]. Pour pouvoir entraîner des algorithmes afin de les améliorer, des collectes de données – souvent personnelles – s'avèrent nécessaires. Les systèmes d'intelligence artificielle posent évidemment certains risques en matière de protection des données personnelles[19].

De nombreux chercheurs conçoivent des technologies d'intelligence artificielle. Ils sont invités à suivre les différents guides éthiques lors de la phase de conception de ces systèmes[20], lesquels suggèrent de protéger le droit au respect de la vie privée. Les chercheurs sont surtout extrêmement demandeurs pour obtenir des données personnelles qui seront utilisées pour l'apprentissage de leurs algorithmes. Souvent, la première question qui se pose en relation avec l'acquisition de données personnelles est celle de la réutilisation légitime des données personnelles ainsi convoitées pour la création ou l'amélioration de ces technologies. Il sied évidemment de vérifier dans quelles conditions ces données ont été collectées pour s'assurer que leur réutilisation soit juridiquement envisageable. Nous nous focaliserons exclusivement sur cette question dans la section *infra* C lorsque nous traiterons du cadre juridique applicable en Suisse à la réutilisation de données personnelles. Pour revenir au propos de notre article consacré à la valorisation des données de la recherche, nous allons dans la partie suivante nous intéresser à une autre stratégie de valorisation qui pose, elle aussi, des questions en matière de réutilisation de données personnelles.

15 CEPF, Strategic Plan 2025–2028, p. 21.

16 ZANOL/BUCHELT/TJOA/KIESEBERG, n. 7 ; SEFRI, Rapport du groupe de travail interdépartemental « Intelligence artificielle », p. 18 ss.

17 BRAUNSCHWEIG/GHALLAB, p. 2.

18 GASSER/ALMEIDA, p. 61 ; COM(2021) 206 final, p. 7, n. 2.2 ; Stratégie Suisse numérique, Données, contenus numériques et intelligence artificielle : <https://digital.swiss/fr/strategie/strategie-suisse-numerique.html> ; SEFRI, Rapport du groupe de travail interdépartemental « Intelligence artificielle », p. 18.

19 CE, White paper on artificial intelligence, p. 11.

20 Citons p. ex. UNESCO, Recommandation sur l'éthique de l'intelligence artificielle ; BAAI, Beijing AI Principles ; CE, Lignes directrices en matière d'éthique pour une IA digne de confiance.

B. Un besoin accru de données en matière de gouvernance institutionnelle

1. La construction d'une réputation grâce aux classements internationaux

Pour les institutions de recherche, certains indicateurs servent de points de comparaison entre universités lors de classements internationaux tels que les classements de *QS Quacquarelli Symonds* (Grande-Bretagne), *Academic Ranking of World Universities* (ARWU) de *ShanghaiRanking Consultancy* (Chine), ou *Times Higher Education* (THE) de l'entité du même nom (Grande-Bretagne). Les comparaisons entre universités existent depuis longtemps, au moins depuis les années soixante[21]. Au fil des décennies, les services d'éducation ont été soumis à une forte compétitivité mondiale[22]. Pour se démarquer de la concurrence et attirer des professeurs renommés, des étudiants à haut potentiel, ainsi que de générer de nouveaux financements, les classements internationaux sont devenus incontournables[23].

Évidemment, ces classements ne sont pas exempts de tout reproche quant à leur méthodologie de classement[24], mais constituent néanmoins des bases de comparaison intéressantes notamment pour construire une réputation[25]. Aussi, ces différents classements internationaux ont besoin pour fonctionner de données fiables. La collecte de données s'effectue au travers de bases de données, de sondages, de données publiques (l'attribution de prix), ou encore grâce à des données délivrées par les universités elles-mêmes[26]. En général, ces données ne devraient pas contenir de données personnelles. Si elles en contiennent, ces instituts proposant un classement, ou les institutions fournissant ces données, devront s'enquérir de la licéité d'une telle utilisation (au travers de sondages), réutilisation ou publication. Puisque ces instituts de classement ne sont pas des institutions de recherche, nous ne nous intéresserons pas au régime juridique applicable à l'organisation des sondages par ces derniers. Pour le reste, nous renvoyons la section consacrée à la réutilisation des données personnelles (*cf. infra* II.,C.).

---

21 AMSLER/BOLSMANN, p. 283-301.
22 LYNCH, p. 190-207.
23 KINZELBACH/SALIBA/SPANNAGEL, p. 3 & 7 ; LYNCH, p. 190-207 ; JÖNS/HOYLER, p. 45-59.
24 KINZELBACH/SALIBA/SPANNAGEL, p. 6. Pour un aperçu des méthodologies utilisées : <https://www.universityrankings.ch/fr/methodology>.
25 KINZELBACH/SALIBA/SPANNAGEL, p. 7.
26 <https://www.shanghairanking.com/methodology/gras/2021> ; <https://www.timeshighereducation.com/world-university-rankings/world-reputation-rankings-2022-methodology> ; <https://www.topuniversities.com/qs-world-university-rankings/methodology> ; <https://www.leidenranking.com/information/data>.

2. Pilotage chiffré des institutions de recherche

La transformation numérique engendre une production massive de données qui permet de mettre en œuvre et évaluer des politiques publiques[27]. À une autre échelle – celle des universités – de nombreuses données sont utilisées à des fins de gouvernance et de statistiques et permettent d'obtenir une photographie de la situation dans certains domaines. Ces données collectées à l'interne d'une université sont appelées « données institutionnelles ». Ces données ont une grande valeur pour les décideurs car elles permettent d'analyser une situation, d'évaluer les résultats d'une action, de développer leur stratégie et de prendre des décisions. Ces données institutionnelles permettent de quantifier certaines activités liées à la recherche comme le nombre de dépôts de brevet, des mesures bibliométriques, le nombre de publications, le nombre de *start-ups* créées, ou des chiffres sur l'employabilité des étudiants, *etc*.[28].

Ces activités pourraient parfois poser des problèmes en matière de protection des données personnelles. Par exemple, l'on peut imaginer une volonté d'utiliser certaines bases de données existantes pour les recouper avec d'autres et ainsi générer des informations supplémentaires, voire simplement de les réutiliser dans un autre but. Ce recoupage d'informations n'était pas forcément reconnaissable pour les personnes concernées au moment de la création de la base de données originale. De plus, certaines données collectées dans un certain contexte par une unité administrative (ou par un service) peuvent être transmises à d'autres unités (ou services) à l'interne d'une institution, posant souvent des complications pour respecter les principes de finalité, de sécurité ou de proportionnalité.

En imaginant un exemple fictif inspiré par des chercheurs italiens[29], il est concevable qu'une institution souhaitant inviter ses collaborateurs lors de conférences scientifiques utilise des données personnelles sur leurs centres d'intérêt et leur profil professionnel afin d'augmenter la participation à ces événements en profitant des services d'un célèbre réseau social professionnel. En souhaitant recouper des données personnelles déjà existantes, voire publiques, l'institution devra se questionner sur la légalité d'une telle réutilisation. Dans la prochaine section, nous nous intéresserons dès lors au cadre juridique applicable en Suisse lorsque l'on souhaite réutiliser certaines données à une autre fin que celle communiquée aux personnes concernées lors de la création de la base de données originale. En d'autres termes, nous allons nous intéresser brièvement à la réutilisation secondaire (*further-use*) de données personnelles. Nous aborderons au surplus l'utilisation de données personnelles déjà publiées et donc accessibles au public.

27 PUGIN, p. 7.
28 EPFL in figures 2021.
29 LOPS/SEMERARO/DE GEMMIS/NARDUCCI.

C. La réutilisation des données personnelles dans le secteur de la recherche

1. Introduction

Que ce soit lors d'acquisition de données pour perfectionner un système d'intelligence artificielle ou lors de l'utilisation de données institutionnelles pour servir le pilotage d'une institution de recherche voire pour les fournir à des instituts de classement (*cf. supra* II., A. & B.), le gestionnaire de projet, le membre d'une direction ou le chercheur devra s'assurer de la licéité de réutiliser les données personnelles en question.

Pour reprendre le canevas d'analyse proposé par ROSENTHAL[30], il faudrait tout d'abord vérifier l'existence d'une loi spéciale qui primerait sur la LPD. Comme évoqué en introduction, il est envisageable que la LRH puisse s'appliquer à une réutilisation de données de santé (*cf. infra* IV.). Ensuite, la réutilisation des données personnelles doit être conforme à la loi applicable et respecter les principes généraux en protection des données personnelles, même si certaines dérogations sont parfois possibles. Enfin, la réutilisation des données personnelles peut être proscrite pour d'autres motifs (en raison d'une obligation contractuelle ou d'une obligation légale par exemple).

Nous nous limiterons ci-après à évoquer les fondements du traitement de données personnelles selon que le responsable du traitement est un organe fédéral ou une personne privée et à décrire quelques principes généraux en protection des données qui nous semblent pertinents à développer dans le cadre des hypothèses de valorisation des données sélectionnées[31]. Nous mettrons aussi en exergue les possibles exceptions qui trouveraient à s'appliquer dans le domaine de la recherche et terminerons cette section sur les cas particuliers de l'utilisation de données personnelles accessibles au public et à la communication de données personnelles à l'étranger.

2. Base de légitimité

En Suisse, les personnes privées n'ont nul besoin de s'appuyer sur une base de légitimité pour fonder leur traitement de données personnelles[32], a fortiori si elles souhaitent réutiliser des données personnelles. Une personne privée doit toutefois justifier un traitement de données qui causerait une atteinte

30 ROSENTHAL.

31 Pour un bon résumé des différents principes applicable à la nouvelle loi fédérale sur la protection des données personnelles, voir MÉTILLE, p. 10.

32 ROSENTHAL/STUDER/LOMBARD (pour la traduction), p. 5, n. 8.

à la personnalité de la personne concernée (art. 31 LPD). Il est présumé qu'une violation des principes de protection des données (art. 6 et 8 LPD), qu'un traitement de données personnelles contre la manifestation expresse de la personne, ou qu'une communication de données personnelles sensibles à un tiers cause irréfragablement une atteinte (art. 30 al. 2 LPD). Conformément à la pratique du Tribunal fédéral, une justification du traitement de données personnelles contraire aux principes généraux en protection des données n'est ainsi pas exclue, mais les motifs justificatifs ne peuvent être affirmés qu'avec une grande réserve dans un cas concret[33].

Quant aux organes fédéraux, le principe de la légalité s'applique. Il concrétise à la fois l'art. 36 al. 1 1re phr. Cst.[34] prévoyant qu'une restriction à un droit fondamental doit reposer sur une base légale, et l'art. 5 al. 1 Cst. consacrant le principe de la légalité[35].Ce principe requiert l'existence d'une base légale au sens matériel (art. 34 al. 1 LPD) ou une base légale au sens formel si le traitement concerne des données sensibles[36] pour pouvoir traiter des données personnelles. Cette exigence s'applique à toutes les phases du traitement[37]. La loi doit avoir une densité normative suffisante et prévoir, par exemple, le contenu des données sensibles récoltées et doit contenir une identification au moins schématique des finalités du traitement des diverses données sensibles, ce qui doit être reconnaissable pour la personne concernée[38]. Certaines exceptions à l'exigence d'une loi au sens formel existent dans la LPD mais leurs conditions d'application sont strictes et ne dispensent pas d'une base légale en tant que telle[39].

Dans les deux cas, la loi prévoit une exception aux exigences précitées si le but du traitement de données personnelles ne s'intéresse pas à l'identité des personnes en tant que telle[40], mais plutôt à une masse d'individus. Dans ce cas, un tel traitement serait moins dangereux pour la personne concernée[41] ce qui justifie d'alléger les obligations du responsable du traitement. En général, c'est le cas pour la recherche scientifique. Pour les personnes privées, moyennant le respect des conditions inscrites à l'art. 31 al. 2 lit. e LPD, une atteinte à la personnalité serait justifiée lorsque cette atteinte est nécessaire pour mener la recherche envisagée. Concernant les organes fédéraux, et sous réserve du respect des conditions fixées à l'art. 39 al. 1 LPD, un allègement du principe de légalité est possible pour justifier un traitement de données personnelles et une exonération

33 ATF 138 II 346, c. 7 ; ATF 136 II 508, c. 5.2.4.
34 Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101.
35 CR LPD-Epiney/Posse, art. 34, N 3.
36 ATF 131 II 413, c. 2.3 et 2.5 ; art. 34 al. 2 LPD.
37 HK DSG-Rosenthal/Jöhri, art. 17, N 2.
38 ATF 137 I 167, c. 9.1.1 ; CR LPD-Epiney/Posse, art. 34, N 35 ss.
39 CR LPD-Epiney/Posse, art. 34, N 57 ss.
40 <https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/forschung_statistik/forschung.html> ; Koç, N 30.10.
41 FF 1988 II 421, p. 479.

du principe de finalité et du principe de légalité pour la communication des données à un tiers est prévue (art. 39 al. 2 LPD). En définitive, même si la LPD permet une certaine souplesse pour motiver une réutilisation de données à des fins de recherche, il n'en demeure pas moins que le respect des principes généraux en protection des données doit être garanti et l'exigence d'une base légale pour les organes fédéraux restent applicable[42]. Ainsi, nous traiterons ci-après de quelques principes généraux auxquels il faut prêter une attention particulière lorsqu'une réutilisation de données personnelles est planifiée.

3. Conformité avec le principe de finalité

La réutilisation de données personnelles est intimement liée au respect du principe de finalité. L'art. 5 al. 4 de la Convention 108+[43] précise que les données personnelles doivent être traitées pour des finalités explicites, déterminées et légitimes et toujours de manière compatible avec la finalité initiale. Généralement, le but selon lequel les données seront utilisées doit avoir été indiqué au moment où les données ont été obtenues ou être autrement obtenu par la personne concernée[44].

La LPD concrétise ce principe à l'art. 6 al. 3, en précisant que les données personnelles doivent être traitées ultérieurement de manière compatible avec ces finalités.

La notion d'utilisation « compatible » signifie ne pas « *nuire à la transparence, à la sécurité juridique, à la prédictibilité ou à la loyauté du traitement de données* »[45]. La personne concernée doit pouvoir s'attendre à une réutilisation ultérieure de ces données personnelles dans ce nouveau but et cette réutilisation doit lui apparaître comme acceptable[46]. Dans le domaine de la recherche scientifique, la réutilisation de données personnelles est, *a priori*, jugée compatible avec la finalité initiale pour autant que certaines mesures techniques et organisationnelles aient été prises[47].

D'ailleurs, la LPD consacre cette exception à l'art. 31 al. 2 lit. e pour les personnes privées et l'art. 39 al. 2 pour les organes fédéraux.

---

42 CR LPD-EPINEY/POSSE, art. 34, N 6 ss.

43 Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

44 EPINEY, p. 538 ss.

45 Conseil de l'Europe, Rapport explicatif de la Convention 108+, n. 49.

46 Conseil de l'Europe, Rapport explicatif de la Convention 108+, n. 49.

47 Conseil de l'Europe, Rapport explicatif de la Convention 108+, n. 50.

a) Personnes privées

En ce qui concerne les personnes privées, si le traitement de données personnelles envisagé viole le principe de finalité, une atteinte à la personnalité de la personne concernée est consommée (art. 30 al. 2 lit. a LPD). Comme énoncé précédemment (*cf. supra* II., C., 2.), cette atteinte peut néanmoins être justifiée par un intérêt privé prépondérant notamment lorsque les données personnelles sont traitées à des fins ne se rapportant pas à des personnes, ce qui est le cas généralement pour des buts de recherche (art. 31 al. 1 et al. 2 lit. e LPD).

Pour être licite, le responsable du traitement devra anonymiser les données personnelles dès que possible ou les pseudonymiser si une telle anonymisation est impossible[48] ; ne transmettre des données personnelles sensibles à des tiers que sous une forme ne permettant pas l'identification de la personne concernée ou, si cela est impossible, d'exiger de ce tiers une utilisation non personnelle des données concernées ; et de publier uniquement les données personnelles sous une forme anonymisée (art. 31 al. 2 lit. e LPD).

b) Organes fédéraux

L'art. 39 LPD prévoit un régime juridique moins sévère pour des traitements de données personnelles effectués par des organes fédéraux à des fins de recherche. Cette disposition n'exempte toutefois pas l'organe fédéral de se fonder sur une base légale topique pour traiter des données personnelles à des fins de recherche[49]. Ainsi, cet article ne saurait justifier à lui seul un traitement de données à des fins de recherche, l'exigence d'une base légale restant pleinement applicable[50].

Entre autres, le principe de finalité ne trouverait pas à s'appliquer si les conditions de l'art. 39 al. 1 LPD sont établies. Pour bénéficier de cet allègement, les données concernées devront être au moins pseudonymisées[51] ; être communiquées sous une forme au moins pseudonymisée si elles sont sensibles[52] ; être communiquées par leur éventuel récipiendaire à des tiers qu'avec l'accord de l'organe fédéral ; et être anonymisées si elles sont publiées (art. 39 al. 1 lit. a à d LPD). En conséquence, les personnes concernées pourraient ignorer que

48 ROSENTHAL.
49 ROSENTHAL.
50 CR LPD-EPINEY/POSSE, art. 39, N 3.
51 Art. 39 al. 1 lit. a LPD ; <https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/forschung_statistik/forschung.html > ; EPINEY/POSSE sont d'un autre avis et estiment qu'une pseudonymisation ne constitue pas une anonymisation (*cf.* CR LPD-EPINEY/POSSE, art. 39, N 24).
52 FF 2017 6565, p. 7083 ss.

leurs données personnelles sont utilisées ultérieurement à des fins de recherche scientifique (voir *infra* II., C., 3., c), et 4.). Cependant, l'organe fédéral devra continuer à satisfaire ses autres obligations, notamment en matière de transparence et d'information. Les personnes concernées devraient donc au moins recevoir les informations minimales exigées par l'art. 19 LPD ou par une loi spéciale, sauf exceptions. Reste à savoir si les personnes concernées doivent absolument être informées de toutes les finalités secondaires ou potentielles et avec quelle granularité.

c) Remarques applicables aux personnes privées et organes fédéraux

Selon nous, la loi ne donne pas de réponse claire sur la question de savoir si les personnes privées ou les organes fédéraux doivent informer les personnes concernées de la nouvelle finalité du traitement de données (art. 19 al. 5 LPD), étant entendu que l'art. 6 al. 3 LPD postule que ces données « *doivent être traitées ultérieurement de manière compatible avec ces finalités* ». Du fait de la compatibilité d'un traitement à des fins de recherche scientifique avec la finalité initiale, il ne nous semble pas impératif, au regard de l'art. 19 al. 2 let. b LPD, d'informer les personnes concernées de cette nouvelle finalité dans la mesure où les informations nécessaires auraient déjà été données. Ceci dit, cette exception n'exonère pas le responsable de traitement de s'assurer que les autres informations requises au sens de l'art. 19 al. 2 let. a et let. c *cum* art. 19 al. 3 et 4 LPD ont été fournies, à savoir, entre autres, l'identité du responsable de traitement et ses coordonnées et les destinataires ou la catégorie des destinataires auxquelles les données personnelles sont transmises. Par ailleurs, pour des raisons de transparence ou d'éthique, il nous semble indiqué de le faire, même en l'absence d'obligation stricte, pour autant évidemment que cela soit réalisable, sans effort démesuré. À tout le moins, l'organe fédéral ou la personne privée serait inspiré de régulièrement communiquer sur ses activités de recherche, ne serait-ce pour maintenir le lien de confiance avec les personnes concernées.

4. Conformité avec le principe de transparence

Même si la loi ne traite pas stricto sensu du principe de transparence – elle utilise le terme de « reconnaissabilité » – un traitement de données personnelles est réputé reconnaissable lorsque la personne concernée a été dûment informée, lorsque ces traitements sont prévus par la loi ou lorsqu'ils ressortent clairement des circonstances[53]. Une collecte de données secrète ou clandestine

[53] FF 2017 6565, p. 6644.

représente une claire violation du principe de reconnaissabilité[54]. En vérité, le principe de transparence se matérialise surtout au travers de l'obligation générale d'informer applicable tant aux personnes privées qu'aux organes fédéraux[55] (avec quelques nuances toutefois). Cette obligation est inscrite à l'art. 19 LPD. L'ordonnance précise que le responsable du traitement doit fournir des informations sur la collecte de données personnelles de manière concise, transparente, compréhensible et facilement accessible (art. 13 de l'Ordonnance sur la protection des données, ci-après « OPDo »[56]). Ces développements sont tributaires d'éventuelles dispositions dérogatoires prévues dans une loi spéciale.

Au préalable, il faut distinguer entre une collecte de données personnelles directement auprès des personnes concernées et celle effectuée auprès d'un intermédiaire. Lorsque celles-ci sont collectées directement auprès de la personne concernée, le responsable du traitement doit communiquer, au moment de la collecte, au moins sur son identité et ses coordonnées (i), sur la finalité du traitement (ii), sur les catégories de destinataires auxquels des données sont transmises (iii), sur le nom de l'État vers lequel les données sont potentiellement communiquées ainsi que les garanties prises pour assurer un niveau de protection adéquat (iv) (art. 19 al. 2 et 4 LPD). Lorsque les données personnelles sont collectées auprès d'un intermédiaire, il faut, au surplus, indiquer les catégories de données personnelles acquises (art. 19 al. 3 LPD) et la fourniture de ces informations doit intervenir au plus tard un mois après l'obtention des données (art. 19 al. 5 LPD). Enfin, le devoir d'informer une seconde fois les personnes concernées par rapport à une réutilisation de données qui serait jugée compatible avec la finalité initiale ne serait pas impératif (*cf. supra* II., C., 3., c)). Toutefois, si un autre élément figurant à l'art. 19 al. 2 LPD change lors de cette réutilisation – comme les destinataires des données –, la personne concernée devra être informée de ces changements.

Le devoir d'informer souffre, en plus, quelques exceptions. Premièrement, un responsable du traitement n'aura pas besoin d'informer une personne derechef si celle-ci a déjà reçu l'information (art. 20 al. 1 lit. a LPD), par exemple lors de l'acceptation de conditions générales de vente[57]. L'information est également réputée donnée lorsque la personne a elle-même rendu accessible les données sans l'intervention du responsable du traitement[58].

Ensuite, il peut s'en exonérer si le traitement de données est prévu dans une loi (art. 20 al. 1 lit. b LPD). Cette exception est problématique car même si le trai-

54 ATF 146 IV 226, c. 3.
55 OFJ, Rapport explicatif, p. 20, n. 1.4.2.2.
56 Ordonnance fédérale du 31 août 2022 sur la protection des données (OPDo), RS 235.11.
57 FF 2017 6565, p. 6670.
58 FF 2017 6565, p. 6671.

tement est prévu par la loi, cela ne signifie pas encore que le principe de transparence ait été respecté car le devoir d'information sous-jacent n'impliquerait pas seulement l'accessibilité de l'information (qui peut être diffuse et difficile à comprendre car contenue dans diverses lois ou ordonnances avec un langage technique et juridique) mais aussi et surtout la communication effective de ces informations aux personnes concernées dans un langage compréhensible[59]. Le principe de légalité et le principe de transparence sont deux composants que le législateur tente régulièrement de matérialiser au sein d'une base légale, alors que le principe de transparence gagnerait à être réalisé grâce à une communication appropriée, par exemple avec l'utilisation de politiques de protection des données personnelles (*privacy policies*)[60]. Autrement, cela signifierait que la plupart des traitements de données opérés par des organes fédéraux n'impliquerait pas d'informer les personnes concernées[61], ce qui viderait de son sens le principe de transparence en protection des données et rendrait plus opaque les activités d'une administration pourtant soumise au principe de la transparence « administrative » (art. 1 LTrans[62]). D'ailleurs, certains organes fédéraux communiquent déjà largement sur leur politique de protection des données personnelles (*privacy policy*) en fournissant des informations parfois plus étendues que ce que n'exige la loi.

En troisième lieu, une personne privée peut ignorer son devoir d'information lorsqu'elle est tenue à une obligation légale de garder le secret (art. 20 al. 1 lit. c LPD) comme le secret professionnel ou médical, et qu'elle traite les données personnelles dans ce contexte uniquement. Puis, les médias à caractère périodique peuvent renoncer à informer les personnes concernées lorsque certaines conditions sont remplies (art. 20 al. 1 lit. d *cum* art. 25 LPD).

Enfin, et seulement lorsque les données ne sont pas collectées directement auprès des personnes concernées, les responsables du traitement peuvent s'exonérer de transmettre les informations si l'information est impossible à donner ou si elle nécessite des efforts disproportionnés (art. 20 al. 2 lit. a et b LPD). À l'instar de ce qui prévaut à l'aune du Règlement de l'Union européenne sur la protection des données (ci-après : « RGPD »[63]), une information est impossible à donner lorsqu'on ne peut pas attribuer une source particulière aux différentes

59 THOUVENIN/BRAUN BINDER, n. 5-29.
60 THOUVENIN/BRAUN BINDER, n. 5-29.
61 ROSENTHAL/STUDER/LOMBARD, p. 42, n. 103.
62 Loi fédérale du 17 décembre 2004 sur le principe de la transparence dans l'administration (Loi sur la transparence, LTrans), RS 152.3.
63 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).

données personnelles détenues sur une personne, pour autant que la compilation n'ait pas été effectuée par le responsable du traitement lui-même[64]. Quant aux critères pour juger de la disproportion des efforts à fournir, ils consistent par exemple à prendre en compte le nombre de personnes concernées ou l'âge des données personnelles.

Dans tous les cas, le responsable du traitement devrait procéder à une pesée des intérêts entre l'effort réel nécessaire au responsable du traitement pour informer les personnes concernées et l'impact sur les personnes concernées si elles ne reçoivent pas ces informations[65]. Il devrait également prendre des mesures appropriées pour protéger les intérêts des personnes concernées. Par exemple, il devrait rendre publiques les informations qui concernent le traitement de données envisagé[66]. D'autres mesures appropriées, en plus de la publication des informations, peuvent inclure : la réalisation d'une étude d'impact sur la protection des données, l'application de techniques de pseudonymisation ; la minimisation des données personnelles collectées et la réduction de la période de stockage ; et la mise en œuvre de mesures techniques et organisationnelles visant à garantir un niveau élevé de sécurité[67].

5. Conformité avec le principe de proportionnalité

Un autre principe cardinal doit être suivi en cas de réutilisation de données personnelles, celui de la proportionnalité. Un responsable du traitement qui souhaiterait réutiliser des données personnelles doit limiter son traitement de données au strict nécessaire et à celles qui sont aptes à atteindre le but fixé[68]. Ainsi, les données personnelles traitées doivent être objectivement nécessaires pour atteindre le but poursuivi et idoines à l'atteindre, tout en préservant le plus possible le droit des personnes concernées en assurant un équilibre raisonnable entre le résultat légitime recherché et le moyen utilisé[69]. Il en résulte une interdiction de collecter des données « en réserve » (*auf Vorrat* en allemand) ce qui irait au-delà du but fixé[70]. Par ailleurs, le principe de proportionnalité doit être appliqué à toutes les étapes du traitement : de la décision de traiter des

64 Article 29 Working Party, Guidelines on transparency, p. 29, n. 60.
65 Article 29 Working Party, Guidelines on transparency, p. 30 ss, n. 61 ss.
66 Article 29 Working Party, Guidelines on transparency, p. 30 ss, n. 61 ss ; Décision du Conseil d'État Français du 30.12.2021 nº 440376, consid. 25.
67 Article 29 Working Party, Guidelines on transparency, p. 31, n. 64 ; Pour un cas récent italien : Garante per la protezione dei dati personali (Italie), Provvedimento del 2 marzo 2023, nº 9875254.
68 FF 1988 II 421, p. 458 ; DESCHENAUX/STEINAUER, p. 270, n. 734c.
69 MÉTILLE, p. 9.
70 ATF 125 II 473, c. 4a.

données personnelles, en passant par la collecte, à l'utilisation des données[71]. Ainsi, on déduit du principe de proportionnalité deux autres principes. Le premier, le principe d'évitement, implique de reconsidérer la collecte de nouvelles données personnelles (en évitant toute collecte), alors que le second, le principe de minimisation des données, suppose la collecte des seules données absolument nécessaires à atteindre le but poursuivi[72].

La réutilisation de données personnelles peut accroître la tension existante avec le principe de proportionnalité, car l'accessibilité des données accroît la tentation de collecter plus de données que nécessaire au cas où un besoin ultérieur et imprévu surviendrait. Or, tant le principe de proportionnalité que celui de la finalité commandent de limiter le type et le nombre de données personnelles en fonction d'un but prédéfini.

6. Cas particuliers

a) La réutilisation de données personnelles accessibles au public

La réutilisation de données personnelles rendues accessibles au public par la personne concernée représente un cas à part. En effet, la LPD prévoit un régime distinct pour ce cas de figure. On songera par exemple aux traitements effectués par « *ChatGPT* », prototype d'agent conversationnel utilisant l'intelligence artificielle développée par *OpenAI*, lequel traite notamment des données personnelles accessibles au public et qui suscite de nombreuses questions juridiques[73].

Pour les personnes privées, la réutilisation de données personnelles déjà publiées par la personne concernée ne constituerait pas une atteinte à la personnalité, pour autant que la personne ne se soit pas opposée expressément au traitement (art. 30 al. 3 LPD) et que le traitement ne viole pas un principe général en protection des données (*cf. supra* II, C.). En effet, la loi ne dispose que d'une présomption réfragable (« *En règle générale, il n'y a pas d'atteinte à la personnalité* […] »)[74]. Le Tribunal administratif fédéral a par exemple exigé que des données personnelles divulguées publiquement par la personne elle-même doit l'avoir été de façon volontaire et on ne peut pas admettre l'intention de cette

71 Conseil de l'Europe, Rapport explicatif de la Convention 108+, n. 40.
72 SHK DSG-Baeriswyl, N 23 ; FF 2017 6565, p. 6644 ; Métille, p. 9.
73 P. ex. : Garante per la protezione dei dati personali (Italie), Provvedimento dell'11 aprile 2023, nº 9874702 ; <https://www.edoeb.admin.ch/edoeb/fr/home/kurzmeldungen/20230404_chatgpt.html>.
74 FF 2017 6565, p. 6688.

personne sur la base d'un comportement passif consistant à simplement tolérer l'action d'un tiers[75].

Pour les organes fédéraux, l'exigence d'avoir une base légale pour traiter des données personnelles accessibles au public tomberait dans la mesure où la personne a volontairement publié ses données personnelles et ne s'y est pas opposée expressément (art. 34 al. 4 lit. b *in fine* LPD). À supposer que les conditions légales soient remplies, les organes fédéraux seraient aussi libres de communiquer ces données personnelles selon les mêmes conditions même en l'absence d'une base légale topique (art. 36 al. 2 lit. d LPD).

Toute réutilisation de données personnelles déjà publiées devra dans tous les cas obéir aux principes généraux de protection des données (art. 6, 7 et 9 LPD) et au devoir d'informer les personnes concernées (art. 19 LPD). Évidemment, comme indiqué plus haut (*cf. supra* II., B., 5.), il est probable qu'un responsable du traitement puisse, dans ce cas, se prévaloir d'une exception si la personne dispose déjà des informations requises (art. 20 al. 1 lit. a LPD), ou si une information s'avérait difficile à donner en raison des efforts disproportionnés que cela engendrerait (art. 20 al. 2 lit. b LPD).

d) Communication des données à l'étranger

Pour conclure cette partie, on ne peut pas traiter du sujet de la valorisation des données en matière d'intelligence artificielle et de gouvernance sans aborder succinctement la question de la communication des données personnelles à l'étranger[76]. Le monde académique est largement globalisé et les interactions entre des institutions de différents pays sont fortes. Ainsi, l'échange potentiel de données personnelles en vue de leur valorisation sous cette forme devra satisfaire aux exigences en matière de transfert de données personnelles à l'étranger.

L'art. 16 LPD exige en principe une protection équivalente des données personnelles par l'État destinataire de ces données. L'objectif est de préserver la situation juridique de la personne dont les données sont communiquées à l'étranger[77]. Cette exigence découle de la Convention 108+, mais les décisions prises par la Cour de justice de l'Union européenne[78] ont certainement influencé les mesures suisses. La Convention 108+ prévoit qu'un transfert de données

75 TAF, A-4232/2015 du 18 avril 2017, c. 5.4.1.

76 Pour un bon état des lieux récent sur cette question (en lien avec des services *clouds*), voir FISCHER/PITTET.

77 K-DSG-MAURER, Art. 6 DSG, N 18.

78 CJUE, arrêt C-362/14 du 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner (Schrems I)* ; CJUE, arrêt C-311/18 du 16 juillet 2020, *Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems (Schrems II)*.

personnelles vers un État non partie à cette convention implique de garantir un niveau de protection approprié (art. 14 al. 2 Convention 108+). Une telle garantie peut être apportée soit par les règles de droit de l'État destinataire, soit par des garanties *ad hoc* ou standardisées, juridiquement contraignantes, opposables et dûment mises en œuvre par l'État destinataire[79]. Le Conseil fédéral doit établir une liste d'États vers lesquels une libre circulation des données personnelles est autorisée[80]. Si l'État destinataire ne garantit pas un niveau de protection adéquat, le responsable du traitement devra justifier le transfert par l'un des motifs prévus à l'art. 16 al. 2 LPD, comme des garanties contractuelles, le consentement exprès de la personne concernée, ou en vue de satisfaire une obligation contractuelle en vertu d'un contrat passé avec la personne en cause. En particulier, ces mesures visent à garantir les droits fondamentaux suivants : le principe de légalité, le principe de proportionnalité, le droit à être suffisamment protégé contre l'emploi abusif de ses données personnelles, et le droit à des garanties générales de procédure[81]. Si l'État destinataire ne garantit pas le respect de ces quatre droits fondamentaux et que les garanties contractuelles ne suffisent pas, des mesures techniques et organisationnelles supplémentaires devraient être prises pour empêcher l'État destinataire d'accéder aux données personnelles[82]. Ainsi, si l'examen final révèle qu'un des droits fondamentaux est violé et que les mesures supplémentaires ne suffisent pas à empêcher tout accès aux données personnelles, le transfert de données personnelles vers l'État destinataire devra être suspendu ou interrompu[83]. Selon le Préposé fédéral à la protection des données et à la transparence, en l'absence des garanties exigées – et même à supposer que la probabilité d'un accès aux données personnelles par l'État destinataire soit faible –, un tel transfert serait illicite. D'ailleurs, selon lui, la loi ne prévoirait pas une approche fondée sur le risque[84].

L'une des grandes problématiques actuelles réside dans le fait que les États-Unis ne disposent pas, à ce jour, de niveau de protection adéquat[85], même s'il est

79 Conseil de l'Europe, Rapport explicatif de la Convention 108+, n. 109.

80 FF 2017 6565, p. 6657 ; art. 8 OPDo.

81 PFPDT, Guide pour l'examen de la licéité de la communication transfrontière de données, N 05.

82 PFPDT, Guide pour l'examen de la licéité de la communication transfrontière de données, N 08 ss.

83 PFPDT, Guide pour l'examen de la licéité de la communication transfrontière de données, N 10.

84 PFPDT, Stellungnahme zur Datenschutz Risikobeurteilung der Suva, n. 23 à 28. Cette approche est cependant critiquée par plusieurs auteurs, notamment FISCHER/PITTET, p. 74 ss.

85 PFPDT, Prise de position sur la transmission de données personnelles vers les États-Unis.

probable que la situation juridique soit résolue prochainement[86], à moins d'un recours contre cette nouvelle décision[87]…

D. Conclusion intermédiaire

Pour achever cette partie, nous proposons une brève synthèse. La valorisation des données de la recherche dans l'intelligence artificielle et dans le pilotage des institutions de recherche implique régulièrement une réutilisation de données personnelles. Pour que cette utilisation secondaire reste licite, le responsable du traitement devra nécessairement s'enquérir de la base de légitimité sur laquelle il entend s'appuyer. Surtout, bien que le traitement ultérieur de ces données personnelles à des fins de recherche soit jugé comme souvent compatible avec la finalité initiale, une réutilisation de ces données n'exempte pas le responsable du traitement de se conformer aux principes généraux en protection des données. En particulier, les principes de licéité, de bonne foi, de proportionnalité, d'exactitude et de sécurité demeurent et ne souffrent a priori aucune exception. À la fin, la réutilisation de données personnelles dépend de la qualité des informations fournies et des précautions prises par le responsable du traitement lors de la collecte des données. Enfin, faut-il le rappeler, le fait que des données soient accessibles au public ne décharge aucunement la responsabilité du chercheur, lequel reste tenu d'appliquer les règles de protection des données personnelles.

III. Valorisation par les mouvements de science ouverte

La troisième forme de valorisation des données de la recherche consiste à rendre plus accessibles les résultats de la recherche. Dans cette troisième section, nous décrirons brièvement ce que l'on entend par *libre accès (Open Access)* et *données ouvertes (Open Data)*, ces deux composants de la science ouverte (*Open Science*), et en quoi cette diffusion de données peut constituer un risque en matière de protection des données personnelles. L'UNESCO définit l'*open-science* comme différents mouvements et pratiques consistant, notamment, à

86 Un nouvel accord-cadre devrait être mis en place entre l'Union Européenne et les États-Unis intitulé « European Union-U.S. Data Privacy Framework » : <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/> ; <https://crsreports.congress.gov/product/pdf/LSB/LSB10846> ; <https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_7631>. À noter également que le Comité Européen de la Protection des Données (EDPB) émet des réserves sur le cadre juridique envisagé même s'il salue certains efforts, *cf.* EDPB, Opinion 5/2023.

87 <https://noyb.eu/en/statement-eu-comission-adequacy-decision-us>.

rendre les connaissances scientifiques librement accessibles et réutilisables par tous et à favoriser le partage des informations au profit de la science et de la société[88]. Parmi ces mouvements, on retrouve le *libre accès (Open Access)* et les *données ouvertes (Open Data)*[89].

E. Du Libre accès (*Open Access*) aux Données ouvertes (*Open Data*)

Traditionnellement, les résultats de la recherche étaient publiés par l'intermédiaire de grands éditeurs, propriétaires de journaux réputés. L'accessibilité du contenu de ces journaux est possible moyennant le paiement d'un abonnement. Depuis près de vingt ans, le secteur de la recherche académique tente de s'extirper du monopole de ces grands éditeurs pour, entre autres, rendre les travaux scientifiques accessibles et économiser des coûts d'abonnement devenus exorbitants avec le temps. Des initiatives internationales ont posé les jalons de ce changement de paradigme[90]. Depuis 2016, le Secrétariat d'État à la formation, à la recherche et à l'innovation (SEFRI) a mandaté *swissuniversities* pour élaborer, de concert avec le Fonds national suisse de la recherche scientifique (FNS), une stratégie nationale de libre accès aux publications dans l'objectif de rendre accessible au public librement les publications académiques financées par de l'argent public[91]. Pour *swissuniversities*, le *Libre accès (Open Access)* a le potentiel de contribuer positivement à la prospérité en Suisse[92].

La publication en *Libre accès (Open Access)* couvre trois approches[93] : (i) *Green Open Access* : l'archivage des résultats de la recherche dans des bases de données ou des archives librement accessibles après le respect d'un embargo ; (ii) *Gold Open Access* : la publication initiale et originale est librement et immédiatement accessible moyennement le paiement de frais de traitement (*Article Processing Charges*) ; *Hybrid Open Access* : publication d'articles en libre accès dans des revues sur abonnement et accès au contenu desdites revues.

---

88 UNESCO, Recommandation sur une science ouverte, p. 7, n. 6.

89 ASS, Swiss Academic Factsheet 14 (2).

90 Déclaration de Berlin ; Déclaration de Budapest.

91 Swissuniversities, Stratégie nationale suisse sur l'Open Access ; Swissuniversities, Plan d'action sur la Stratégie nationale suisse sur l'Open Access ; FNS, Lettre ouverte ; Règlement relatif à l'encouragement des publications en libre accès (Open Access) du Fonds national suisse (FNS) du 7 novembre 2017 ; <https://oa100.snf.ch/fr/home-fr/>.

92 Swissuniversities, Stratégie nationale suisse sur l'Open Access, p. 1-2.

93 Swissuniversities, Stratégie nationale suisse sur l'Open Access, p. 2 ; Swissuniversities, Plan d'action sur la Stratégie nationale suisse sur l'Open Access, p. 8. NB : d'autres auteurs ont une classification un peu différente et intègrent des moyens d'accès illégaux (*black open access*) : p. ex. BJÖRK.

Dans la veine du *Libre accès (Open Access)*, il est désormais question de partager les données numériques de la recherche en Suisse financée par des fonds publics afin de rendre possible la réutilisation de ces données et la reproduction des résultats de la recherche par les chercheurs[94]. La Suisse entend mettre en place une stratégie nationale suisse sur l'*Ouverture des données de recherche (Open Research Data)* (ORD). Cette dernière s'inspire du mouvement de *Science ouverte (Open Science)* qui vise à permettre l'accès, la diffusion et la réutilisation de publications, données, documents et méthodes scientifiques[95]. Elle s'aligne notamment sur l'initiative internationale *FAIR* (*Findable*, *Accessible*, *Interoperable*, *Reusable*) promouvant une meilleure exploration (les données sont aisément trouvables), accessibilité (les données peuvent être facilement récupérées), interopérabilité (données enregistrées sous un format standard), et une réutilisation facilitée (données documentées et réutilisables dans des conditions claires)[96]. Cette stratégie encourage la transparence, l'efficacité et la reproductibilité des résultats de la recherche[97]. Elle reconnaît aussi la valeur des données de recherche qui se manifeste à différents niveaux : acquisition des données, traitement des données comme ressources, maintenance et curation des données[98]. D'ailleurs, le plan stratégique du Domaine des EPF s'attelle à rendre accessibles au public tous les résultats de recherche financés par des fonds publics d'ici à 2024, y compris les données de la recherche afin qu'elles puissent être utilisées, réutilisées et communiquées[99]. Le Domaine des EPF a même constitué un groupe de travail pour réfléchir à ces questions[100]. Le Fonds national suisse de la recherche scientifique (FNS) soutient également l'accessibilité des données de la recherche[101] et prévoit que « [l]*'ensemble des données recueillies et générées durant les travaux de recherche sur lesquelles se basent les publications doivent être partagées, pour autant qu'aucune clause juridique, éthique, de propriété intellectuelle ou autre ne s'y oppose* » (art. 11.8 Règlement d'exécution général relatif au règlement des subsides du 9 décembre 2015).

– Par exemple, de nombreux chercheurs publient leurs données de recherche sur les plateformes *Zenodo* ou *Dryad*. *Zenodo* est une plateforme gérée et financée principalement par le CERN, tandis que Dryad est géré sous l'égide d'une organisation à but non lucratif américaine[102]. Nous pouvons citer aussi la plateforme suisse *SWISSUbase*, née

94 Swissuniversities, Stratégie Nationale Suisse Open Research ; Accord ORD.
95 Levin/Leonelli/Weckowska/Castle/Dupré, p. 128-141.
96 Swissuniversities, Stratégie Nationale Suisse Open Research Data, p. 6 ; <https://www.go-fair.org/fair-principles/>.
97 Swissuniversities, Stratégie Nationale Suisse Open Research Data, p. 6.
98 Swissuniversities, Stratégie Nationale Suisse Open Research Data, p. 7.
99 Conseil des EPF, Strategic Plan 2025–2028, p. 31.
100 Conseil des EPF, Open Research Data.
101 <https://www.snf.ch/fr/dMILj9t4LNk8NwyR/dossier/open-research-data> ; FNS, Open Research Data Policy.
102 <https://about.zenodo.org/terms/>; <https://datadryad.org/stash/our_governance>.

d'un partenariat avec plusieurs institutions suisses, qui est une solution interdisciplinaire nationale pour les universités suisses et autres organismes de recherche qui ont besoin de dépôts de données institutionnels locaux pour leurs chercheurs[103].

De surcroît, le Code d'intégrité scientifique, publié par les Académies suisses des sciences dans sa version datée de 2021, s'adresse à tous les « *acteurs impliqués dans la production, la diffusion et la promotion des connaissances au sein du système des hautes écoles suisses* » et institue un devoir de mettre à disposition d'un large public les travaux scientifiques et de rendre accessibles les données issues de ces travaux lorsqu'aucune règlementation ne s'y oppose[104]. On retrouve ces mêmes obligations au sein de diverses institutions de recherche en Suisse[105].

Nous mentionnons aussi l'exemple de l'Union Européenne qui a légiféré dans ce secteur avec la Directive UE 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (ci-après la « Directive UE 2019/1024 ») et le Règlement UE 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données (ci-après le « Règlement UE 2022/868 »). Elle juge indispensable de s'attaquer aux obstacles restants et émergents à une large réutilisation des informations détenues par le secteur public dans l'ensemble de l'Union Européenne, pour tenir compte des progrès des technologies numériques et de stimuler davantage encore l'innovation numérique, notamment en ce qui concerne l'intelligence artificielle[106].

En définitive, les chercheurs sont amenés à publier les résultats de leur recherche dans des journaux en *Libre accès (Open Access)*, mais sont également encouragés à publier les données ou métadonnées obtenues au cours de leur recherche. Le principe de *Science ouverte (Open Science)*, au travers du *Libre accès (Open Access)* et de l'*Ouverture des données de recherche (Open Research Data)*, est un facteur de développement pour nos sociétés actuelles permettant une diffusion large des résultats de la recherche et une réutilisation accrue des données pour favoriser l'innovation technologique que l'on songe à l'intelligence artificielle ou la médecine personnalisée. Si ces résultats concernent des données personnelles, les chercheurs devront se demander si une telle publication est conforme au droit de la protection des données personnelles.

103 <https://www.swissubase.ch/fr/>.

104 SAMW, Code d'intégrité scientifique, 2021, art. 4.3 et art. 4.5.

105 P. ex., art. 13 de la Directive de la Direction de l'UNIL 4.5 sur le traitement et la gestion des données de recherche du 1er janvier 2019 et la Charte institutionnelle pour la science ouverte de l'Université de Genève du 9 décembre 2021

106 Préambule de la Directive UE 2019/1024, consid. 3.

F. Ouverture aux données personnelles ?

Avec l'*Ouverture des données de recherche (Open Research Data)*, les données de recherche, ainsi que les métadonnées associées, devraient ainsi être toujours publiées pour notamment satisfaire à l'exigence d'accessibilité[107]. Pour répondre à cette ambition, peut-on légitimement publier les données personnelles récoltées lors de la recherche ? Sur quelle base et avec quelles limites ?

Comme évoqué plus haut (*cf. supra* chiffre II., B., 2.), le responsable du traitement devra s'enquérir de sa base de légitimité s'il est un organe fédéral (art. 34 et art. 36 al. 1 LPD) ou se prévaloir d'un motif justificatif s'il est une personne privée car cette publication constituerait une atteinte à la personnalité (art. 30 LPD), notamment du fait d'une violation du principe de finalité et de proportionnalité. À ce stade, les bases légales qui autoriseraient la publication de données personnelles pour remplir les objectifs de l'*Ouverture des données de recherche (Open Research Data)* sont insuffisantes à notre avis[108]. Partant, en l'absence de base légale topique, le consentement des personnes concernées s'avérera nécessaire (art. 31 al. 1 LPD et art. 36 al. 2 lit. b LPD) et celles-ci devront avoir été informées de la publication de leurs données personnelles, mais aussi de la possibilité que d'autres puissent les utiliser à leur tour (art. 19 al. 2 lit. c LPD). Pour les organes fédéraux, la publication des données personnelles pourrait aussi procéder d'une information officielle du public à l'aune de la Loi fédérale sur le principe de la transparence dans l'administration (LTrans), (art. 36 al. 3 LPD).

Sur le principe, si le traitement s'est opéré dans un but de recherche, les données personnelles devraient être anonymisées au préalable (art. 31 al. 2 lit. e ch. 3 et art. 39 al. 1 lit. d LPD). Toutefois, des données anonymisées perdent de leur valeur car elles sont dépouillées de leur granularité, voire rendent impossible une réidentification qui puisse s'avérer nécessaire dans certains cas – pour des raisons médicales par exemple[109]. Si, d'emblée, une anonymisation n'est pas opportune, alors le responsable du traitement devrait proactivement recueillir le consentement des personnes concernées pour la publication de leurs données personnelles. Ce consentement devra énumérer les conditions relatives au dépôt

107 Swissuniversities, Stratégie Nationale Suisse Open Research Data, p. 6.

108 P. ex. art. 36*c* ss de la loi fédérale du 4 octobre 1991 sur les écoles polytechniques fédérales (Loi sur les EPF), RS 414.110.

109 FF 2009 7259, p. 7320 ; Vincent Mooser/Dominique Sprumont, « Qu'est-ce qu'une biobanque ? », *in* : Emission radio RTS On en parle du 21 avril 2016, <https://www.rts.ch/audio-podcast/2016/audio/qu-est-ce-qu-une-biobanque-25723340.html> ; Erard/Heusghem/Parisato, p. 12, n. 31.

des données personnelles (possiblement sensibles) sur la plateforme dont il est question et les droits du patient/sujet à ce propos.

Par ailleurs, la publication devra aussi et surtout respecter les principes généraux en protection des données, notamment celui de la proportionnalité. A l'instar de différentes décisions tant européennes que suisses[110], le principe de proportionnalité ou celui de la minimisation des données devra être respecté dans un tel cas. Sous réserve d'une base de légitimité adéquate, une publication de données personnelles serait ainsi justifiée si cela est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, mais pour autant que la finalité du traitement ne puisse pas être raisonnablement atteinte par d'autres moyens. En outre, cette publication ne devrait pas porter préjudice à des données personnelles dignes de protection à l'instar de données issues de profilage ; dans tous les cas, une pesée des intérêts devra être menée[111]. En d'autres termes, l'objectif d'*Ouverture des données de recherche (Open Research Data)* ne saurait être un blanc-seing à la publication de données personnelles et celles-ci devraient être publiées uniquement si l'on peut démontrer un intérêt légitime pour la science et que, sans cette accessibilité, les objectifs scientifiques seraient considérablement affaiblis. En outre, si les données personnelles sont sensibles (comme des données de santé), alors une analyse d'impact relative à la protection des données personnelles devrait être réalisée avant toute publication (art. 22 LPD). Elle servira à déterminer si la publication envisagée sert un intérêt prépondérant par rapport au droit au respect à la sphère privée et que les mesures prévues pour protéger la personnalité et les droits fondamentaux des personnes concernées réduisent les risques à un niveau acceptable.

En premier lieu, un chercheur devrait d'abord estimer si une publication des données dans un format anonymisé pourrait satisfaire à une réutilisation ultérieure de ces données. Si ce n'est pas le cas, il devrait en second lieu s'assurer de disposer d'une base de légitimité suffisante et devrait justifier en quoi la publication servirait les missions dévolues à l'*Ouverture des données de recherche (Open Research Data)* et vérifier que la publication respecte le principe de proportionnalité. À notre avis, si la personne concernée a consenti préalablement à la publication de ses données personnelles, cette publication serait licite sous réserve du respect des principes généraux en protection des données, en particulier le principe de finalité et de proportionnalité. Si les données sont sensibles, une pesée des intérêts devrait, en plus, être effectuée au travers d'une

110 CJUE, arrêt du C-439/19 du 22 juin 2021, *Latvijas Republikas Saeima*, consid. 104 ss ; TAF, A-2479/2020 du 26 mars 2021, c. 4.5.1 ; TAF, A-4232/2015 du 18 avril 2017, c. 5.4.2.2 ss.

111 TAF, A-2479/2020 du 26 mars 2021, c. 4.5.1 ; TAF, A-4232/2015 du 18 avril 2017, c. 5.4.2.2 ss.

analyse d'impact relative à la protection des données personnelles afin de déterminer si les risques liés à la publication sont raisonnables pour les droits et libertés des personnes concernées. Ensuite, d'autres limites juridiques peuvent s'opposer à la publication des données de recherche en général – même en l'absence de données personnelles – que ce soit pour des raisons liées au contrôle des biens à l'exportation[112], au respect de secret de fonction ou professionnel[113], des raisons de responsabilités[114], voire pour des motifs de confidentialité, ou encore de propriété intellectuelle[115].

G. Conclusion intermédiaire

Pour conclure cette troisième partie, nous avons constaté que les chercheurs sont de plus en plus encouragés à publier les données de recherche, y compris parfois les données personnelles y relatives. À nouveau, le respect des principes de protection des données, en particulier celui de la proportionnalité, est fondamental. En outre, nous retiendrons deux variantes possibles lors de la publication en *open source* des données personnelles issues d'une recherche : (1) premièrement, le chercheur utilise une plateforme où seules des données anonymisées peuvent être publiées et le consentement devrait contenir le droit d'anonymiser les données à cette fin ; (2) deuxièmement, le chercheur utilise une plateforme autorisant la publication de données personnelles en vue de leur réutilisation par des tiers, pour autant que des garde-fous soient engagés – par exemple, il est primordial de s'assurer que la (ou les) finalité(s) secondaire(s) prévue(s) au sein de la plateforme soi(en)t compatible(s) avec la finalité initiale (une utilisation commerciale serait rarement admise[116]), que la plateforme impose des conditions juridiques et techniques strictes pour préserver la confidentialité des données par le réutilisateur, qu'elle ne communique des données personnelles à l'étranger qu'avec des garanties suffisantes ou qu'elle l'interdise si nécessaire[117], enfin qu'un retrait de consentement puisse être effectif et communiqué aux récipiendaires. Sur ce dernier point, la création d'un nouveau système de consentement se pose, incluant la possibilité pour les réutilisateurs des données de pouvoir prendre automatiquement contact avec les personnes concernées ou

112 Voir la loi fédérale sur le contrôle des biens utilisables à des fins civiles et militaires, des biens militaires spécifiques et des biens stratégiques du 13 décembre 1996 (Loi sur le contrôle des biens, LCB), RS 946.202 ; son ordonnance et ses annexes.

113 ERARD, p. 133 ss, n. 331 ss.

114 Voir la loi fédérale sur la responsabilité du fait des produits du 18 juin 1993, RS 221.112.944 ; et les autres régimes de responsabilités civiles.

115 Comme par exemple se préserver de la possibilité de déposer un brevet d'invention.

116 Sauf si la personne a consenti expressément à une utilisation commerciale ou si une base légale le permet expressément.

117 COM/2020/767 final, consid. 11.

les patients, pour les informer de la réutilisation des données, voire, au surplus, des résultats de la recherche se rapportant à leur santé conformément à l'article 8 LRH (consentement dynamique). Ce consentement pourrait aussi traiter de la réutilisation ultérieure de nouvelles données de santé générées au travers de la recherche.

En définitive, le choix et les modalités de la plateforme sur laquelle les données personnelles seraient publiées est crucial. Plus encore s'il s'agit de données personnelles sensibles comme des données de santé.

IV. Valorisation des données de santé

Dans cette dernière section, nous allons expliquer plus précisément pourquoi les données de santé ont pris de la valeur et, surtout, nous allons décrire les risques juridiques que nous avons soulevés en lien avec cette politique de valorisation. Nous examinerons aussi les conditions selon lesquelles des données de santé pourraient être valorisées.

Avant toute chose, nous allons définir ce que nous entendons par données de santé, auxquelles se réfère la LPD. La LRH utilise le terme de « *données personnelles liées à la santé* » et les définit comme suit : « [toutes] *informations concernant une personne déterminée ou déterminable qui ont un lien avec son état de santé ou sa maladie, données génétiques comprises* » (art. 3 lit. f LRH). Cependant, le législateur suisse n'a pas défini ce qu'il entendait par « données de santé ». Nous savons simplement que les données de santé appartiennent à la catégorie des données dites sensibles (art. 5 lit. c ch. 2 et 3 LPD). D'aucuns définissent cette notion comme regroupant toutes les informations qui fournissent des renseignements sur des résultats médicaux et qui peuvent avoir des conséquences négatives pour les personnes concernées[118]. Cette notion est donc variable et ne saurait contenir une liste exhaustive d'informations qui constitueraient des données de santé[119]. Il s'agit donc d'un concept relativement flou qui englobe potentiellement des informations très différentes.

Après avoir défini ce qu'on entendait par données de santé, nous pouvons entrer dans le vif du sujet en décrivant l'historique qui a débouché sur la volonté d'une meilleure accessibilité des données de santé. En 2013, le Conseil fédéral fixait déjà certains buts pour améliorer notamment l'accès aux données sur la santé grâce à des outils numériques. Le progrès technologique dans les méthodes de génétiques moléculaires a rendu possible la médecine personnalisée. La recherche dans le domaine de la médecine personnalisée « *cherche à mettre à*

118 AEBI-MÜLLER/FELLMANN/GÄCHTER/RÜTSCHE/TAG, p. 437 ; BsK DSG-BLECHTA, Art. 3 DSG, N 33.

119 VOKINGER.

profit des résultats de la recherche fondamentale pour progresser sur des axes prioritaires tels que le développement de nouveaux médicaments, l'optimisation des thérapies et l'identification et le traitement de maladies rares »[120].

Or, la compétitivité de la Suisse dépend dans ce domaine de l'accessibilité des données de santé aux acteurs de la recherche clinique[121]. Ces données sont essentielles pour la recherche médicale, pour assurer une organisation efficace et optimale des soins personnalisés et pour préserver et renforcer la santé publique[122]. L'objectif consiste par exemple à l'utilisation de standards sémantiques uniformes pour la documentation médicale[123]. D'ailleurs, le plan directeur 2022-2026 du Conseil Fédéral pour renforcer la recherche et la technologie biomédicales précise la reconduction du financement du *Swiss Personalized Health Network* (SPHN) et plaide en faveur d'une facilitation de l'utilisation secondaire des données de santé pour la recherche[124]. Le projet SPHN est né à l'initiative de la Confédération en 2017[125] et a pour objectif de créer une infrastructure permettant de mettre en réseau les données des hôpitaux universitaires, des universités, *etc*.[126]. Parallèlement, le domaine des EPF[127], par le truchement du Conseil des EPF, finance en 2017 un programme de financement similaire dénommé « *Personalized Health and Related Technologies* » (PHRT), lequel met au centre la médecine et la santé personnalisées[128]. Ce financement permettrait par exemple le développement de nouvelles technologies qui détermineraient la composition moléculaire précise des patients ou détermineraient l'état phénotypique des personnes[129].

Ces différentes initiatives stratégiques démontrent que l'accessibilité et l'interopérabilité des données de santé œuvrent à renforcer la valeur de ces données personnelles sensibles, car leur partage et leur réutilisation ont une valeur

120 FF 2016 2917, p. 3023.
121 DFI, Mesures de la Confédération afin de renforcer la recherche et la technologie biomédicales, p. 118, n. 7.5.5.
122 OFSP, Politique de la santé, p. 14.
123 DFI, Mesures de la Confédération afin de renforcer la recherche et la technologie biomédicales, p. 114 ss, n. 7.5.
124 OFSP, Rapport 2022-2026, p. 23 ss, n. 5 ss.
125 FF 2016 2917, p. 3023.
126 <https://sphn.ch/wp-content/uploads/2022/06/BMI003_Prod_Factsheet_SPHN_digital.pdf> ; <https://www.samw.ch/fr/Projets/Apercu-des-projets/Sante-personnalisee/Swiss-Personalized-Health-Network.html>.
127 Qui comprend les écoles polytechniques fédérales de Lausanne (EPFL) et de Zurich (EPFZ), ainsi que quatre établissements de recherche : l'Institut Paul Scherrer (PSI), l'Institut fédéral de recherches sur la forêt, la neige et le paysage (WSL), le Laboratoire fédéral d'essai des matériaux et de recherche (Empa) et l'Institut fédéral pour l'aménagement, l'épuration et la protection des eaux (Eawag), <https://www.sbfi.admin.ch/sbfi/fr/home/he/hautes-ecoles/le-domaine-des-epf.html>.
128 Conseil des EPF, Strategic Planning 2021–2024, p. 24.
129 Conseil des EPF, Strategic Planning 2021–2024, p. 24.

inestimable pour réaliser les objectifs de santé publique de la Confédération. Pour pouvoir être utilisées à d'autres fins que celles prévalant au moment de la collecte, tout responsable du traitement sur ces données de santé devra au préalable s'enquérir de la légalité d'une éventuelle réutilisation de ces données personnelles.

De nombreuses institutions de recherche ont pour mission d'encourager l'innovation. D'aucuns pourraient voir derrière le terme innovation les intentions commerciales des institutions de recherche. Si les institutions de recherche poursuivent légitimement des buts lucratifs[130] (que ce soit au travers de la réalisation de services ou de l'octroi de licences payantes relatives à la propriété intellectuelle développée et protégée au sein des institutions à des *start-ups* souvent issues du travail généré au sein des institutions), les recettes de ces activités commerciales n'ont pas pour objectif d'enrichir les chercheurs ni ces institutions, mais de servir l'intérêt général en favorisant la création d'entreprises ou d'emplois, et en obtenant un remboursement partiel de certains coûts engendrés par les activités de recherche ou par les coûteuses procédures d'enregistrement de droits de propriété intellectuelle. Partant, les institutions déposent les brevets d'invention issus de la recherche menée en leur sein en vue de les licencier à des tiers tout comme les logiciels dont elles détiennent les droits exclusifs[131].

Les institutions de recherche ont conscience de la valeur du nombre de données personnelles qu'elles ont pu constituer au travers du temps et qu'elles continueront de créer. Nous allons donc nous demander quelles seraient les limites juridiques applicables si des institutions de recherche souhaitaient valoriser également les données de santé collectées dans des projets de recherche. Mais avant, il nous faut mentionner le régime applicable à la réutilisation des données de santé selon la LRH (*cf. infra* IV, A.), puis construire une analogie avec les règles pertinentes entourant l'extra-commercialité du corps humain (*cf. infra* IV, B).

H. Aperçu du régime applicable à la réutilisation des données de santé selon la LRH

Nous allons brièvement rappeler les règles qui prévalent lors de la réutilisation de données de santé. En l'occurrence, si les données de santé sont réutilisées pour effectuer une recherche en lien avec une maladie humaine ou

130 Art. 2 al. 1 lit. d et e et art. 10 loi sur les EPF ; art. 2 al. 1 lit. d et g Loi vaudoise sur l'Université de Lausanne ; art. 2 al. 2 de la Loi genevoise sur l'Université.

131 Ordonnance du Conseil des EPF sur les biens immatériels dans le domaine des EPF ; Règlement sur la valorisation des résultats de recherche au sein de l'Université de Lausanne et des Hospices cantonaux.

sur la structure et le fonctionnement du corps humain, la LRH peut s'appliquer (art 2 al. 1 LRH). Le terme recherche doit être compris de manière relativement large : il est défini comme de la recherche méthodologique de connaissances généralisables[132]. Quant au terme maladie, il se réfère tant aux diagnostics relatifs à des troubles physiques ou psychiques, mais aussi à leur prévention, leur thérapie, ou leur épidémiologie[133]. La recherche sur la structure et le fonctionnement du corps humain renvoie notamment à la recherche générale de base dans les domaines de l'anatomie, de la physiologie et de la pathophysiologie, ainsi que de la génétique du corps humain[134].

Si un projet remplit les conditions exigées par la LRH, et pour autant que les données reçues n'ont pas été anonymisées ou qu'elles n'ont pas été collectées anonymement (art. 2 al. 2 let c LRH), les exigences de la LRH et de ses ordonnances devront être suivies.

Une réutilisation de données de santé peut se matérialiser lors de l'acquisition de telles données personnelles, lors de leur enregistrement ou de leur catalogage, lors de leur saisie dans une banque de données, voire lorsqu'elles sont rendues accessibles ou communiquées (art. 24 de l'Ordonnance relative à la recherche sur l'être humain, ci-après « ORH »[135]).

Toute réutilisation de données personnelles de santé, collectées antérieurement, dans un projet de recherche soumis à la LRH doit obtenir au préalable l'approbation de la commission éthique compétente (art. 45 al. 1 lit. b LRH et art. 33 ORH). Un chercheur pourra se fonder sur plusieurs bases de légitimité pour sa recherche : le consentement spécifique du patient, le consentement général du patient, ou, en l'absence de consentement du patient, sur décision exceptionnelle de la commission d'éthique compétente après que cette dernière ait jugée, en particulier, que l'intérêt de la science prime sur celui de la personne concernée à décider du sort de ses données (art. 32, art. 33 et art. 34 LRH)[136]. Le choix de la base de légitimité se détermine en fonction du type de données personnelles, à savoir si elles comprennent des données génétiques, et en fonction de leur format, c'est-à-dire si elles sont anonymisées, codées, ou non codées (art. 32 et 33 LRH). S'il est nécessaire, le consentement devra être éclairé, ce qui exige de remplir son devoir d'information envers le patient (art. 16 al. 1 LRH). Dans tous les cas, une information sera fournie au patient. L'étendue de l'information à donner dépend également du type et du format des données

132 FF 2009 7259, p. 7307.
133 FF 2009 7259, p. 7308.
134 FF 2009 7259, p. 7309.
135 Ordonnance fédérale du 20 septembre 2013 relative à la recherche sur l'être humain (ORH), RS 810.301.
136 En pratique, il semble néanmoins que l'exception confirme la règle puisque les réutilisations de données personnelles sont souvent demandées sur la base de l'art. 34 LRH (voir DRIESSEN/CHRISTEN/GERVASONI).

personnelles concernées (art. 8 et/ou art. 28ss ORH). L'exportation éventuelle de données génétiques à l'étranger requiert le consentement éclairé de la personne, et le respect du régime dévolu aux communications à l'étranger lorsqu'il ne s'agit pas de données génétiques (art. 42 LRH). Enfin, tout projet de recherche réutilisant des données personnelles devra se conformer aux principes généraux ancrés dans la LRH, notamment le principe de primauté des intérêts de l'être humain (art. 4 LRH), le principe du consentement (art. 7), ou encore l'interdiction de commercialiser le corps humain (art. 9 LRH).

I. La non-patrimonialité des données de santé ?

Avant d'analyser si des données de santé peuvent être commercialisées, nous aimerions nous référer par analogie à ce qui s'applique au matériel biologique humain et, plus généralement, au corps humain. À notre sens, les limites à la commercialisation du corps humain ressortissent à la protection de la personnalité et du principe de non-patrimonialité du corps humain.

La protection de la personnalité est régie par le Code civil, aux art. 27 à 30*b* CC[137], et vise à protéger les valeurs qui constituent l'essentiel du domaine personnel de l'individu[138]. La personnalité comprend tout ce qui sert à individualiser une personne et qui apparaît comme digne de protection au regard des bonnes mœurs[139]. Elle regroupe les biens, les faits, les espaces, la réputation qui rend unique une personne[140]. Par exemple, elle concrétise le droit à l'honneur[141], la protection de la sphère privée ou secrète[142], le droit à la considération sociale[143], ou encore le droit à l'image[144]. Par ailleurs, le corps humain et ses éléments sont, pour beaucoup d'entre eux, des biens de la personnalité[145]. Concernant le corps humain, le droit suisse régule le sort des parties du corps dans différentes lois spéciales. On distingue ainsi la personne par destination (implants ou dispositifs qui sont réputés faire partie intégrante du corps humain ; p. ex. des prothèses ou valves cardiaques), l'objet humain et la chose d'origine humaine[146]. Pour les objets humains, comme des échantillons biologiques ou des gamètes, le lien que ces choses entretiennent avec la personne source est

137 Code civil suisse du 10 décembre 1907 (CC), RS 210.
138 BUCHER, p. 87, n. 384.
139 ATF 143 III 297, c. 6.4.1.
140 ATF 143 III 297, c. 6.4.1.
141 ATF 96 IV 148, p. 149.
142 ATF 97 II 97, c. 2.
143 ATF 121 III 168, c. 3a.
144 ATF 143 III 205, c. 4.3.3.
145 DUCOR, p. 251-348 ; MANAÏ, p. 171 ; le corps humain étant un bien de la personnalité selon la FF 2009 7259, p. 7315.
146 DUCOR, p. 251-348.

important. Elles sont donc subordonnées aux règles spéciales ou aux droits de la personnalité. Quant aux choses d'origine humaine comme des cheveux, calculs rénaux, transplants standardisés ou certaines lignées cellulaires, le lien que ces choses entretiennent avec la personne source est très distendu. Elles ont par exemple été modifiées à tel point par la main de l'homme qu'elles sont devenues autre chose[147]. Dans le but de protéger la dignité humaine et la personnalité d'un être humain, on notera par exemple que la Constitution suisse prohibe le commerce d'organes humains (art. 119*a* al. 3 *in fine* Cst.) et le commerce de matériel germinal humain et des produits résultant d'embryons (art. 119 al. 2 let. e), l'art. 7 de Loi fédérale sur la transplantation d'organes, de tissus et de cellules du 8 octobre 2004 (ci-après : « Loi sur la transplantation »[148]) interdit de faire le commerce d'organes, de tissus ou de cellules d'origine humaine en Suisse ou à l'étranger à partir de la Suisse[149], et que l'art. 9 LRH interdit de faire commerce du corps humain et des parties du corps humain.

En parallèle à l'existence d'une protection de la personnalité en droit suisse, le principe de non-patrimonialité du corps humain est consacré par la Convention d'Oviedo, promulguée par le Conseil de l'Europe, qui est entrée en vigueur en Suisse le 1er novembre 2008. En particulier, l'art. 21 de la convention dispose ce qui suit : « *Le corps humain et ses parties ne doivent pas être, en tant que tels, source de profit* ». L'art. 22 précise en outre que si une partie du corps humain a été néanmoins prélevé, celle-ci doit être utilisée et conservée uniquement dans le but pour lequel son prélèvement a été effectué conformément aux procédures d'information et de consentement. Ce principe n'a toutefois pas été spécifiquement concrétisé en Suisse et ne figure pas dans une disposition légale générale, bien que le commerce de matériel biologique humain soit considéré comme contraire aux mœurs[150]; dans le domaine biomédical, deux principes en sont tout de même tirés : celui de la gratuité et celui de la non-commercialisation[151]. L'interdiction du commerce s'étend ainsi à toute obtention d'un avantage quelconque en échange d'organes humains, de matériel germinal humain, de produits issus d'embryons, aux tissus et cellules d'origine humaine[152]. Cette

147 DUCOR, p. 251-348 ; FF 2009 7259, p. 7316. On relèvera par ailleurs que plusieurs décisions américaines ont admis que le produit de la recherche développé à partir de tissus humains est distinct sur le plan factuel et juridique du tissu d'origine et devient à ce titre la propriété du chercheur, le donneur ne conservant aucun droit (Supreme Court of California, *Moore v. Regents of the University of California* du 9 juillet 1990 ; United States District Court for the Southern District of Florida, *Greenberg v. Miami Children's Hospital Research Institute*, du 29 mai 2003).

148 Loi fédérale du 8 octobre 2004 sur la transplantation d'organes, de tissus et de cellules (Loi sur la transplantation), RS 810.21.

149 FF 2002 19, p. 135.

150 FF 2009 7259, p. 7359.

151 MANAÏ, p. 169.

152 MANAÏ, p. 178-179.

prohibition ne s'applique pas au remboursement des coûts liés à la transplantation, notamment aux coûts du prélèvement, du transport, du traitement, de la conservation et de la transplantation elle-même, ni aux transplants standardisés[153] (art. 7 al. 2 Loi sur la transplantation). Le principe de non-patrimonialité a pour objectif de contrecarrer la marchandisation du corps[154] et certains États ont élaboré des principes de protection du corps[155]. Cependant, ce principe est plutôt malmené et souffre de nombreuses exceptions à travers le monde[156]. En réalité, ce principe aurait vocation à jouer pleinement son rôle pour « *bannir tout paiement qui porterait sur la personne elle-même* »[157].

En appliquant ces principes aux biobanques, qui sont donc des collections de matériel biologique, il en ressort que leur commercialisation est plutôt controversée. La plupart des biobanques sont organisées sous la forme d'organisation à but non lucratif. Pour la Commission européenne et la Commission nationale pour la médecine humaine[158], puisque le donateur du matériel biologique s'est séparé d'une partie de son corps – un objet humain – de façon altruiste, les biobanques ne devraient pas poursuivre de but lucratif et devraient s'engager à servir l'intérêt général. Par ailleurs, selon la Commission nationale pour la médecine humaine, si elles sont financées par des fonds publics, leurs activités lucratives devraient servir uniquement à indemniser leurs coûts de fonctionnement. Paradoxalement, toujours selon cette commission, « *une biobanque devrait* [néanmoins] *être libre de prévoir, dans les accords de transfert conclus avec des équipes de recherche, une participation aux revenus générés par les projets de recherche qu'elle a soutenus* » et « *ne saurait par ailleurs être assimilée à une commercialisation moralement inadmissible du matériel biologique humain* » sans plus de précision[159]. À notre sens, en partant du postulat que des revenus tirés de l'exploitation de droits de propriété intellectuelle soit juridiquement acceptable, il serait conseillé de se conformer à la Déclaration de Taipei[160]. Un consentement serait donc valable uniquement si les personnes concernées ont été notamment informées de manière adéquate sur l'utilisation commerciale et le partage des bénéfices, la propriété intellectuelle et le transfert de données ou de matériel à d'autres institutions ou à des pays tiers (art. 12 *in fine* de cette Déclaration).

---

153 Par transplants standardisés, il faut entendre les produits fabriqués à partir d'organes, de tissus ou de cellules d'origine humaine ou animale, qui peuvent être standardisés ou dont le processus de fabrication peut être standardisé (FF 2002 19, p. 132).

154 LE BRETON, Patrimonialité du corps, p. 353.

155 FEUILLET-LIGER/SCHAMPS.

156 FEUILLET-LIGER, p. 390 ss.

157 P. ex., dans le cas des gestations pour autrui, voir FEUILLET-LIGER, p. 411.

158 CE, Ethical aspects of human tissue banking, 1.10 ; CNE, Prise de position nº 24/2015, p. 63 ss, n. 185 ss.

159 CNE, Prise de position nº 24/2015, p. 63 ss, n. 85 ss.

160 Association Médicale Mondiale, Déclaration de l'AMM.

Concernant l'exploitation de données de santé, rien ne semble prohiber une éventuelle commercialisation des données personnelles, tant que le cadre légal est respecté[161]. En réalité, en tant qu'attributs de la personnalité, de telles données personnelles sont des droits absolus strictement personnels qui ne peuvent pas être cédés *stricto sensu* ; seul leur usage peut être cédé dans les limites de la loi[162]. Le responsable du traitement devra généralement obtenir le consentement libre et éclairé de la personne concernée au moment de leur collecte. La liberté de disposer des données personnelles est toutefois tempérée par l'interdiction des engagements excessifs au sens de l'art. 27 al. 2 CC, par le respect des droits de la personnalité (art. 28 CC), mais aussi par l'art. 20 al. 1 de la loi fédérale complétant le Code civil suisse du 30 mars 1911 (ci-après : « CO »[163]). Dans tous les cas, un engagement qui serait contraire aux mœurs pourrait être qualifié d'excessif voire être frappé de nullité. *A fortiori*, tout comme certaines parties du corps humain, les données de santé, de par leur nature sensible, nouent avec le corps humain un lien privilégié en décrivant l'état de santé, des attributs physiologiques ou métaboliques du patient, voire même des informations génétiques ou génomiques. Par analogie avec le principe de non-patrimonialité, nous pensons que le commerce de données de santé devrait également être contraire aux bonnes mœurs.

Premièrement, il est important de préserver la confiance des patients dans la médecine ou la science. Selon l'institut de sondage *Sotomo*, en 2022, les Suisses sont pour la première fois majoritairement en faveur de mettre à disposition leurs données de santé au secteur de la recherche médicale[164]. Un autre sondage européen tend à confirmer que le niveau de confiance des citoyens-patients est loin d'être acquis[165]. Il est à craindre qu'une commercialisation des données de santé – fût-ce indirecte – ruinerait la confiance des Suisses à confier leurs données de santé aux institutions de recherche.

Deuxièmement, dans une perspective plus philosophique que juridique, nous devrions au moins réfléchir aux conséquences de la réification des attributs humains, dont font partie à notre sens les données de santé, et à pousser la réflexion sur le transhumanisme et ses éventuelles dérives[166]. Le transhumanisme

161 CELLINA, p. 209 ss.
162 CELLINA, p. 212, n. 872.
163 Loi fédérale complétant le Code civil suisse du 30 mars 1911 (Livre Cinquième : Droit des obligations), RS 220.
164 Sotomo, Opinion et comportement de la population suisse 2022, p. 38.
165 BEUC, p. 9 notamment.
166 FERRY/ONFRAY, p. 34 ss ; FERRY. Par ailleurs, en France, lors de la deuxième révision de la loi nº 2011-814 relative à la bioéthique, le rapport *Leonetti* listait un certain nombre de problèmes éthiques liés au transhumanisme : l'emploi de substances pour avoir de meilleurs enfants, l'amélioration de performances physiques à l'aide de substance, détournement de la fonction de la médecine qui deviendrait une anthropotechnie, *etc*. (Assemblée nationale française, Rapport d'information, n. 1027 ss).

est, selon le sociologue David LE BRETON, une pensée « *qui revendique une recherche scientifique illimitée et une application immédiate à l'humain des modifications génétiques, du clonage, de la transgenèse, des nanotechnologies, du couplage du cerveau et de l'informatique, etc.* »[167]. Avec la marchandisation du corps, de ses attributs ou même ses données, nous pourrions craindre une déshumanisation par la perte de la spécificité de l'être humain et de sa dignité[168]. Surtout, il est souvent difficile de juger sur un plan moral et éthique ce qui serait acceptable, de ce qui ne le serait pas.

Troisièmement, la fourniture de données de santé est une activité qui relève des missions du secteur public. Les organismes du secteur public devraient rendre ces données disponibles à un coût inférieur à celui consenti ou même gratuitement, par exemple pour certaines finalités de réutilisation non commerciales ou pour leur réutilisation par des petites et moyennes entreprises, de manière à encourager leur utilisation secondaire afin de stimuler la recherche et l'innovation[169].

Une valorisation commerciale des données de santé elles-mêmes, à savoir en tant qu'objet de la valorisation, ne saurait être admissible. Du fait de la non-patrimonialité des données de santé (*cf. supra* IV, B.), cette commercialisation paraît hautement hasardeuse tant d'un point de vue éthique que juridique. Le modèle de consentement général développé par *swissethics*, association suisse des commissions d'éthique de la recherche confirme ce principe du fait de l'incorporation d'une section sur les bénéfices financiers escomptés, laquelle est libellée comme suit : « *La loi exclut la commercialisation des données et des échantillons. Ainsi, aucun avantage financier ne sera généré pour vous ou pour l'hôpital* »[170]. À supposer que l'on admette la valorisation commerciale des données de santé en tant que telles, ce procédé relèverait d'un but commercial. Les participants à la recherche devraient dans cette hypothèse donner leur consentement éclairé spécifique à ce propos (art. 41 let. b LRH). Le consentement des sujets à la recherche devrait être revu sur ce point le cas échéant, par exemple en prévoyant un consentement séparé car l'objectif recherché sort du but de recherche scientifique. En outre, un participant à un projet de recherche sur l'être humain doit notamment recevoir une information compréhensible sur le bénéfice escompté du projet de recherche, notamment pour elle-même mais aussi pour d'autres personnes (art. 16 al. 2 lit. c LRH). Finalement, éthiquement, il n'est pas acceptable de donner des informations incomplètes et amener des

167 LE BRETON, Le transhumanisme ou l'adieu au corps, p. 81-93.

168 FEUILLET-LIGER, p. 398 ; Décision nº 94-343/344 du Conseil constitutionnel français (DC) du 27 juillet 1994, Loi relative au respect du corps humain et loi relative au don et à l'utilisation des éléments et produits du corps humain, à l'assistance médicale à la procréation et au diagnostic prénatal, JORF du 29 juillet 1994, p. 11024, point 18.

169 COM/2020/767 final (considérant 20).

170 <https://swissethics.ch/fr/templates/studieninformationen-und-einwilligungen>.

patients à donner un consentement qu'ils n'auraient pas donné s'ils avaient reçu des informations plus complètes ou plus conformes à la vérité[171].

La commercialisation directe des données de santé ne se confond pas avec les revenus générés suite à la commercialisation d'un produit matériel (une vente d'un dispositif médical par exemple) ni avec les redevances issues d'un bien immatériel (comme une licence payante concernant un brevet d'invention) tous deux développés également à l'aide de données de santé dans un contexte de recherche. Ce type de commercialisation est acceptable selon nous car la valorisation onéreuse concerne le bien matériel ou immatériel et en aucun cas les données de santé elles-mêmes, qui peuvent être des éléments utiles à la création dudit bien. En effet, l'innovation fait partie intégrante de la recherche et les institutions de recherche sont transparentes vis-à-vis du citoyen à ce sujet[172]. Au surplus, les patients mettant à disposition leurs données de santé à des fins de recherche savent – ou devraient savoir – que la recherche menée vise à développer des biens matériels ou immatériels. Tant l'art. 16 al. 2 let. c LRH que les art. 12 et 18 de la Déclaration de Taipei exigent, à notre avis, un devoir accru de transparence vis-à-vis du patient dans l'hypothèse où un projet de recherche viserait aussi l'exploitation de droits de propriété intellectuelle générant un bénéfice financier.

Quant au travail effectué sur des données de santé, nous pensons, par exemple, aux activités de curation opérées par des *data scientists* ou des médecins consistant à sélectionner les données de santé, à standardiser leur structure ou leur format, à les agrémenter éventuellement de données médicales ou démographiques supplémentaires, et enfin à décider des modalités de conservation de ces données de santé, ce dans le but de rendre les données plus exploitables et de les préserver sur un long terme (*data curation*). Ces tâches effectuées sur les données de santé ne sauraient autoriser une rémunération avec pour seule contrepartie la fourniture de données de santé « travaillées », car le principe de non-patrimonialité des données évoquée plus haut l'interdirait (cf. *supra* IV, B). L'exécution de ces activités par les spécialistes est inhérente à des compétences particulières (savoir-faire, compétences techniques) et revêt ainsi des caractéristiques d'une prestation de services qui peut, quant à elle, faire l'objet d'un contrat commercial contrairement aux données « travaillées ». Même si ces dernières données ont acquis une certaine valeur supplémentaire d'un point de vue scientifique, cette plus-value ne pourrait pas être valorisée en tant que telle, car elle est indissociable des données de santé et ne consiste pas en un

171 ASSM, Guide pratique, p. 68, n. 8.3 ; en faveur d'une plus grande transparence, voir aussi Association Médicale Mondiale, Déclaration de l'AMM, art. 12.

172 À titre d'exemple, en vertu de l'article 36 Loi sur les EPF, les écoles polytechniques fédérales exploitent certains biens immatériels créés par leurs chercheurs conformément à la législation qui s'applique. Enfin, dans la pratique, les personnes concernées devraient toujours au moins être informées de cette finalité commerciale.

bien immatériel valorisable au sens de la loi. Seuls les coûts supportés pour les activités de curation pourraient alors être remboursés par le truchement d'un contrat de prestation de services ou un système de redevance légal. Par ailleurs, plus le fournisseur de données souhaite obtenir une marge importante, plus la probabilité que le fournisseur de données poursuive un but lucratif est grande, ce qui supposerait que les patients aient été au moins informés de l'existence de cet objectif commercial.

J. Conclusion intermédiaire

En définitive, il nous semble légitime de questionner l'objet de la valorisation avant de définir l'admissibilité de cette dernière, la forme qu'elle peut prendre ainsi que ses modalités (commercialité ou non). La valorisation directe des données de santé ne saurait être admissible d'un point de vue éthique et juridique selon nous. Dans la mesure où leur commerce serait juridiquement envisageable, nous conseillons fortement à tout fournisseur de données de santé, qui souhaite valoriser les données de santé en sa possession, d'obtenir un consentement éclairé du participant au sujet de la commercialisation directe de ses données de santé. Dans tous les cas, tout objectif commercial devrait être révélé de manière transparente vis-à-vis du patient.

V. Conclusion

Nous constatons quatre domaines principaux où l'on souhaite valoriser des données de recherche au sein des institutions de recherche suisses : dans le domaine de l'intelligence artificielle, dans le domaine de la gouvernance des données (ou le pilotage des institutions de recherche), dans le domaine de la recherche scientifique avec les nouvelles obligations d'ouverture et d'accessibilité des données et dans le domaine de la santé et de la médecine personnalisées.

Dans le domaine de la recherche, la valorisation des données n'implique pas automatiquement une exploitation commerciale des données en tant que telles. Si les données prennent de la valeur, c'est bien parce qu'on leur attribue une utilité ou un but nouveau, que ce soit sous l'impulsion de choix politiques, ou grâce au développement des nouvelles technologies ou à une progression de la numérisation au sein des institutions de recherche. De ce fait, les données deviennent utiles et attractives. Une donnée peut ainsi être vue comme un actif numérique car elle comporte un potentiel de création de valeur en favorisant le développement de nouveaux services ou le rayonnement du contenu généré[173].

[173] MONINO/SEDKAOUI, p. 107 ss.

Notre premier constat est que la prise de valeur des données de recherche génère aussi une volonté accrue de les exploiter commercialement. Comme nous l'avons mentionné ci-dessus en rapport avec les données de santé (*cf supra* IV, B), celles-ci ne sauraient être directement commercialisées par les fournisseurs de données, mais pourraient être valorisées, par exemple, au travers de l'*Ouverture des données de recherche (Open Research Data)* (ORD), si les conditions légales le permettent, ou grâce au développement de biens immatériels. À supposer qu'une commercialisation directe soit admise, le consentement de la personne concernée devra être obtenu pour se conformer aux exigences éthiques et juridiques. Au surplus, nous recommandons avant toute valorisation qu'une analyse de son objet soit accomplie avant de définir sa forme et ses modalités incluant une probable commercialisation.

Notre deuxième constat est qu'à l'heure du développement des technologies comme l'intelligence artificielle ou le *big data*, la valorisation des données de recherche est de plus en plus significative dans le quotidien d'un chercheur. La valorisation des données contribue non seulement à des besoins sociétaux et économiques majeurs, mais également à la visibilité du chercheur dans son domaine scientifique de prédilection et à l'augmentation de son *h-index*[174].

Troisièmement, les activités de valorisation de ces actifs numériques que sont les données de recherche peuvent parfois entrer en contradiction avec certaines normes en protection des données. Outre le respect des normes légales, il est primordial de préserver la confiance des utilisateurs, citoyens, ou patients envers la science, la médecine, ou les autorités. Les objectifs affichés sont légitimes pour ne pas dire primordiaux dans le contexte de la société de connaissance et d'une concurrence mondiale du savoir. Il n'en demeure pas moins que rien de tout cela ne sera pérenne sans la préservation de la confiance des personnes concernées et sans la fourniture d'efforts supplémentaires en matière de transparence.

Enfin, il est requis de prendre des mesures pour accompagner les chercheurs dans cette mission des institutions publiques en plein essor, notamment en les soutenant, en améliorant l'écosystème des services et infrastructure des données de recherche (qui soutiennent la pratique ORD), en accroissant la disponibilité et la qualité de la formation sur la gestion des données de recherche (en application des pratiques ORD) et en apportant un soutien juridique aux chercheurs. Pour conclure, l'élaboration d'un cadre juridique pour réglementer la réutilisation des données détenues par le secteur public et faisant l'objet de droits de tiers, similaire à celui dont s'est dotée la Communauté européenne[175], semble

174 Selon HIRSCH, le *h-index* est défini comme le nombre d'articles avec un nombre de citations supérieur à *h*, comme un indice utile pour caractériser la production scientifique d'un chercheur (HIRSCH).

175 Directive UE 2019/1024 et le Règlement UE 2022/868 : entre autres, pour éviter que des expectatives financières constituent une barrière à la réutilisation des données, et

utile et nécessaire au niveau suisse également[176]. Cette législation permettrait de favoriser la disponibilité des données en vue de leur utilisation, en augmentant la confiance dans les intermédiaires de données et en renforçant le mécanisme de partage au niveau national voire international.

VI. Bibliographie

A. Littérature

Regina Aebi-Müller/Walter Fellmann/Thomas Gächter/Bernhard Rütsche/Brigitte Tag, Arztrecht, Bern 2016 ; **Sarah S. Amsler/Chris Bolsmann**, University ranking as social exclusion, British Journal of Sociology of Education, 33(2), 2012 ; **Bruno Beariswyl/Kurt Pärli (éds)**, Datenschutz – Stämpfli Handkommentar, Berne 2015 (cité : SHK DSG-auteur) ; **Bo-Christer Björk**, Gold, green, and black open access, in Wiley Online Library, 7 février 2017 ; **Bertrand Braunschweig/Malik Ghallab**, Reflections on AI for Humanity: Introduction, in Reflections on Artificial Intelligence for Humanity, 2021 ; **Andreas Bucher**, Personnes physiques et protection de la personnalité, 5e éd., Bâle 2009 ; **Eva Cellina**, La commercialisation des données personnelles, Aspect de droit contractuel et de protection des données, Genève 2020 ; **Isabelle Collin-Lachaud/Géraldine Michel**, Valoriser la recherche : une nouvelle mission des enseignants-chercheurs ?, Décisions Marketing, 2020/1 (No 97), p. 5-16 ; **Henri Deschenaux/Paul-Henri Steinauer**, Personne physiques et tutelles, 4e éd., Berne 2001 ; **Susanne Driessen/Andri Christen/Pietro Gervasoni**, Humanforschung, Weiterverwendung und informierte Einwilligung, in: Jusletter 1er février 2021 ; **Philippe Ducor**, Statut juridique des parties détachées du corps humain, Une approche anatomique et fonctionnelle, Zeitschrift für Papyrologie und Epigraphik, 2016, vol. 135/ Halbbd. 2, no 1 ; **Astrid Epiney**, Datenschutzrechtliche Grundsätze und Garantien *in* : Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (éds), Datenschutzrecht, Berne 2011 ; **Frédéric Erard**, Le secret médical, Étude des obligations de confidentialité des soignants en droit suisse, Thèse Neuchâtel, Zürich 2021 ; **Frédéric Erard/Mathilde Heusghem/ Clément Parisato**, Recherche biomédicale et Open Data, Jusletter 30 janvier 2023 ; **Luc**

en dérogation au principe de gratuité, l'Union européenne admet la rémunération des coûts dits marginaux qui peuvent recouvrir des coûts issus d'une recherche particulièrement approfondie portant sur les données, de modifications extrêmement coûteuses du format des données, ou admet aussi le paiement de redevance qui permet à l'entité publique de générer des recettes destinées à couvrir une part substantielle des coûts liés à l'accomplissement d'autres missions de service public (Préambule de la Directive UE 2019/1024, consid. 36 ss). Ces redevances devraient être fixées selon des critères objectifs, transparents et vérifiables, et le total des recettes acquises de ce chef ne devrait pas dépasser les coûts afférents à la collecte et à la production, y compris l'achat auprès de tiers, à la reproduction, à la maintenance, à la conservation et à la diffusion, le tout en permettant un retour sur investissement raisonnable (au maximum de 5 % par exemple), voire également les coûts supportés en raison des mesures prises pour assurer l'anonymisation ou la confidentialité des données (Préambule de la Directive UE 2019/1024, consid. 36 ss).

176 Motion CSEC, no 22.3890, « Élaboration d'une loi-cadre sur la réutilisation des données » du 22 août 2022.

Ferry, La révolution transhumaniste, Paris 2016 ; **Luc Ferry/Michel Onfray**, Le transhumanisme, progrès de la civilisation ou barbarie ?, propos recueillis par Alexandre Devecchio et Raphaël Pinault, Le Figaro Magazine du 14 octobre 2022 ; **Brigitte Feuillet-Liger**, La non-patrimonialité du corps humain : un principe sans l'être !, *in* Brigitte Feuillet-Liger/Saïbe Oktay-Özdemir (éds), La non-patrimonialité du corps humain : du principe à la réalité, Panorama international, Bruxelles 2017, p. 385 ss ; **Brigitte Feuillet-Liger/Geneviève Schamps**, Principes de protection du corps et biomédecine, approche internationale, Bruxelles 2015 ; **Philipp Fischer/Sébastien Pittet**, L'utilisation de services *cloud* par des responsables du traitement privés, *in* Sylvain Métille (éd.), L'informatique en nuage, Collection CEDIDAC, Berne 2022 ; **Urs Gasser/Virgilio A. F. Almeida**, A Layered Model for AI Governance, IEEE Internet Computing, November/December 2017 ; **Dave Hill**, Globalisation and its educational discontents: Neoliberalisation and its impacts on education workers' rights, pay and conditions, International Studies in Sociology of Education, Vol. 15, 2005 ; **Jorge E. Hirsch**, An index to quantify an individual's scientific research output, Proceedings of the National Academy of Science, The National Academy of Science, Washington (USA), 2005 ; **Heike Jöns/Michael Hoyler**, Global Geographies of Higher Education: The Perspective of World University Rankings, Geoforum, Volume 46, May 2013 ; **Maxi Kindling/Peter Schirmbacher**, „Die digitale Forschungswelt" als Gegenstand der Forschung, in Information – Wissenschaft & Praxis, 2013 ; **Katrin Kinzelbach/Ilyas Saliba/Janika Spannagel**, Global data on the freedom indispensable for scientific research: towards a reconciliation of academic reputation and academic freedom, in The International Journal of Human Rights, 2021 ; **Karin Koç**, Datenschutz in Statistik und Forschung, *in* Nicolas Passadelis/David Rosenthal/Hanspeter Thür (éds.), Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Bâle 2015 ; **David Le Breton**, Le transhumanisme ou l'adieu au corps, Écologie et politique 2017/2, Lormont, 2017 ; **David Le Breton**, Patrimonialité du corps : approche anthropologique, *in* Brigitte Feuillet-Liger/Saïbe Oktay-Özdemir (éds), La non-patrimonialité du corps humain : du principe à la réalité, Panorama international, Bruylant, Bruxelles 2017, p. 351 ss ; **Nadine Levin/Sabina Leonelli/Dagmara Weckowska/David Castle/John Dupré**, How Do Scientists Define Open-ness? Exploring the Relationship between Open Science Policies and Research Practice, Bulletin of Science, Technology & Society, 36 (2), 2016 ; **Pasquale Lops/Giovanni Semeraro/Marco de Gemmis/Fedelucio Narducci**, Leveraging the LinkedIn social network data for extracting content-based user profiles, Octobre 2011 ; **Kathleen Lynch**, Control by numbers: new managerialism and ranking in higher education, in Critical Studies in Education, 56:2, 2015 ; **Dominique Manaï**, Gratuité et non-commercialisation du corps humain en droit Suisse : des valeurs relatives, *in* Brigitte Feuillet-Liger/Saïbe Oktay-Özdemir(éds), La non-patrimonialité du corps humain : du principe à la réalité, Panorama international, Bruxelles 2017, p. 169 ss ; **Samuel Mätzler**, Datenschutz in der (Human-)Forschung: Grundlagen und Probleme bei der Sekundärnutzung von Personendaten, Jusletter 30 janvier 2023 ; **Urs Maurer-Lambrou (éd.)**, Basler Kommentar Datenschutzgesetz / Öffentlichkeitsgesetz, 3e édition, Bâle, 2014 (cité : BsK DSG-Auteur) ; **Urs Maurer/Nadim Peter Vogt (éds)**, Kommentar zum schweizerischen Datenschutzgesetz, Bâle 1995 (cité : K-DSG-Auteur) ; **Philippe Meier/Sylvain Métille (éds)**, Loi sur la protection des données, Commentaire romand, 1re éd., Bâle 2023 (cité : CR LPD Auteur, art. X, N Y) ; **Sylvain Métille**, Le traitement de données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données personnelles du 25 septembre 2020, SJ 2021 II ; **Jean-Louis Monino/Soraya Sedkaoui**, Big Data, Open Data et valorisation des données, Volume 4, ISTE Group, Londres 2016 ; **Catherine Pugin**, La valorisation des données comme mission de l'État, Le Temps, 16 août 2022 ; **David Reinsel/John Gantz/**

John Rydning, The Digitization of the World From Edge to Core, in IDC White Paper, 2018 ; **David Rosenthal/Yvonne Jöhri (éds)**, Handkommentar zum Datenschutzgesetz, 2e édition, Zürich 2021 (cité : HK DSG-Auteur, art. X, N Y) ; **David Rosenthal**, Die rechtlichen und gefühlten Grenzen der Zweitnutzung von Personendaten, sic! (4) 2021 Forum – Zur Diskussion ; **David Rosenthal/Samira Studer/Alexandre Lombard** (pour la traduction), La nouvelle loi sur la protection des données, Jusletter 16 novembre 2020 ; **Florent Thouvenin/Nadja Braun Binder**, Transparenz durch Datenschutzerklärungen von Behörden, Zeitschrift für Schweizerisches Recht (ZSR), p. 5 ss ; **Kerstin Noëlle Vokinger**, Gesundheitsdaten im digitalen Zeitalter, Jusletter 27 janvier 2020 ; **Jakob Zanol/Alexander Buchelt/Simon Tjoa/Peter Kieseberg**, What is "AI"?, Jusletter IT 24 Février 2022.

B. Documents officiels

Académie Suisse des Sciences Médicales (ASSM), Recherche avec l'être humain, Guide pratique, 2e édition, 2015 ; **Académies suisses des sciences (ASS)**, Open Science in Switzerland: Opportunities and challenges, Swiss Academic Factsheet 14 (2), 2019 ; **Académies suisses des sciences (ASS)**, Code d'intégrité scientifique, 2021 ; **Article 29 Working Party**, Guidelines on transparency under Regulation 2016/679, tel que révisé et adopté en dernier lieu le 11 avril 2018 ; **Assemblée nationale française**, Doc. AN no 2235, Rapport fait au nom de la mission d'information sur la révision des lois de bioéthique, 10 janv. 2010 ; **Association Médicale Mondiale**, Déclaration de l'AMM sur les considérations éthiques concernant les bases de données de santé et les biobanques, Adoptée par la 53e Assemblée générale de l'AMM, Washington 2002 et révisée par la 67e Assemblée Générale, Taipei, Taiwan, Octobre 2016 ; **Beijing Academy of Artificial Intelligence (BAAI)**, Beijing AI Principles, daté du 28 mai 2019 ; **Bureau européen des unions de consommateurs (BEUC)**, Consumer attitudes to health data sharing, Survey results from eight EU countries, publiée en mai 2023 ; **Comité Européen de la Protection des Données (EDPB)**, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, adopté le 28 février 2023 ; **Commission européenne (CE)**, Proposition de Règlement du Parlement Européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle du 21 avril 2021 (cité : COM(2021) 206 final) ; **Commission européenne (CE)**, Proposition de Règlement du Parlement Européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données) du 25 novembre 2020 (cité : COM(2020) 767 final) ; **Commission européenne (CE)**, Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle constitué par la Commission européenne en juin 2018, Lignes directrices en matière d'éthique pour une IA digne de confiance, 2019 ; **Commission européenne (CE)**, Opinion of the European Group on Ethics in Science and New Technologies, Ethical aspects of human tissue banking, 21 juillet 1998 ; **Commission européenne (CE)**, White paper on artificial intelligence, A European approach to excellence and trust, du 19 février 2020 ; **Commission nationale d'éthique pour la médecine humaine (CNE)**, Prise de position no 24/2015, Les biobanques destinées à la recherche, Berne, décembre 2015 ; **Conférences des recteurs des hautes écoles/FNS**, Déclaration de Berlin sur le Libre Accès à la Connaissance en Sciences exactes, Sciences de la vie, Sciences humaines et sociales du 22 octobre 2003, signée en 2006 ; **Conseil de l'Europe**, Rapport explicatif de la Convention 108+, juin 2018 ; **Conseil des EPF (CEPF)**, Strategic Plan 2025–2028 of the ETH Board for the ETH Domain, Juin 2022 ; **Conseil des EPF**, Open Research Data, Position of the ETH Domain, adopté par les 13-

14 mai 2020 ; **Conseil Fédéral**, Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988 (cité : FF 1988 II 421) ; **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 : FF 2017 6565) ; **Conseil Fédéral**, Message concernant la loi fédérale sur la transplantation d'organes, de tissus et de cellules du 12 septembre 2001 (cité : FF 2002 19) ; **Conseil Fédéral**, Message concernant la révision partielle de la loi fédérale sur les écoles polytechniques fédérales (loi sur les EPF) du 27 février 2002 (cité : FF 2002 3251) ; **Conseil Fédéral**, Message relatif à l'encouragement de la formation, de la recherche et de l'innovation pendant les années 2017 à 2020 du 24 février 2016 (cité : FF 2016 2917) ; **Conseil Fédéral**, Message sur la loi fédérale relative à la recherche sur l'être humain du 21 octobre 2009 (cité : FF 2009 7259) ; **Département fédéral de l'intérieur (DFI)**, Mesures de la Confédération afin de renforcer la recherche et la technologie biomédicales du 18 décembre 2013 ; **Fonds national suisse de la recherche scientifique (FNS)**, Lettre ouverte du FNS aux éditeurs Elsevier, Springer Nature et Wiley, daté du 5 décembre 2019 ; **Fonds national suisse de la recherche scientifique (FNS)**, SNSF Open Research Data Policy ; **ISO**, 15489-1:2016, Information et documentation – Gestion des documents d'activité, seconde édition, avril 2016 (cité : ISO 15489-1:2016) ; **Office fédéral de la justice (OFJ)**, Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales du 21 décembre 2016 ; **Office fédéral de la santé publique (OFSP)**, Mesures de la Confédération afin de renforcer la recherche et la technologie biomédicales, Rapport 2022-2026 du 22 juin 2022 ; **Office fédéral de la santé publique (OFSP)**, Politique de la santé : stratégie du Conseil fédéral 2020-2030 ; **Open society Institute**, Déclaration de Budapest, Open Access Initiative du 14 février 2002, signée notamment par l'Université de Lausanne et la Haute école pédagogique du Canton de Vaud ; **Préposé fédéral à la protection des données et à la transparence (PFPDT)**, Guide pour l'examen de la licéité de la communication transfrontière de données (art. 6, al. 2, let. a, LPD), juin 2021 ; **Préposé fédéral à la protection des données et à la transparence (PFPDT)**, Stellungnahme zur Datenschutz Risikobeurteilung der Suva zum Projekt Digital Workplace «M365», 13 juin 2022 ; **Préposé fédéral à la protection des données et à la transparence (PFPDT)**, 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, 8 septembre 2020 ; **Secrétariat d'État à la formation, à la recherche et à l'innovation (SEFRI)**, Défis de l'intelligence artificielle, Rapport du groupe de travail interdépartemental « Intelligence artificielle » au Conseil fédéral, 2019 ; **Secrétariat général de l'EPFL,** Rapport complet de l'impact économique de l'EPFL, Décembre 2022 ; **SEFRI, swissuniversities, le Conseil des EPF, l'ETH Zurich, l'EPFL et le FNS**, Accord ORD pour l'élaboration de la Stratégie nationale suisse ORD et du plan d'action correspondant, janvier 2020 ; **Sotomo**, Observatoire « Société numérique et solidarité », Opinion et comportement de la population suisse 2022 ; **Swissuniversities**, Plan d'action sur la Stratégie nationale suisse sur l'Open Access, adopté le 8 février 2008 ; **Swissuniversities**, Stratégie Nationale Suisse Open Research Data, adopté le 23 avril 2021 ; **Swissuniversities**, Stratégie nationale suisse sur l'Open Access, adopté le 31 janvier 2017 ; **UNESCO**, Recommandation de l'UNESCO pour une science ouverte, 2021 ; **UNESCO**, Recommandation sur l'éthique de l'intelligence artificielle, adoptée le 23 novembre 2021.

La pollinisation croisée entre droit de la protection des données et droit de la non-discrimination

Le rôle des chercheurs pour garantir une intelligence artificielle non-discriminatoire

FABIAN LÜTZ
Doctorant en droit
Faculté de droit, Université de Lausanne

Table des matières

I. Introduction

Depuis une demi-décennie, la protection des données est régie par le Règlement général sur la protection des données (RGPD)[1] tant dans l'Union européenne[2] qu'en-dehors de la juridiction de l'UE, compte tenu de son effet extraterritorial[3] et à travers l'imitation, le fameux *Brussels effect*[4]. En Suisse, la nouvelle loi de la protection de données entrera en vigueur en septembre 2023, reprenant largement le contenu du RGPD, mais favorisant quelques spécificités suisses. Dans ce contexte, le *AI Act* proposé par la Commission européenne en 2021 et actuellement débattu par les colégislateurs, prévoit un cadre législatif pour réguler les algorithmes[5]. En Suisse, il n'y a pas encore de règles juridiques qui gouvernent spécifiquement l'intelligence artificielle (IA)[6] et la discrimination algorithmique sur la base d'une caractéristique protégée par le droit, par exemple le genre ou la religion, même si en principe les règles générales et plus

1 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) (Texte présentant de l'intérêt pour l'EEE), JO L 119, 4.5.2016, p. 1-88.

2 Voir MÉTILLE/DI TRIA.

3 Voir MÉTILLE/ACKERMANN.

4 BRADFORD, The Future of the Brussels Effect ; BRADFORD, Brussels Effect ; concernant l'égalité des genres, voir LÜTZ, Brussels effect, p. 142-163.

5 La dernière version disponible est le texte compromis du Conseil, <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/fr/pdf> et la position du Parlement européen, <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf>.

6 La Suisse s'engage néanmoins internationalement dans l'élaboration des règles, notamment en ce qui concerne le Conseil de l'Europe, voir par exemple, RICART *et. al*., p. 78.

particulièrement l'interdiction de la discrimination[7] s'appliquent également dans le contexte de l'IA[8]. C'est dans ce cadre législatif et politique que s'inscrit la présente comparaison et analyse du droit de la protection des données et du droit de la non-discrimination dans l'ère algorithmique[9]. Cette contribution vise à éclairer le(s) rôle(s) des chercheurs en sciences informatiques et juridiques au cours de l'élaboration des algorithmes ainsi qu'à faire la lumière sur leur implication dans le processus législatif.

S'il est souvent question d'équité (*fairness*) dans l'IA, ce concept est loin de faire l'unanimité parmi les théoriciens et la définition de cette *fairness* reste débattue.[10] Par conséquent, l'article privilégiera le concept plus concret et spécifique de l'IA non discriminatoire.

En guise d'introduction, l'article détaillera de manière générale les similarités, l'interdépendance, le potentiel pour l'imitation et la complémentarité entre les deux domaines du droit que sont la protection des données et de la non-discrimination, en se référant principalement au cadre juridique de l'Union européenne et de la Suisse (II.). Ensuite, seront examinés le droit à l'information et à la transparence (III.), la confiance et le droit à la participation d'un humain dans le processus (IV.), les questions de sphère privée et de non-discrimination dès la conception et par défaut (V.) et les analyses d'impact ainsi que le *monitoring* (VI.). L'article conclut en soulignant le rôle des chercheurs et en identifiant les pistes de participations des chercheurs afin d'assurer une meilleure protection des citoyens et de leurs droits fondamentaux.

II. Interdépendance, conflictualité, imitation et complémentarité

Dans l'ère algorithmique[11], le RGPD est sans aucun doute le produit d'exportation phare de l'Union européenne. Il est par conséquent devenu le

7 Par l'interdiction de discrimination on entend toutes les règles de droit qui visent à empêcher la discrimination sur la base d'une caractéristique protégée, tel que le sexe, la religion ou la race.

8 Voir par exemple l'explication du CONSEIL FÉDÉRAL, « Intelligence artificielle » – lignes directrices pour la Confédération, Cadre d'orientation en matière d'IA dans l'administration fédérale (2020), p. 9 concernant l'applicabilité des normes générales comme les droits fondamentaux, droits de l'homme et l'interdiction de la discrimination.

9 Pour un aperçu du *AI Act*, voir LÜTZ, Gender equality and AI in Europe, p. 33-52.

10 Il existe au moins 21 conceptions fréquemment discutées en sciences informatiques, voir BAROCAS/HARDT/NARAYANAN ; voir aussi sur les risques de qualification incorrecte par les algorithmes qui prennent des décisions « juste », CREEL/HELLMANN, p. 2.

11 ABITEBOUL/DOWEK, p. 1 et not. le titre de l'ouvrage.

centre de gravité global visant une convergence régulatrice en termes de protection des données[12]. Les données se situent au cœur de tous les projets récents de l'Union européenne en matière digitale dans cette *décennie numérique*[13], tels que le *Digital Markets Act* (DMA)[14], *Digital Services Act* (DSA)[15], *Data Governance Act* (DGA)[16], *Artificial Intelligence Act* (AI Act)[17]. Ce sont en effet principalement les données[18] qui font fonctionner les algorithmes, l'IA et les données étant interdépendantes.[19] Cependant, ce sont aussi ces données qui doivent être protégées au profit des individus. Le RGPD reconnaît que :

> « *Des risques pour les droits et libertés des personnes physiques* […] *peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier : lorsque le traitement peut donner lieu à une discrimination* […] ».[20].

---

12 Voir p. ex., SMUHA ; BENBOUZID/MENECEUR/SMUHA, p. 29-64 ; La nouvelle LPD en Suisse par exemple est très similaire, voir DI TRIA.

13 Voir not. EC, European Declaration on Digital Rights and Principles for the Digital Decade, para. 9 : « *Toute personne devrait être en mesure de bénéficier des avantages qu'offrent les systèmes algorithmiques et d'intelligence artificielle* […] *tout en étant protégée contre les risques et les atteintes à sa santé, à sa sécurité et à ses droits fondamentaux.* »

14 Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (Texte présentant de l'intérêt pour l'EEE), JO L 265 du 12.10.2022, p. 1-66.

15 Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (Texte présentant de l'intérêt pour l'EEE), JO L 277 du 27.10.2022, p. 1-102.

16 Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (Texte présentant de l'intérêt pour l'EEE), JO L 152 du 3.6.2022, p. 1-44.

17 Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (Législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM/2021/206 final.

18 Les données utilisées par les algorithmes pour l'entraînement et la décision peuvent être affectées par des biais et stéréotypes ce qui facilite les discriminations, voir EU FUNDAMENTAL RIGHTS AGENCY, Bias in Algorithms, p. 24. SUSSKIND, p. 257-258 (« *The real world contains patterns of injustice. These patterns are reflected in data. Algorithms reproduce and amplify them.* »).

19 Voir, EC, European Declaration on Digital Rights and Principles for the Digital Decade, para. 9 (c) : *« veiller à ce que les systèmes algorithmiques reposent sur des ensembles de données appropriés, afin d'éviter toute discrimination* […]. *»*.

20 RGPD, consid. 75. Même si le RGPD mentionne des risques de discrimination dans les considérants du règlement, son objectif premier n'est pas la protection contre les discriminations basées par exemple sur le sexe ou la religion, mais bien *« la protection des*

A. Interdépendance

Le fait que la doctrine a souvent combiné la protection des données et la non-discrimination afin d'illuminer la discrimination algorithmique témoigne de l'interdépendance et de la complémentarité de ces deux domaines juridiques pour adresser la problématique[21]. Ceci s'explique également par le fait qu'initialement dans la doctrine émergente, le seul outil adapté au monde numérique dans le droit européen était le RGPD. À la suite de l'adoption de la proposition du règlement *AI Act*, la doctrine s'est progressivement tournée vers d'autres (futurs) instruments.

B. La conflictualité entre protection des données et non-discrimination

La doctrine admet que le RGPD ne vise pas uniquement la protection des données, mais également d'autres droits, comme le droit à la non-discrimination[22]. Il n'en reste pas moins que les objectifs poursuivis par ces deux domaines juridiques peuvent entrer en conflit (conflictualité)[23]. Plus précisément, le RGPD crée une dichotomie entre les données relatives aux caractéristiques protégées qui peuvent être récoltées et celles qui ne le peuvent pas. Ces dernières comprennent les « catégories particulières de données à caractère personnel », notamment la race, la religion et l'orientation sexuelle, à l'exception des caractéristiques « sexe » ou « âge »[24]. Par conséquent, le principe d'interdiction ne permet pas de collecter des données relatives à des caractéristiques protégées par le droit de la non-discrimination (sauf sexe et âge), même dans l'objectif d'empêcher, de diminuer ou de détecter des discriminations. C'est une des raisons pour lesquelles le *AI Act* rappelle :

personnes physiques à l'égard du traitement des données à caractère personnel » (Art. 1 par. 1 RGPD) tout en protégeant les libertés et droits fondamentaux (Art. 1 par. 2 RGPD).

21 À titre d'exemple, voir HACKER, p. 55 ; KULLMANN, p. 61 ainsi que l'étude préparée pour le Conseil de l'Europe par BORGHESIUS, p. 36-46 (droit de la protection des données) et p. 32-36 (droit de la non-discrimination).

22 VAN BEKKUM/BORGESIUS, p. 5.

23 Voir aussi sur le manque de données qui peut mener à une discrimination algorithmique, WILLIAMS/BROOKS/SHMARGAD, p. 78-115.

24 Art. 9 par. 1 RGPD.

> « *Afin de protéger le droit d'autres personnes contre la discrimination qui pourrait résulter des biais dans les systèmes d'IA, les fournisseurs devraient être en mesure de traiter également des catégories spéciales de données à caractère personnel, pour des motifs d'intérêt public important au sens de l'article 9, paragraphe 2, point g), du règlement (UE) 2016/679 et de l'article 10, paragraphe 2, point g), du règlement (UE) 2018/1725, afin d'assurer la surveillance, la détection et la correction des biais liés aux systèmes d'IA à haut risque.* »[25].

Vu que la plupart des algorithmes et *business models* des entreprises nécessitent une large quantité de données (de qualité), cela peut créer un conflit entre les intérêts des personnes concernées et ceux des entreprises. La question se complique encore lorsque la protection des données, notamment à caractère personnel, impacte la lutte efficace contre la discrimination. Afin d'éviter ou diminuer le risque d'une discrimination, il peut en effet être nécessaire d'avoir connaissance du sexe ou de la religion, justement afin d'empêcher toute discrimination[26]. Ceci en raison de la corrélation effectuée par les algorithmes qui, même sans identification spécifique en tant qu'homme ou femme, trouvent des indices dans les données fournies et par conséquent peuvent mener à une discrimination.

Dans ce cas, l'obstacle que représente l'interdiction générale de collecter des données relatives à des caractéristiques protégées comme la race ou l'orientation sexuelle peut être levé, soit par une exception créée par la loi – ce qui est proposé dans le *AI Act*, soit par le consentement de l'individu concerné. Concernant le consentement, celui-ci est prévu par exemple dans le RGPD, à l'art. 9 par. 2 lit. a. S'il est donc en principe envisageable, il s'avère impossible et irréaliste dans les situations d'inégalité de pouvoir comme dans la relation employeur/employée. Même en dehors de ces cas, l'obtention du consentement libre et valable reste complexe et fait l'objet de nombreux débats en doctrine[27].

Outre l'*AI Act*, pour la Suisse les travaux du Conseil de l'Europe en matière de protection des données[28] et d'intelligence artificielle[29] sont très pertinents. Un rapport a été publié sur l'impact de l'IA sur l'égalité de genre et les risques de discriminations algorithmiques dans le cadre du développement d'un cadre législatif général relatif à l'IA à l'échelle du Conseil de l'Europe prévu pour

25 *AI Act*, consid. 44.
26 *AI Act*, consid. 44.
27 VAN BEKKUM/BORGESIUS, p. 6.
28 Voir not. CONSEIL DE L'EUROPE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, N° 108.
29 Voir CONSEIL DE L'EUROPE, Recommendation on the human rights impacts of algorithmic systems.

2023 et du cadre spécifique pour l'égalité de genre et non-discrimination prévu pour 2025[30].

C. Imitation

Les règles spécifiques, comme l'*AI Act* ou tout acte législatif suisse à venir, s'inspireront très certainement à plus ou moins grande échelle des règles européennes existantes, phénomène décrit comme le *Brussels Effect*[31]. Cela s'explique par la force d'attraction du marché intérieur, les soucis de compliance des entreprises ainsi que la rapidité d'adoption de ces règles en comparaison avec d'autres juridictions dans le monde[32]. Ainsi, les règles sur la régulation de l'IA s'inspirent largement du RGPD en prenant comme outil majeur les *algorithmic impact assessments*, connus du RGPD. En matière de protection de données, les observateurs ont fait état du fait que l'UE exerçait une influence afin que le contenu de la Convention 108+ du Conseil de l'Europe (CdE) soit aligné sur le RGPD. Un alignement semblable paraît possible concernant le AI Act et le projet législatif du CdE, qui impactera directement et indirectement la Suisse.

D. Complémentarité

Au niveau du droit européen, le RGPD reste un cadre juridique incontournable, à présent complété par le DSA, DMA et DGA en ce qui concerne la régulation des plateformes algorithmiques qui peuvent éventuellement mener à des discriminations. Dans un proche avenir, le *AI Act* s'ajoutera aux règles spécifiques et concrètes concernant quelques scénarios de discrimination algorithmique.

Nous avons analysé ci-dessus une série d'interdépendances et des opportunités pour une *imitation* des concepts du droit de la protection des données dans le droit de la non-discrimination, et évoqué quelques questions de conflictualité et complémentarité.

Ensuite, il incombe à l'individu de savoir s'il est soumis à une décision automatisée (si un algorithme est utilisé), car cette connaissance conditionne tout

30 CONSEIL DE L'EUROPE, Preliminary draft Council of Europe study on the impact of artificial intelligence, its potential for promoting equality, including gender equality, and the risks to non-discrimination, GEC(2022)9 CDADI(2022)21.

31 BRADFORD, The Future of the Brussels effect.

32 La ville de New York City a toutefois adopté une loi spécifique pour les systèmes de recrutement automatisés en 2021 qui est entrée en vigueur le 1er janvier 2023. Pour plus de détails, voir LÜTZ, Discrimination algorithmique.

autre droit ultérieur et c'est aussi ce qui mène au sujet de la transparence. Mis en place depuis quelques années, les dispositifs du droit de la protection des données peuvent servir de modèle, mais aussi être combinés afin de créer des synergies, par exemple dans le cas des analyses d'impact.

La présente section examinera le droit de savoir, car sans information il est impossible d'introduire une action en raison d'une possible discrimination.

III. Droit de savoir et transparence

Le droit de savoir et l'information qui en résulte sont des conditions préalables et essentielles pour permettre la transparence[33] et l'exercice effectif des droits fondamentaux[34]. En effet, sans cette connaissance, ni les victimes de discrimination ni les chercheurs ne sont en mesure de vérifier si les systèmes d'IA ne sont pas discriminatoires, une condition vitale de toute démocratie[35]. De plus, l'information concernant l'utilisation d'un algorithme et les éléments clés du fonctionnement constituent la base pour permettre une compréhension[36] et une explicabilité d'une décision algorithmique[37].

33 Voir Art. 13 *AI Act* sur la transparence et fourniture d'informations aux utilisateurs ainsi que EC, European Declaration on Digital Rights and Principles for the Digital Decade, par. 9 (b) : « *assurer un niveau de transparence adéquat quant à l'utilisation des algorithmes et de l'intelligence artificielle, et à faire en sorte que les citoyens soient formés à les utiliser et qu'ils soient informés lorsqu'ils interagissent avec ces technologies* » ; voir aussi CoE, Zero Draft Convention on AI, Art. 15 (*Principle of Transparency and Oversight*).

34 UNESCO, Guidelines for regulating digital platforms, par. 5 : « *Information empowers citizens to exercise their fundamental rights, supports gender equality, and allows for participation and trust in democratic governance and sustainable development, leaving no one behind.* ».

35 DJEFFAL, p. 255-284 ; BERSINI, p. 131.

36 En Italie, la *Corte di Cassazione* a récemment rendu un jugement dans le contexte du RGPD qui impose une connaissance des citoyens du fonctionnement des algorithmes, LA CORTE SUPREMA DI CASSAZIONE, Cassazione civile sez. I, 25/05/2021, (ud. 24/03/2021, dep. 25/05/2021), sentenza n. 14381, <https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/QUOTIDIANI_VERTICALI/Online/_Oggetti_Embedded/Documenti/2021/05/26/14381.pdf>.

37 Voir le projet de recherche suisse « *Nachvollziehbare Algorithmen* », qui utilise le terme « *Nachvollziehbarkeit* » plutôt que « *Erklärbarkeit* », qui est plus réaliste parce qu'il se focalise plutôt sur la traçabilité d'une décision au lieu d'une explication (souvent difficile), <https://ius.unibas.ch/de/e-piaf/nachvollziehbare-algorithmen/> ; BINDER *et. al.* ; THOUVENIN/BRAUN BINDER/LOHMANN ; THOUVENIN *et. al.*, Positionspapier : Ein Rechtsrahmen für KI.

Les recherches empiriques ont montré que les individus perçoivent différemment les décisions des algorithmes et des humains[38], d'où la nécessité et la valeur ajoutée d'accompagner le processus décisionnel par algorithme d'informations et d'explications.

Ces dernières années, de nombreuses méthodes ont été développées afin d'ouvrir la *black box* des algorithmes et d'essayer d'en expliquer le fonctionnement[39], au moins pour un public spécifique[40]. Néanmoins, la question clé reste de savoir à qui doivent profiter la transparence et la compréhension. Est-il suffisant que les experts en IA et les chercheurs comprennent le fonctionnement de l'IA en question, ou est-ce que l'utilisateur standard doit également pouvoir comprendre l'IA dans les grandes lignes ? Peut-être qu'il faudrait une sorte de *label* pour les consommateurs, qui réduit les explications techniques destinées aux experts à l'essentiel.

Des recommandations en la matière, comme celles du *European Law Institute* (ELI)[41] ou du récent rapport des Nations Unies[42], ont souligné l'importance de la transparence et de l'information et peuvent inspirer des solutions.

A. Connaître l'existence et le contenu d'une décision automatisée en matière d'IA

La première étape pour une administration ou une entreprise est de décider de l'utilisation d'un algorithme pour soutenir ou substituer un processus décisionnel. L'utilisation de l'IA doit alors être rendue publique ou communiquée aux personnes ou autorités concernées, d'une part afin qu'elles sachent quelles règles juridiques seront applicables et d'autre part afin de leur

38 Voir les recherches empiriques sur cette question, HERMSTRÜWER/LANGENBACH, Fair governance with humans and machines.

39 Les chercheurs académiques sont aussi importants que des organisations telles que *AlgorithmWatch* (<www.algorithmwatch.ch>), le *AI Now Institute* avec leurs rapports annuels (<https://ainowinstitute.org/our-work.html>), the *Ada Lovelace Institute* (<https://www.adalovelaceinstitute.org>), le *Weizenbaum Institute* (<https://www.weizenbaum-institut.de>) ou le *Alan Turing Institut*e (<https://www.turing.ac.uk>) qui contribuent massivement aux discours académiques et scientifiques ainsi qu'à la compréhension de l'IA.

40 Voir HACKER/PASSOTH, p. 343-373.

41 Voir ELI, Guiding Principles for Automated Decision-Making.

42 Voir UNITED NATIONS, A/77/196, Principles underpinning privacy and the protection of personal data, par. 45 (« *One of the principles relating to the processing of personal data is that controllers must process data* [...]. *In accordance with this principle, controllers must inform subjects of the processing conditions to which their personal information will be subject from the time of collection, so that subjects are in a position to exercise due control over the data.* »).

permettre de faire valoir leurs droits dans des cas de violations des droits individuels (protection des données et non-discrimination)[43].

Dans le contexte administratif, si les autorités publiques utilisent des algorithmes, le droit d'accès devrait inclure l'accès aux informations sur l'utilisation d'un algorithme ainsi que sur son fonctionnement, et ce afin de permettre un éventuel recours contre un acte administratif devant les tribunaux[44]. Dans le contexte civil, ceci impliquerait par exemple d'accéder aux éléments de preuves générés par l'algorithme qui sont nécessaires afin d'établir les éléments constitutifs d'une discrimination ou une discrimination *prima facie*.

B. Expliquer les décisions de l'IA

Dans la doctrine, plusieurs points de vue[45] ont été exposés concernant l'existence[46] ou non[47] d'un droit à l'explication dans le RGPD. Ceux-ci pourront servir d'exemple (à imiter ou à corriger) dans le contexte de la régulation des algorithmes afin d'éviter les discriminations.

Ce qui est important pour la présente discussion, c'est l'accès aux informations utiles et utilisables pour les humains[48]. Pour cela, il est impératif de connaître les grandes lignes du fonctionnement, le type d'algorithme, les données utilisées. Ces éléments pourraient être présentés de façon succincte par des *labels*, sans rentrer dans les détails.

43 Voir par exemple, CoE, Zero Draft Convention on AI, Art. 20 par. 2 : « *(..) any person has the right to know that one is interacting with an artificial intelligence system rather than with a human and, where appropriate, shall provide for the option of interacting with a human in addition to or instead of such system.* ».

44 Voir BVGer, C-5007/2019 du 1er juin 2022 qui traitait de la question de savoir si le droit d'accès incluait bien les algorithmes ; BVGer, B-626/2016, par. 7.2.1 (sur le droit d'accès et les algorithmes). Le droit général d'accès découle de l'art. 29 de la Constitution fédérale du 18 avril 1999 de la Confédération Suisse (RS 101) en combinaison avec les art. 61 par. 2 BBG, 26 VwVG (le principe) et 27 VwVG (les exceptions).

45 Begley/Schwedes/Frye/Feige ; Hacker/Krestel/Grundmann/Naumann ; Kaminski, The right to explanation, explained ; Malgieri/Comande ; Wachter/Mittledstadt/Floridi, p. 76-99.

46 Voir not. Kaminski, The right to explanation, explained, p. 209-217.

47 Contre l'existence d'un tel droit, Wachter/Mittledstadt/Floridi, p. 76-99.

48 Selbst/Powles, p. 48.

En Europe[49] et en Suisse[50], il y a plusieurs projets de recherche en cours essayant d'éclairer le sujet de la compréhension et de l'explicabilité des algorithmes. Afin de faciliter la transparence et l'explicabilité, une publication, notamment des tests, des analyses d'impact et des audits augmenterait probablement la confiance des citoyens dans les algorithmes[51].

C. Enregistrement du processus décisionnel automatisé

L'utilisation des algorithmes n'est pas seulement basée sur les données, elle produit également une large quantité de données. Afin d'atteindre plus de transparence et de permettre éventuellement d'expliquer le processus de prise de décision de l'algorithme, l'enregistrement du processus décisionnel s'impose pour créer des traces[52]. Ces traces peuvent être utilisées par des victimes potentielles, par exemple pour prouver une éventuelle discrimination dans le cadre d'une procédure de recrutement, et par les employeurs pour démontrer l'absence de discrimination. À ces fins, l'*AI Act* prévoit une documentation technique (art. 11) et un enregistrement des données qui doivent permettre de garantir

> « *un degré de traçabilité du fonctionnement du système d'IA tout au long de son cycle de vie qui soit adapté à la destination du système.* » (art. 12 par. 1 et 2)[53].

---

49 Voir pour un projet européen avec collaboration de *AlgorithmWatch CH*, qui a démarré en novembre 2022, FINDHR: an interdisciplinary project to prevent, detect, and mitigate discrimination in AI, <https://www.mpi-sp.org/43595/news_publication_18991677_transferred> ; un projet allemand de l'université de Hannovre "Bias and Discrimination in Algorithmic Decision-Making" explore la question *"How can we ensure that big data analysis and algorithm-based decision-making are unbiased and nondiscriminatory?"*, <https://www.bias-project.org>.

50 Voir notamment le projet "Nachvollziehbare Algorithmen: ein Rechtsrahmen für den Einsatz von Künstlicher Intelligenz", https://ius.unibas.ch/de/e-piaf/nachvollziehbare-algorithmen/ (consulté le 28 mars 2023).

51 SUSSKIND, p. 194 ; Voir COURT OF AUDITORS NL, Algorithm Audit, not. p. 38 sur les biais.

52 Voir pour une telle obligation du point de vue de la protection des données, MÉTILLE, Le traitement des données personnelles sous l'angle de la nLPD, p. 16 ; voir aussi COE, Zero Draft Convention on AI, Art. 19 lit. a. (« […] *the relevant usage of the system is recorded* […] »).

53 Ces obligations sont spécifiées par l'art. 18 *AI Act* concernant l'obligation d'établir une documentation technique et l'art. 20 *AI Act* sur les journaux générés automatiquement par les systèmes d'IA à haut risque. L'annexe IV de l'*AI Act* finalement prévoit des spécifications à respecter.

Cela n'aidera pas seulement dans de tels cas spécifiques, mais contribuera plus globalement à une plus grande transparence des algorithmes[54].

Afin de protéger les données des employés et d'éviter des discriminations, les encadrements juridiques issus du *algorithmic work management*[55] deviennent de plus en plus importants, non seulement pour permettre aux employeurs de procéder à des tests et vérifications du bon fonctionnement des algorithmes, mais aussi et surtout pour permettre un accès ultérieur aux données afin d'établir une éventuelle discrimination.

D. Rôle des chercheurs

En ce qui concerne la transparence et l'explicabilité des algorithmes, les chercheurs, notamment en sciences informatiques, en éthique et en sciences juridiques, ont le rôle de diriger vers les différentes méthodes d'analyse des décisions des algorithmes et d'attirer l'attention des juristes et des *policy makers* afin que celles-ci soient intégrées dans les lois.

Afin de garantir la transparence, le code des algorithmes pourrait être publié dans son intégralité ou en partie. Cette publication devrait idéalement se faire en ligne (si cela est possible au vu des droits de la propriété intellectuelle) ou du moins mise à disposition des chercheurs afin de tester, vérifier ainsi qu'améliorer le code en vue du respect des obligations légales[56].

Même si les développeurs des entreprises de l'IA sont dotés de compétences comparables, l'avantage du recours aux chercheurs (indépendants et sans financement ni conflit d'intérêt) par rapport aux entreprises utilisant des algorithmes et aux administrations se trouve notamment dans leur expertise indépendante afin d'identifier des problèmes et solutions pour des algorithmes spécifiques. Ceci peut aider à la fois les entreprises et les autorités publiques[57].

Finalement, la transparence et l'explicabilité offrent aux chercheurs la possibilité de détecter des discriminations qui restent souvent cachées en l'absence d'une analyse automatisée approfondie[58]. Les chercheurs jouent ainsi un rôle crucial afin de faire respecter l'art. 21 du *AI Act* et entamer des mesures correctives :

54 Voir en général BURRELL, p. 10.
55 ALOISI.
56 Voir par COE, Zero Draft Convention on AI, Art. 17.
57 Dans ce sens, la remarque des autorités néerlandaises, voir COLLEGE VOOR DE RECHTEN VAN DEN MENS, pt. 2.
58 HEINRICHS, not. p. 143 et 151.

> « *Les fournisseurs de systèmes d'IA à haut risque qui considèrent ou ont des raisons de considérer qu'un système d'IA à haut risque qu'ils ont mis sur le marché ou mis en service n'est pas conforme au présent règlement prennent immédiatement les mesures correctives nécessaires pour le mettre en conformité, le retirer ou le rappeler, selon le cas. Ils informent les distributeurs du système d'IA à haut risque en question et, le cas échéant, le mandataire et les importateurs en conséquence.* ».

Finalement, l'UNESCO, qui a publié des recommandations sur l'IA[59], plaide également pour un accès des chercheurs aux données afin de comprendre les enjeux, les risques et les opportunités des algorithmes[60]. Concrètement, la suggestion est :

> « *Digital platforms should provide access to non-personal data and anonymised data for vetted researchers that is necessary for them to undertake research on content to understand the impact of digital platforms. This data should be made available through automated means, such as application programming interfaces (APIs), or other open and accessible technical solutions allowing the analysis of said data.* »[61].

Cela peut inclure notamment d'impliquer la communauté de chercheurs :

> « *Develop and launch inclusive structured community feedback mechanisms to eliminate gender bias in generative AI and generative algorithms producing content that perpetuates or creates gendered disinformation or harmful or stereotypical content.* »[62].

In fine, il incombe aux développeurs d'algorithmes d'en faire davantage, notamment en permettant aux chercheurs de différentes disciplines d'accéder aux modèles et données des algorithmes afin d'assurer plus de transparence, de compréhension et d'acceptation[63].

59 Voir UNESCO, Recommendation on the Ethics of AI, not. par. 87-93.
60 UNESCO, Guidelines for regulating Digital Platforms, par. 72-74.
61 UNESCO, Guidelines for regulating Digital Platforms, par. 72.
62 UNESCO, Guidelines for regulating Digital Platforms, par. 98 (d).
63 JATON, p. 7.

IV. Confiance et droit au « *human-in-the-loop* »

L'utilisation des algorithmes pour remplacer ou compléter les décisions humaines, nécessite une acceptation sociétale et une confiance des citoyens[64] dans les systèmes algorithmiques[65]. Dans ce contexte, la doctrine et des projets législatifs parlent souvent de confiance dans l'IA ou d'IA digne de confiance[66] et prévoient l'implication d'un humain dans le processus décisionnel qui pourra influencer, mettre fin ou intervenir dans la prise de décision de l'algorithme. Il est clair que l'humain est toujours impliqué « dans » les algorithmes au sens de *human-in-the-loop*[67], car tous les algorithmes, du moins au début, sont pensés, créés et mis en place par des humains[68]. Inclure l'humain dans la surveillance de l'algorithme devient plus compliqué lorsqu'il s'agit d'algorithmes de type *machine learning*, *deep learning etc*.[69]. Dans ces cas, la question de la décision deviendra essentielle ; si c'est un humain qui décide (ou peut décider) ou si la machine prend les décisions toute seule. Inclure l'humain au cours du processus de décision des algorithmes constitue alors la garantie d'une transparence et confiance[70]. Inclure les humains dans le processus prévient aussi les risques d'*automation bias*[71]. Tel qu'il a été démontré dans la section *supra* II., la question est étroitement liée à la connaissance par l'individu du fait que la décision est prise par un algorithme et si possible de quelle manière exactement ou à quel pourcentage l'algorithme a été impliqué dans le processus décisionnel.

---

64 La confiance est utilisée telle que définie par le Larousse comme « *sentiment d'assurance* » ou « *sentiment de quelqu'un qui se fie entièrement à quelqu'un d'autre, à quelque chose* », <www.larousse.fr>.

65 Voir 2023. European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01., par. 9 (a) : « *promouvoir des systèmes d'intelligence artificielle axés sur l'humain, fiables et éthiques tout au long de leur mise au point, de leur déploiement et de leur utilisation, conformément aux valeurs de l'UE.* » et para. 9 (c) : « […] *permettre une surveillance humaine de tous les résultats qui affectent la sécurité et les droits fondamentaux des citoyens* ».

66 Voir par exemple le projet du *AI Act* qui utilise 41 fois le terme « *trust* » ou « *trustworthy* » et qui explique dans l'exposé des motifs : « *La présente proposition vise à mettre en œuvre le deuxième objectif, relatif à la mise en place d'un écosystème de confiance, en proposant un cadre juridique pour une IA digne de confiance* ».

67 Voir en général sur ce sujet et l'expertise humaine, PASQUALE ; CROOTOF/KAMINSKI/PRICE II, not. p. 45-49 (sur le rôle des humains qui consisterait surtout dans la correction des erreurs et des biais).

68 ENARSSON/ENQVIST/NAARTTIJÄRVI, p. 123-153.

69 Voir pour l'apprentissage des algorithmes, notamment LE CUN, not. p. 298-299.

70 Voir comme l'illustration l'art. 14 par. 1 *AI Act* sur le contrôle humain qui le suggère « *au moyen d'interfaces homme-machine appropriées, un contrôle effectif par des personnes physiques pendant la période d'utilisation du système d'IA* ». L'art. 14 par. 2 spécifie que « *Le contrôle humain vise à prévenir ou à réduire au minimum les risques pour* [...] *les droits fondamentaux* ».

71 Art. 14 par. 4, let. b *AI Act*.

Un droit de ne pas être soumis à un processus de décision automatisé pourrait aussi être envisagé[72], étroitement lié au droit à la supervision par un humain du processus de l'IA et à l'intervention d'un humain si besoin ou si souhaité par un individu qui exerce ce droit. À cet égard, l'IA pourrait modifier la façon dont les humains prennent des décisions et la façon dont les humains se perçoivent[73]. Les *Guiding Principles* 9 et 10 du ELI sont importants dans ce contexte[74], car ils prévoient une supervision humaine de l'IA qui devrait être raisonnable et proportionnelle, notamment au vu des coûts et des efforts engendrés pour les entreprises utilisant des systèmes d'IA.

Le jugement de la CJUE C-817/19 *Ligue des Droits Humains*[75], qui est à ce jour la seule décision de la CJEU traitant des questions d'algorithmes et de *machine learning,* éclaire l'utilisation d'algorithmes (notamment le *machine learning*) et les limites imposées par le droit européen, par exemple dans le cas d'une directive qui requiert des critères définis et préétablis :

> « *Cette exigence s'oppose à l'utilisation de technologies d'intelligence artificielle dans le cadre de systèmes d'autoapprentissage (machine learning), susceptibles de modifier, sans intervention et contrôle humains, le processus de l'évaluation et, en particulier, les critères d'évaluation sur lesquels se fonde le résultat de l'application de ce processus ainsi que la pondération de ces critères.* »[76].

A. Art. 22 RGPD

La littérature abondante est en constante évolution au vu des récentes propositions adoptées en matière d'IA, mais la majorité des auteurs souligne qu'il existe un droit de ne pas être soumis à une décision automatisée[77].

---

72 CABITZA *et. al*..

73 Voir pour cela l'ouvrage de NOWOTNY, not. p. 111-126.

74 ELI, Guiding Principles for Automated Decision-making in the EU, not. les principes 9, p. 22 et (Guiding Principle 9: Human oversight/action. The operator shall ensure reasonable and proportionate human oversight over the operation of ADM taking into consideration the risks involved and the rights and legitimate interests potentially affected by the decision.) et principe 10, p. 24 (Guiding Principle 10: Human review of significant decisions Human review of selected significant decisions on the grounds of the relevance of the legal effects, the irreversibility of their consequences, or the seriousness of the impact on rights and legitimate interests shall be made available by the operator.).

75 CJUE, arrêt C-817/19 du 21 juin 2022, *Ligue des Droits Humains*, par. 194.

76 CJUE, arrêt C-817/19 du 21 juin 2022, *Ligue des Droits Humains*, par. 194.

77 ROIG ; TOSONI, p. 145-162 ; DJEFFAL, p. 255-284.

On peut dire que dans le RGPD, l'UE a fait le choix conscient d'inclure l'humain dans le processus de décision automatisé, comme l'indique l'art. 22 par. 1 RGPD :

> « *La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.* »[78].

On pourra aussi parler d'un droit à s'opposer à l'IA dans des contextes de prise de décision spécifiques[79]. Ce droit/cette possibilité prévu(e) par le RGPD trouve toute sa signification dans le cadre des décisions automatisées ayant un potentiel de discrimination.

B. Art. 21 LPD

L'art. 21 LPD[80] intitulé « *Devoir d'informer en cas de décision individuelle automatisée* » précise à son paragraphe 1 que :

> « *Le responsable du traitement informe la personne concernée de toute décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour elle ou l'affecte de manière significative (décision individuelle automatisée).* »[81].

Le droit suisse prévoit donc un devoir d'informer le citoyen de l'utilisation exclusive d'un algorithme pour la prise de décision. Ce qui poserait par contre un problème en pratique, ce sont les scénarios dans lesquels les algorithmes contribuent à la prise de décision à une certaine hauteur (p. ex. 50 %, 75 %, 90 %) sans pour autant qu'une décision soit prise sans intervention humaine. Ici, le risque qu'un humain suive aveuglément la suggestion de l'IA pourrait être comparé à une situation ou la décision humaine est substituée à 100 % par un algorithme, ce qui semble être pris en compte par exemple dans la proposition du CdE[82].

78 Voir dans ce sens, HOOFNAGLE/VAN DER SLOOT/BORGESIUS, spécialement p. 68.
79 KAMINSKI/URBAN, p. 1957-2048.
80 Loi fédérale sur la protection des données (LPD) du 25 septembre 2020, RS 235.1.
81 Voir aussi MÉTILLE, p. 13.
82 CoE, Zero Draft Convention on AI, Art. 20 para. 1, qui parle de *substantially informs* : « […] *where an artificial intelligence system substantially informs or takes decision(s)* ».

C. Art. 14 *AI Act* et Art. 20 CdE *Zero Draft Convention on AI*

Les propositions de l'UE et du CdE sont pour l'instant les seules propositions législatives qui incluraient un tel droit au *human-in-the-loop* et qui concerneraient les scénarios ayant un impact pour le genre ou d'autres caractéristiques protégées dans le cadre d'une discrimination causée par un système de recrutement automatisé[83].

Le contrôle humain prévu par l'art. 14 du *AI Act* devrait être mis en place avant toute mise sur le marché et rendre possible aux personnes chargées d'effectuer le contrôle humain d'atteindre cinq objectifs : appréhender entièrement les capacités et les limites du système d'IA et surveiller son fonctionnement, afin de pouvoir détecter et traiter dès que possible les signes d'anomalies, de dysfonctionnements et de performances inattendues (a), avoir conscience d'une éventuelle tendance à se fier automatiquement ou excessivement aux résultats produits par un système d'IA à haut risque (« biais d'automatisation ») (b), être en mesure d'interpréter correctement les résultats du système d'IA à haut risque (c), être en mesure de décider, dans une situation particulière, de ne pas utiliser le système d'IA (d) et être capable d'intervenir sur le fonctionnement du système d'IA à haut risque ou d'interrompre ce fonctionnement au moyen d'un bouton d'arrêt ou d'une procédure similaire (e)[84].

Le projet législatif du CdE prévoit par exemple le droit à un examen humain (*human review*)[85].

Une question qui s'impose est de savoir si dans la collecte et l'utilisation des données une approche *discrimination awareness* est une possibilité[86]. Ceci dépendra largement de l'implication des chercheurs.

D. Rôle des chercheurs

Il est envisageable que les chercheurs fassent partie intégrante des commissions d'éthique, comités de surveillance ou de régulation établis à l'échelle européenne ou nationale. Toutefois, vu que les instances régulatrices traitent des questions d'algorithmes existants et prêts à être commercialisés ou

---

83 Pour l'UE, ceci en raison de la qualification des systèmes de recrutement comme IA à haut risque conformément à l'art. 6 conjointement avec l'Annexe 2. Pour le CdE, l'art. 12 CoE, Zero Draft Convention on AI prévoit l'application de principe d'égalité et de non-discrimination.

84 Art. 14 (4) a) - e).

85 CoE, Zero Draft Convention on AI, Art. 20 para. 1 : « […] *where an artificial intelligence system substantially informs or takes decision(s) affecting human rights and fundamental freedoms there is a right to human review of the decisions.* ».

86 Berendt/Preibusch, p. 135-152.

qui sont déjà sur le marché, il est également important d'intégrer les questions éthiques et juridiques dès la conception des algorithmes[87]. Au plus les risques de discrimination sont connus dès la phase de conception des algorithmes, au plus les chances de réduire les biais et possibles discriminations sont élevées. Le rôle des chercheurs est d'abord pédagogique[88], afin de traduire en pratique la transparence tel que définie dans les propositions législatives. Ils pourront également alerter les citoyens, les entreprises utilisant l'IA et les administrations qui supervisent l'utilisation dans les cas où la substitution ou l'assistance de décisions humaines par l'IA pourrait porter atteinte aux principes de non-discrimination et donc recommander ou dissuader l'utilisation de l'IA compte tenu des risques. En ce qui concerne le droit d'information, le rôle des chercheurs est notamment d'expliquer le fonctionnement de l'IA dans des termes compréhensibles et de contribuer à la communication des informations essentielles aux utilisateurs finaux. Finalement, concernant la mise en place du *human-in-the-loop*, il est clair que la présence et/ou la disponibilité des chercheurs pour mettre en œuvre de tels droits sont importantes.

V. Sphère privée et non-discrimination dès la conception et par défaut

En ce qui concerne la discrimination algorithmique, le droit de la non-discrimination peut s'inspirer du droit de la protection des données en utilisant les concepts de vie privée dès la conception et par défaut (A.) et pour établir des concepts similaires de non-discrimination par conception et par défaut (B.). Comme déjà plus ou moins accepté pour la protection des données, le principe de non-discrimination de tout système algorithmique devrait être non seulement intégré dès la conception[89], mais également internalisé par défaut par toute entreprise créant ou utilisant des algorithmes.

A. Sphère privée dès la conception et par défaut

Peter SCHAAR, ancien préposé fédéral à la protection des données (*Bundesdatenschutzbeauftragter)* en Allemagne qui a largement contribué à renforcer la protection des données au niveau national et européen avait déjà

87 BAUMER, p. 2.

88 BERSINI, p. 84 qui suggère l'implication des informaticiens et des citoyens pour contrer l'analphabétisme informatique et faciliter une meilleure compréhension des algorithmes.

89 Pour quelques réflexions sommaires concernant le concept de *non-discrimination dès la conception* sans pour autant traiter les règles juridiques de la protection des données, voir LÜTZ, Discrimination by correlation, not. p. 278-279.

souligné l'importance de la sphère privée dès la conception en 2010[90]. Dix ans plus tard en 2020, il a réitéré la nécessité d'utiliser des solutions techniques afin d'assurer la protection des données[91]. Dans le droit de l'UE, on retrouve le modèle d'une régulation dès la conception notamment dans le droit de la protection des données, avec le concept de la sphère privée dès la conception et surtout à l'art. 25 RGPD[92]. Le but de ce concept est d'intégrer dans la conception de tout mécanisme qui utilise des données dans le sens du RGPD des mesures qui protègent les données et protègent la sphère privée des utilisateurs[93].

B. Non-discrimination dès la conception and par défaut

On pourra s'inspirer des méthodes et du cadre législatif instaurés par le RGPD afin d'élaborer un processus similaire pour le droit de la non-discrimination. Même si plusieurs problèmes persistent concernant cette approche en *privacy law*[94] et si certains outils du RGPD ne sont pas encore mis en place comme prévu, ce modèle semble la bonne voie à suivre.

D'abord, les chercheurs étaient largement impliqués lors du développement du concept de non-discrimination dès la conception[95]. La non-discrimination par défaut signifie que les principes juridiques de non-discrimination sont intégrés ou pris en compte le mieux possible lors de la conception des algorithmes[96]. Cela pourrait contribuer à éliminer des biais ou des discriminations dès la conception des algorithmes.

Ensuite, l'approche non-discrimination par défaut, requiert non seulement l'intégration technique dans le code des algorithmes, mais également et avant tout une connaissance, ouverture et compréhension des concepts juridiques de non-discrimination. Sans cela, il est difficilement envisageable que les concepteurs des algorithmes puissent intégrer de manière cohérente des spécifications et paramètres dans le modèle et le code des algorithmes qui soutiennent l'objectif

90 SCHAAR, Privacy by design, p. 267-274.
91 SCHAAR, Datenschutz, p. 179-185.
92 RUBINSTEIN/GOOD, p. 37-56 ; LAGIOIA/SARTOR, p. 75.
93 Voir CAVOUKIAN/DIXON ; SHEN/PERASON. Voir not. Comité européen de la protection des données, Lignes directrices 4/2019 relatives à l'article 25, Protection des données dès la conception et protection des données par défaut, Version 2.0 Adoptées le 20 octobre 2020, <https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fr.pdf>.
94 GÜRSES/TRONCOSO/DIAZ, p. 25.
95 Voir TILBURG UNIVERSITY, Report Non-discrimination by design.
96 Pour une explication pratique sur comment les principes de non-discrimination devraient être intégrés lors de la conception des systèmes d'IA, voir REBSTADT *et al*., p. 495-511.

de non-discrimination[97]. Il est donc nécessaire de former les ingénieurs et développeurs en leur fournissant quelques bases en droit de la non-discrimination, ou au moins d'intégrer dans les toolkits ou les logiciels préfabriques et les bases de données qui servent comme exemple pour les développeurs des paramètres et spécifications qui permettent d'utiliser des blocs contenant déjà ces paramètres qui essaient de mettre en œuvre ce principe de non-discrimination.

C. Quel modèle à suivre pour la discrimination algorithmique ?

> « *The mechanics of modern algorithms offered promises of transparency and of equal, dispassionate treatment – behind the veil of ignorance – without making distinctions based on prohibited demographic characteristics such as race or gender.* »[98].

La réalité est toutefois très différente, comme cela a été montré dans la présente contribution, qui a développé la nécessité de transparence des algorithmes qui sont loin d'être neutres et qui requièrent une supervision afin d'empêcher des biais et discriminations. Détailler le modèle de régulation idéal pour contrer la discrimination algorithmique dépasserait largement l'espace et le but de la présente contribution[99]. Néanmoins, il est évident que les outils et les droits et éléments clés qui sont présentés ici devront faire partie intégrante de toute régulation. Idéalement, des outils comme l'analyse d'impact ou les audits devraient être intégrés dans un cadre juridique contraignant afin de pouvoir assurer efficacement la protection des droits humains.

D. Le rôle des chercheurs

Les chercheurs sont impliqués dès la conception des algorithmes, notamment en se basant sur la recherche effectuée par le monde académique[100], mais aussi par les chercheurs associés aux grandes entreprises technologiques[101].

97 THOMPSON, not. p. 1-3.

98 BURREL/FOURCADE, p. 222.

99 Pour des pistes de solution en Europe, voir LÜTZ, Gender Equality and AI in Europe. Pour l'exemple de la discrimination algorithmique dans le recrutement automatisé, voir LÜTZ, Discrimination algorithmique.

100 Il faut néanmoins garder en tête qu'une récente étude a déterminé que plus que la moitié des chercheurs a reçu un financement des grandes entreprises technologiques, voir GOFMAN/JIN ; voir aussi UNESCO/MILA, Missing Links in AI Governance, p. 35 ss (concernant l'industrie IA, l'éthique et l'équité).

101 Les chercheurs employés par ces entreprises ont publié des milliers des articles scientifiques sur l'IA : *Alphabet* (9000), *Microsoft* (8000) et *Meta* (4000) selon Big tech and

Ces recherches peuvent ensuite être utilisés dans les tests des systèmes d'IA à l'interne ou l'externe (p. ex. à travers des *hackathons*), et servir de base pour des conseils aux entreprises et pouvoirs publics. Finalement, la présence dans des structures publiques de surveillance peut contraindre une utilisation éthique et conforme aux règles juridiques en vigueur. Durant toute leur implication, il est essentiel que les chercheurs intègrent et respectent la conception et les valeurs des droits fondamentaux et le principe de la non-discrimination[102].

VI. Analyse d'impact pour les données et les algorithmes

Le RGPD prévoit à l'art. 35 par. 1 l'analyse d'impact pour la protection des données :

> « *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.* ».

Ces outils d'analyse d'impact sont incorporés dans le droit et envisagés dans les cadres juridiques et politiques proposés[103] ainsi que vivement discutés dans la doctrine[104].

Le rôle des chercheurs consiste notamment en la conception des outils permettant de détecter des biais et des discriminations[105] et à consulter les entreprises

artificial intelligence, Mastering the machine, *The Economist*, 1er Avril 2023, p. 54-55. Les centres de recherche en IA de grandes entreprises technologiques comme *Microsoft Research* emploient environ 8000 chercheurs en IA et sont donc souvent plus larges que les départements des grandes universités du monde, voir JUROWETZKI/HAIN/MATEOS-GARCIA/STATHOUPOULOS ; BISHOP, Microsoft AI Research.

102 EC, European Declaration on Digital Rights and Principles for the Digital Decade, par. 9 (f) : « *prendre des mesures pour faire en sorte que la recherche en matière d'intelligence artificielle respecte les normes éthiques les plus élevées et la législation pertinente de l'UE* ».

103 *AI Act* (art. 29 par. 6 qui réfère aux obligations découlant du RGPD) ; OECD, Recommendation on AI, not. V.) 2.3(b) (« *assessment mechanisms* ») ; CONSEIL DE L'EUROPE, Recommendation on the human rights impacts of algorithmic systems (qui fait référence aux *Human Rights Impact Assessment* 15 fois dans différents contextes).

104 MOSS/WATKINS/METCALF/ELISH.

105 Voir par exemple *Aequitas Bias & Fairness Audit* et leur *Bias and Fairness Audit Toolkit*, <http://aequitas.dssg.io> dont le code est disponible sur *GitHub.com* en open access: <https://github.com/dssg/aequitas> et où les entreprises peuvent auditer leurs propres données à travers leur site web.

et les administrations pour la mise en œuvre des outils. Au niveau européen, par exemple, le *European Centre for Algorithmic Transparency* a été créé auprès du *Joint Research Centre* (JRC) de la Commission européenne pour le suivi des questions de transparence algorithmique en lien avec le DSA :

> « *In addition to the Commission's supervisory role, such risk assessments and any accompanying mitigation measures will be subject to an external independent audit and oversight by researchers and civil society.* »[106].

Pour le droit de la non-discrimination, pour l'instant, sur la base du *AI Act*, seuls les systèmes d'IA à haut risque seront soumis à conditions. Cela concerne par exemple les systèmes de recrutement automatiques, mais pas d'autres applications, ce qui laisse un large vide par rapport au champ d'application classique du droit de la non-discrimination. Ce vide devra être comblé par d'autres outils législatifs, par exemple le projet du Conseil de l'Europe ou le droit national.

A. Analyse d'impact dans la protection des données

L'analyse d'impact est prévue dans le RGPD à l'art. 22 par. 3 qui spécifie que :

> « *le responsable du traitement met en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision*. ».

L'intervention humaine est donc en théorie une possibilité qui pourrait être requise par l'individu afin de faire valoir son droit à la non-discrimination par exemple. Pour cela, l'individu doit être informé du fait qu'une décision est automatisée (de par l'utilisation d'un algorithme), par exemple aux fins du traitement de sa demande de crédit ou de sa candidature à une offre d'emploi.

De plus, en vertu de l'art. 22 par. 1,

> « *la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire*. ».

[106] <https://algorithmic-transparency.ec.europa.eu/about_en>.

Donc, au-delà de demander l'intervention humaine dans le processus algorithmique, un individu peut demander à ne pas faire l'objet d'une décision automatisée, requérant en quelque sorte une intervention plus forte en comparaison avec le scénario d'acceptation d'une décision d'un algorithme sous une surveillance humaine accrue.

En principe, les exceptions prévues notamment à l'art. 22 par. 2 – nécessité à la conclusion ou exécution d'un contrat, autorisation par le droit national ou européen et le consentement – pourraient s'appliquer. Il n'est néanmoins pas très clair dans quel contexte par exemple un algorithme pourrait être requis à la conclusion d'un contrat de travail lors d'une procédure de recrutement (l'alternative étant de ne pas utiliser un algorithme), car le simple fait de dire qu'on utilise un algorithme pour le recrutement suffira à faire jouer l'exception établie par l'art. 22 RGPD. Le consentement, bien connu et débattu dans le cadre du droit de la protection des données, s'avère délicat s'il s'agit par exemple d'une procédure de recrutement, car refuser le consentement résulterait probablement dans l'impossibilité de postuler pour l'offre d'emploi. Dans ce cas spécifique, on pourrait parler d'un consentement qui n'est pas libre.

Avant la mise sur le marché, les analyses d'impact peuvent détecter les biais[107] ou stéréotypes, par exemple concernant le genre[108] ainsi que de possibles discriminations. Une telle vérification peut être mise en place soit par les entreprises elles-mêmes, soit par le pouvoir public, soit par des entreprises tierces ou chercheurs indépendants.

B. Analyse d'impact afin d'éviter les discriminations algorithmiques

Se distinguant de l'analyse d'impact dans le domaine de la protection des données, l'analyse d'impact algorithmique ou l'analyse des biais d'audit a pour but d'identifier des biais, des stéréotypes ou des risques de discriminations[109]. Il s'agit d'une certaine manière de tester les algorithmes avant leur

107 Voir ZERILLI, p. 43-45.

108 WAJCMAN/YOUNG/FITZMAURICE, not. p. 15 (concernant les biais et les *feedback loops*).

109 Voir pour des efforts d'opérationnaliser le concept de biais, JATON, p. 2-3 ; pour des propositions de régulation au niveau globale UNITED NATIONS, Commission on the Status of Women (CSW), 67th Conference, March 2023, E/CN.6/2023/3 – draft agreed conclusions (zero draft), para. 45 (u) « *Adopt regulations mandating evaluation and audit requirements for the development and use of artificial intelligence to provide a secure and high-quality data infrastructure and systems that are either continually improved or terminated if human rights violation or gendered bias are identified* », disponible : <https://www.unwomen.org/sites/default/files/2023-02/CSW67%20Agreed%20Conclusions_zero%20draft_1%20February%202023.pdf>.

mise sur le marché au moyen de *datasets* différents permettant de tester et vérifier si un algorithme montre des tendances biaisées ou produit des discriminations visibles. Tel qu'est le cas dans le monde non-algorithmique, l'exclusion *ex ante* de toute discrimination ou tout biais est illusoire, mais l'analyse d'impact permettra d'exclure *ex ante* certains dysfonctionnements graves pouvant causer des discriminations. La standardisation d'une telle procédure sur la base d'un standard technique ou une législation peut donc contribuer à réduire les effets néfastes des algorithmes. S'il est bien entendu toujours possible d'avoir recours à l'arsenal juridique du droit de la non-discrimination afin de faire valoir ses droits, au vu de l'opacité des algorithmes décrite dans la section *supra* II.), et afin de garantir un terrain de jeu plus au moins équivalent au monde d'avant les algorithmes, cette approche semble pouvoir porter ses fruits.

L'art. 29 par. 6 de l'*AI Act* fait référence à l'art. 35 RGPD pour les utilisateurs des systèmes d'IA à haut risque qui peuvent avoir recours aux données fournies sur la base de l'art. 13 *AI Act* afin de se conformer aux RGPD. Bien que préconisés par la majorité des chercheurs et faisant partie des outils préférés des législateurs afin d'adresser le problème de la discrimination algorithmique, les AIAs sont confrontés à un problème. En effet, leur efficacité est conditionnée à la coopération des opérateurs privés, car ce sont ces derniers qui ont accès aux informations, aux données ainsi qu'à l'expertise permettant d'analyser les algorithmes. Même en cas de cadre législatif contraignant, le résultat sera donc fort dépendant de la volonté des développeurs et des utilisateurs des algorithmes, ce qui peut menacer le bon fonctionnement de la régulation[110].

C. *Monitoring*

Après l'analyse d'impact en principe effectuée avant la mise sur le marché du produit IA, le monitoring est généralement mis en place une fois que l'algorithme est disponible pour le grand public. Le *monitoring* vise alors à identifier d'éventuels problèmes sur la base d'une collecte des données relatives à l'utilisation du système d'IA sur le marché. C'est notamment au cours de cette phase que les biais et les discriminations pourront remonter à la surface, les données utilisées par les individus étant forcément différentes de celles utilisées pour l'entraînement de l'algorithme. Il s'agit donc d'observer constamment le bon fonctionnement des algorithmes afin de documenter et de corriger d'éventuels impacts négatifs en matière de non-discrimination. Ceci nécessite une *data governance* bien établie comme requise par l'art. 10 par. 2 *AI Act* :

110 Voir SELBST, p. 117-118 et p. 152-153.

« *Les jeux de données d'entraînement, de validation et de test sont assujettis à des pratiques appropriées en matière de gouvernance et de gestion des données* », notamment en vue d'« *un examen permettant de repérer d'éventuels biais* ».

Dans le *AI Act*, cette étape est désignée comme le « *post-market monitoring* », tandis que le *US Accountability Act* parle de « *augmented decision-making proccesses* »[111].

Au vu de la récente popularité des applications d'IA se basant sur des *Large Language Models* (LLMs), comme *ChatGPT*, *Bard*, *Claude*, *etc*., le monitoring devient de plus en plus important[112].

D. Rôle des chercheurs

Si en principe les développeurs des entreprises et les chercheurs indépendants effectuent des recherches pouvant mener à des produits d'IA qui seront ensuite mise en production, ils poursuivent des objectifs différents. En effet, les développeurs employés par une entreprise ont pour but de développer des produits spécifiques pour le compte de l'entreprise. Par contre, le but poursuivi par les chercheurs n'est pas principalement de développer une application spécifique pour une entreprise, mais de s'engager dans la recherche fondamentale. Le rôle des chercheurs pour l'avancement des technologies et pour empêcher des effets négatifs[113] sur les droits fondamentaux n'est de ce fait pas seulement essentiel, mais ancré dans les droits humains[114]. Quant aux juristes, un de leurs rôles serait sûrement d'informer quelles sont les lois applicables qui doivent être respectées et par conséquent intégrées dans les algorithmes, mais aussi prises en compte lors des analyses d'impact.

---

111 Voir pour une comparaison des approches EU et US, MÖKANDER/JUNEJA/WATSON/FLORIDI, not. p. 752.

112 MÖKANDER *et al*., Auditing LLMs.

113 Voir par exemple l'avertissement des chercheurs en IA sur le développement des LLMs qui sont plus performants que *GPT-4*, "Pause Giant AI Experiments: An Open Letter" of March 22, 2023: "We call on all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4.", <https://futureoflife.org/open-letter/pause-giant-ai-experiments/> ; voir aussi CoE, Zero Draft Convention on AI, l'art. 24 par. 3 CoE qui prévoit un moratoire ou une interdiction sur certaines applications d'IA.

114 Voir l'art. 27 de la Déclaration universelle des droits de l'homme et l'art. 15 du International Covenant on Economic, Social and Cultural Rights (ICESCR) qui stipule une sorte de droit aux sciences, ce qui implique naturellement un rôle primordial des scientifiques d'éclairer le public par exemple sur les effets des algorithmes et peut être même un devoir d'anticiper les conséquences (négatives) des algorithmes sur les droits fondamentaux, voir DONDERS/PLOZZA.

Les chercheurs en sciences informatiques et les développeurs, sachant que les techniques informatiques sont en constante évolution, sont notamment chargés d'informer et d'éclairer sur les dernières techniques pouvant être utilisées par exemple afin d'éviter ou de détecter des biais ou des discriminations[115].

Il s'impose d'impliquer les chercheurs en droit et en sciences informatiques qui n'ont aucun lien contractuel avec l'entreprise en cause et qui seront donc considérés comme personnes tierces dans tout le processus d'analyse d'impact et des audits. Les audits pourront être demandés aux entreprises et administrations avant ou après de la mise sur le marché[116]. La preuve de l'implication d'un certain nombre de chercheurs experts dans le domaine pourrait être requise. Les autorités européennes ou nationales devraient pouvoir se reposer sur des informaticiens et des juristes spécialisés dans la discrimination. Afin de pouvoir contrôler et vérifier la mise en place des différentes mesures, il faut garder à l'esprit que l'instrument phare proposé par de multiples chercheurs et repris dans des propositions législatives diverses représente aussi des risques, notamment au vu de la dépendance de l'expertise du secteur privé qui détient le savoir-faire permettant de procéder aux *bias* audits. Afin d'exercer le contrôle par *AI Act* et le monitoring *ex-post*, ceux-ci doivent dès lors être encadrés par des règles juridiques strictes[117], comme c'est le cas par exemple dans le secteur pharmaceutique, où les entreprises mènent les études cliniques elles-mêmes et l'administration procède à des vérifications. De manière similaire, il est envisageable que les employés de l'entreprise elle-même procèdent à la vérification des impacts de l'IA en interne, à condition d'ensuite être soumis au contrôle d'une autorité de surveillance. Afin de garantir plus d'impartialité, une entreprise tierce pourrait également procéder à une telle analyse des impacts, également sous le contrôle (plus sommaire) de l'autorité responsable. Finalement, impliquer les chercheurs académiques comporte l'avantage de l'impartialité et de la transparence, car leur travail est souvent inspiré par l'*open access* en comparaison avec ceux travaillant pour les entreprises privées[118].

115 Voir p. ex. MÖKANDER *et al*., Auditing LLMs, p. 1 qui alertent au fait que les mesures d'*audit* utilisées à présent et prévues dans les propositions législatives peuvent potentiellement encourir des risques pour les LLMs qui sont des systèmes en constante évolution.

116 Voir l'exemple des Pays-bas qui procédent à de telles audits pour le secteur public, COURT OF AUDITORS NL, Algorithm Audit ; RAJI/CONSTANZA-CHOCK/BUOLAMWINI, p. 5-26.

117 Dans ce sens aussi SUSSKIND, p. 194 qui est en faveur des règles contraignantes favorisant l'approche par la loi plutôt que le libre choix des entreprises.

118 BERSINI, p. 147.

VII. Conclusion

L'implication des chercheurs dans les débats avant l'adoption des actes juridiques, en ce compris les groupes de travail[119], les comités élaborant les standards[120], la doctrine et les conférences en général, est évidente. Leurs rôles définis dans les propositions législatives, demeurent cependant moins clair.

En raison de l'importance des données et de l'objectif commun de protéger des droits fondamentaux, l'article a d'abord constaté l'interdépendance, la conflictualité, la complémentarité ainsi que le potentiel d'imitation du droit de la protection des données et du droit de la non-discrimination. Le droit de la protection des données ayant une demi-décennie d'avance en matière de décision automatisée et d'algorithmes, le droit de la non-discrimination peut s'inspirer de ses cadres juridiques, de sa pratique et de ses institutions.

Concrètement, la présente contribution a exposé que le droit de connaitre l'implication d'un algorithme dans la prise de décision est essentiel et constitue souvent la base de toute action juridique ultérieure. Le droit de savoir si et comment un algorithme prend ou contribue à une décision fait partie de ce qui est souvent appelé la transparence. Celle-ci est souvent qualifiée de véhicule (« *tool* »), mais elle constitue en réalité plutôt l'objectif à atteindre.

Ensuite, le droit à l'intervention humaine dans tout processus algorithmique, qui était déjà présent dans le RGPD, est envisagé pour les projets de régulation de l'IA à l'échelle européenne.

En ce qui concerne le concept de non-discrimination dès la conception et par défaut qui découle du *privacy law*, il est clair qu'il devrait constituer un principe de guidage pour la conception des algorithmes, idéalement ancré dans une règle juridique.

Les analyses d'impact nécessaires afin d'éviter les biais et discriminations algorithmiques sont également prescrites par le RGPD. Par conséquent, il convient de créer des synergies entre le RGPD et le futur *AI Act* en la matière. Il en est de même pour le *monitoring* et les analyses *ex-post* tant pour la législation que pour le fonctionnement des algorithmes, qui devraient être surveillés constamment afin de signaler des dysfonctionnements ou des risques pour les droits fondamentaux.

Dans tous les domaines discutés, le rôle des chercheurs est crucial, non seulement avant la mise en place d'un cadre législatif, mais surtout au cours du fonctionnement des algorithmes et la mise en œuvre des lois ainsi que pour le

119 Des groupes d'experts sur l'IA, comme p. ex la *High level expert group on Artificial Intelligence*, <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai>.

120 CEN-CENELEC ou ISO p. ex. dont la Suisse est membre.

futur développement et d'éventuelles révisions de celles-ci. Les chercheurs ne sont pas seulement (plus) indépendants que le pouvoir public et les entreprises, il est également dans l'intérêt commun et public de tester et aviser des risques concernant le fonctionnement des algorithmes et de l'application des règles. Afin de permettre aux chercheurs d'effectuer ce travail, il est important d'ancrer leurs rôles dans les textes législatifs ainsi que d'établir les mécanismes pertinents permettant leur participation[121]. Cela implique aussi de donner accès dans un cadre spécial aux données et aux modèles des algorithmes, sans mettre en danger les intérêts des entreprises protégés notamment par la propriété intellectuelle ou des secrets d'affaires.

VIII. Bibliographie

A. Littérature

Serge Abiteboul/Gilles Dowek, Le temps des algorithmes, Paris 2017 ; **Antonio Aloisi**, Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights, International Journal of Comparative Labour Law and Industrial Relations, 2022 (*à paraître*) ; **Solon Barocas/Moritz Hardt/Arvind Narayanan**, Fairness in machine learning, 2022 ; **Eric Baumer**, Toward human-centered algorithm design, Big Data & Society 2017, Nº 4 ; **Tom Begley/Tobias Schwedes/Christopher Frye/Ilya Feige**, Explainability for fair machine learning, 2020 ; **Bilel Benbouzid/Yannick Meneceur/Nathalie Alisa Smuha**, Quatre nuances de régulation de l'intelligence artificielle : Une cartographie des conflits de définition, Réseaux (Centre national d'études des télécommunications (France)) 2022, Nº 232-233, p. 29-64 ; **Bettina Berendt/Sören Preibusch**, Toward accountable discrimination-aware data mining: the Importance of keeping the human in the loop – and under the looking glass. Big data 2017, Nº 5, p. 35-152 ; **Hugues Bersini**, Algocratie : Allons-nous donner le pouvoir aux algorithmes ?, Louvain-La-Neuve 2023 ; **Nadja Braun Binder/Thomas Burri/Melinda Florina Lohmann/Monika Simmler/Florent Thouvenin/Kerstin Noëlle Vokinger**, Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht, Jusletter du 28 juin 2021 ; **Todd Bishop**, One year later, Microsoft AI and Research grows to 8k people in massive bet on artificial intelligence, GeekWire 22 septembre 2017, <https://www.geekwire.com/2017/one-year-later-microsoft-ai-research-grows-8k-people-massive-bet-artificial-intelligence/ (consulté le 5 mars 2023>) (cité : Bishop, Microsoft AI Research) ; **Frederik Borgesius**, Discrimination, artificial intelligence, and algorithmic decision-making, 2018, Study for the Council of Europe ; **Anu Bradford**, The brussels effect, Northwestern University Law Review 2012, 107, p. 1 ss (cité : Bradford, Brussels Effect) ; **Anu Bradford**, The Future of the Brussels Effect, The Brussels Effect, Oxford 2020 (cité : Bradford, The Future of the Brussels Effect) ; **Jenna Burrell**, How the

[121] Voir EC, European Declaration on Digital Rights and Principles for the Digital Decade, par. 9 (e) : « *prévoir des garanties et prendre des mesures appropriées, y compris en promouvant des normes fiables, pour que l'intelligence artificielle et les systèmes numériques soient, en permanence, sûrs et utilisés dans le plein respect des droits fondamentaux*. ».

machine 'thinks': Understanding opacity in machine learning algorithms, Big data & society 2016, N° 3 ; **Jenna Burrell/Marion Fourcade**, The Society of Algorithms. Annual Review of Sociology 2020, p. 47 ss ; **Federico Cabitza/Andrea Campagner/Gianclaudio Malgieri/Chiara Natali/David Schneeberger/Karl Stoeger/Andreas Holzinger**, Quod erat demonstrandum?-towards a typology of the concept of explanation for the design of explainable AI, Expert Systems with Applications 2023, Vol. 213, p. 118888 (cité : Cabitza *et al*.) ; **Ann Cavoukian/Mark Dixon**, Privacy and security by design: An enterprise architecture approach, Information and Privacy Commissioner, Ontario 2013 ; **Kathleen Creel/Deborah Hellman**, The Algorithmic Leviathan: Arbitrariness, Fairness, and Opportunity in Algorithmic Decision-Making Systems, Canadian Journal of Philosophy 2022, p. 1-18 ; **Rebecca Crootof/Margot Kaminski/William Nicolson Price II**, Humans in the Loop, Vanderbilt Law Review, Forthcoming, 2023 ; **Livio Di Tria**, Comparaison entre la nLPD et le RGPD, 12 février 2021, <www.swissprivacy.law/55> ; **Yvonne Donders/Monika Plozza**, Look before you Leap: Anticipation Duties and Responsibilities under the Right to Science, in: International Journal of Human Rights (forthcoming) 2023 ; **Christian Djeffal**, AI, Democracy and the Law, *in* Andreas Sendmann (ed.), The Democratization of Artificial Intelligence, p. 255284, Bielefeld 2020 ; **Therese Enarsson/Lena Enqvist/Markus Naarttijärvi**, Approaching the human in the loop – legal perspectives on hybrid human/algorithmic decision-making in three contexts, Information & Communications Technology Law 2022, N° 31, p. 123-153 ; **Florian Jaton**, Assessing biases, relaxing moralism: On ground-truthing practices in machine learning design and application, Big Data & Society 2021, Vol. 8., Nr. 1 ; **Raquel Esther Jorge Ricart/Fiametti Rossetti/Luca Tangi/Vincent Van Roy**, AI watch, national strategies on artificial intelligence: a European perspective, 2022, Publications Office of the European Union (cité : Jorge Ricart et. al., AI watch, national strategies on AI) ; **Francesca Lagioia/Giovanni Sartor**, The impact of the general data protection regulation on artificial intelligence, European Parliament 2021, Publications Office ; **Michael Gofman/Zhao Jin**, Artificial Intelligence, Education, and Entrepreneurship, Journal of Finance 2022, Forthcoming ; **Seda Gürses/Carmela Troncoso/Claudia Diaz**, Engineering privacy by design, Computers, Privacy & Data Protection 2011, 14, p. 25 ; **Philip Hacker**, Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law, Common Market Law Review 2018, p. 55 (cité : Hacker, Teaching fairness to AI) ; **Philip Hacker/Ralf Krestel/Stefan Grundmann/Felix Naumann**, Explainable AI under contract and tort law: legal incentives and technical challenges, Artificial Intelligence and Law 2020, 28, p. 415-439 ; **Philip Hacker/Jan-Hendrik Passoth**, Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond. xxAI-Beyond Explainable AI: International Workshop, Held in Conjunction with ICML 2020, July 18, 2020, Vienna, Revised and Extended Papers 2022, p. 343-373 ; **Ronan Hamon/Hendrik Junklewitz/Ignacio Sanchez/Gianclaudio Malgieri/Paul de Hert**, Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making, IEEE Computational Intelligence Magazine 2022, 17, p. 72-85 ; **Bert Heinrichs**, Discrimination in the age of artificial intelligence, AI & SOCIETY 2022, 37, p. 143-154 ; **Yoan Hermstrüwer/Pascal Langenbach**, Fair governance with humans and machines. MPI Collective Goods Discussion Paper 2022 ; **Chris Jay Hoofnagle/Bart Van Der Sloot/Frederik Zuderveen Borgesius**, The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law 2019, 28, p. 65-98 ; **Roman Jurowetzki/Daniel S. Hain/Juan Mateos-Garcia/Konstantinos Stathoulopoulos**, The Privatization of AI Research (-ers): Causes and Potential Consequences--From university-industry interaction to public research brain-drain? arXiv preprint

arXiv:2102.01648, 2021 ; **Florian JATON**, Assessing biases, relaxing moralism: On ground-truthing practices in machine learning design and application, Big Data & Society 2021, 8(1), 20539517211013569 (cité : JATON, Assessing biases, relaxing moralism) ; **Margot E. KAMINSKI**, The right to explanation, explained. Berkeley Tech 2019, LJ, 34, p. 189 ss (cité : KAMINSKI, The right to explanation, explained) ; **Margot E. KAMINSKI**, The right to explanation, explained, Research Handbook on Information Law and Governance, Cheltenham 2021 (cité : KAMINSKI, The right to explanation, explained) ; **Margot E. KAMINSKI/Jennifer M. URBAN**, The right to contest AI, Columbia Law Review 2021, 121, p. 1957-2048 ; **Miriam KULLMANN**, Algorithmenbasiertes Personalrecruiting: antidiskriminierungs-und datenschutzrechtliche Aspekte, Zeitschrift für Arbeits-und Sozialrecht, 2021, p. 61 ; **Yann LE CUN**, Quand la machine apprend : la révolution des neurones artificiels et de l'apprentissage profond, Paris 2019 ; **Fabian LÜTZ**, How the 'Brussels effect' could shape the future regulation of algorithmic discrimination, Duodecim Astra 2021, 1, p. 142-163 (cité : LÜTZ, Brussels effect) ; **Fabian LÜTZ**, Discrimination by correlation. Towards eliminating algorithmic biases and achieving gender equality, (Dis) Obedience in Digital Societies, Bielefeld 2022, p. 250-293 (cité : LÜTZ, Discrimination by correlation) ; **Fabian LÜTZ**, Gender equality and artificial intelligence in Europe, Addressing direct and indirect impacts of algorithms on gender-based discrimination. ERA Forum 2022, p. 33-52 (cité : LÜTZ, Gender Equality and AI in Europe) ; **Fabian LÜTZ**, Le rôle du droit pour contrer la discrimination algorithmique dans le recrutement automatisé, *in* Florence GUILLAUME (éd.) La technologie, l'humain et le droit, Bern 2023 (cité : LÜTZ, Discrimination algorithmique) ; **Gianclaudio MALGIERI/Giovanni COMANDÉ**, Why a right to legibility of automated decision-making exists in the general data protection regulation, International Data Privacy Law 2017 ; **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, p. 1-48 ; **Sylvain MÉTILLE/Annelise ACKERMANN**, RGPD : application territoriale et extraterritoriale. Datenschutzgrundverordnung (DSGVO): Tragweite und erste Erfahrungen = Le règlement général sur la protection des données (RPDG) : portée et premières expériences, 2020 ; **Sylvain MÉTILLE/Livio DI TRIA**, Protection des données: responsabilité croissante ? ; **Jakob MÖKANDER/Prathm JUNEJA/David WATSON/Luciano FLORIDI**, The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other? Minds and Machines 2022, 32, p. 751-758 ; **Jakob MÖKANDER/Jonas SCHUETT/Hannah Rose KIRK/Luciano FLORIDI**, Auditing large language models: a three-layered approach, 2023 (cité : MÖKANDER *et al*., Auditing LLMs) ; **Emanuel MOSS/Elizabeth Anne WATKINS/Jacob METCALF/Madeleine Clare ELISH**, Governing with algorithmic impact assessments: six observations, 2020 ; **Helga NOWOTNY**, In AI We Trust: Power, Illusion and Control of Predictive Algorithms, 2021, Polity Press ; **Frank PASQUALE**, New Laws of Robotics: Defending Human Expertise in the Age of AI, Belknap Press 2020 ; **Inioluwa Deborah RAJI/Sasha COSTANZA-CHOCK/Joy BUOLAMWINI**, Change From the Outside: Towards Credible Third-Party Audits of AI Systems, In: Missing Links in AI Policy, UNESCO/MILA Paris 2023 ; **Jonas REBSTADT/Henrik KORTUM/Laura Sophie GRAVEMEIER/Birgit EBERHARDT/Oliver THOMAS**, Non-Discrimination-by-Design: Handlungsempfehlungen für die Entwicklung von vertrauenswürdigen KI-Services, HMD 2022 59, p. 495-511 ; **Antoni ROIG**, Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR). European Journal of Law and Technology 2017, Vol. 8, Nº 3 ; **Ira RUBINSTEIN/Nathaniel GOOD**, The trouble with Article 25 (and how to fix it): the future of data protection by design and default, International Data Privacy Law 2020, 10, p. 37-56 ; **Peter SCHAAR**, Privacy by design, Identity in the Information Society 2010, 3, p. 267-274 (cité : SCHAAR, Privacy by

design) ; **Peter SCHAAR**, Datenschutz und Internet – Es ist kompliziert!, Informatik Spektrum 2020, 43, p. 179-185 (cité : SCHAAR, Datenschutz) ; **Andrew SELBST/Julia POWLES**, "Meaningful information" and the right to explanation. Conference on fairness, accountability and transparency, 2018. PMLR, p. 48-48 ; **Andrew SELBST**, An institutional view of algorithmic impact, Harvard Journal of Law & Technology 2021, p. 35 ss ; **Yun SHEN/Siani PEARSON**, Privacy enhancing technologies: A review, 2011, Hewlet Packard Development Company, disponible à : <https://bit. ly/3cfpAKz> ; **Nathalie SMUHA**, From a 'Race to AI' to a 'Race to AI Regulation': Regulatory Competition for Artificial Intelligence 2021 ; **Erica THOMPSON**, Escape from Model Land: How Mathematical Models Can Lead Us Astray and What We Can Do About It, London 2022 ; **Florent THOUVENIN/Nadia BRAUN BINDER/Melinda F. LOHMANN**, Regeln für den Einsatz von künstlicher Intelligenz (Gastkommentar), Neue Zürcher Zeitung, 27 février 2021 ; **Jamie SUSSKIND**, The Digital Republic, On Freedom and Democracy in the 21st Century, London 2022 ; **Florent THOUVENIN/ Markus CHRISTEN/Abraham BERNSTEIN *et. al.***, Positionspapier: Ein Rechtsrahmen für Künstliche Intelligenz ; **Luca TOSONI**, The right to object to automated individual decisions: resolving the ambiguity of Article 22 (1) of the General Data Protection Regulation. International Data Privacy Law 2021, 11, p. 145-162 ; **Marvin VAN BEKKUM/Frederic ZUIDERVEEN BORGESIUS**, Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? Computer Law & Security Review 2023, 48, p. 105770 ; **Sandra WACHTER/Bent MITTELSTADT/Luciano FLORIDI**, Why a right to explanation of automated decision-making does not exist in the general data protection regulation, International Data Privacy Law 2017, 7, p. 76-99 ; **Judy WAJCMAN/Erin YOUNG/Anna FITZMAURICE**, The digital revolution: Implications for gender equality and women's rights 25 years after Beijing 2020 ; **Betsy Anne WILLIAMS/Catherine F. BROOKS/Yotam SHMARGAD**, How algorithms discriminate based on data they lack: Challenges, solutions, and policy implycations, Journal of Information Policy 2018, 8, p. 78-115 ; **John ZERILLI**, A citizen's guide to artificial intelligence, Boston 2021.

B. Documents officiels

Conseil fédéral, « Intelligence artificielle » – lignes directrices pour la Confédération, Cadre d'orientation en matière d'IA dans l'administration fédérale 2020 ; **Organization for European Cooperation and Development (OECD)**, OECD/LEGAL/0449, Recommendation of the Council on Artificial Intelligence ; **College voor de Rechten van den Mens**, Inbreng College voor de Rechten van den Mens op verzoek van de commissie voor digitale Zaken 2022, 13 mai 2022 ; **Council of Europe**, Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, 2020 ; **Council of Europe**, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Nº 108, https://rm.coe.int/1680078b37 ; **Council of Europe**, Preliminary draft Council of Europe study on the impact of artificial intelligence, its potential for promoting equality, including gender equality, and the risks to non-discrimination, GEC(2022)9 CDADI(2022)21 ; **Council of Europe,** Committee on Artificial Intelligence (CAI), Revised zero draft [framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, CAI(2023)01 (cité : CoE, Zero Draft Convention on AI) ; **European Commission (EC)**, European Declaration on Digital Rights and Principles for the Digital Decade, JO 2023/C 23/01 ; **European Law Institute (ELI)**, Guiding Principles for Automated Decision-Making in the EU, Vienne 2022, disponible :

<https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf> ; **European Union Agency for Fundamental Rights (FRA)**, Bias in algorithms: artificial intelligence and discrimination, 2022, Publications Office of the European Union ; Netherlands Court of Auditors, An audit of 9 algorithms used by the Dutch government, The Hague 2022, disponible à : https://english.rekenkamer.nl/binaries/rekenkamer-english/documenten/reports/2022/05/18/an-audit-of-9-algorithms-used-by-the-dutch-government/An+Audit+of+Algorithms.pdf (cité : Court of Auditors NL, Algorithm Audit) ; **United Nations**, A/77/196: Principles underpinning privacy and the protection of personal data, 2022 ; **United Nations**, Commission on the Status of Women (CSW), 67th Conference, March 2023, E/CN.6/2023/3 – draft agreed conclusions (zero draft) ; **UNESCO**, Recommendation on the Ethics of Artificial Intelligence, 2021 (cite : UNESCO, Recommendation on the Ethics of AI) ; **UNESCO**, Guidelines for regulating digital platforms: A multistakeholder approach to safeguarding freedom of expression and access to information, 2023 ; **UNESCO/Mila**, Missing Links in AI Governance, Paris 2023 ; **Tilburg University**, Report Non-discrimination by design, 2019, disponible : <https://www.tilburguniversity.edu/sites/default/files/download/07%20Onderzoeksrapport%20non-discriminatie%20by%20design%20%28compr%29.pdf>.

La recherche scientifique dans le cadre de la Stratégie européenne pour les données

CECILE DE TERWANGNE
Professeure
Faculté de droit, Université de Namur
Directrice de recherches
Centre de Recherche Information, Droit et Société (CRIDS)

Table des matières

I. Introduction

Avec sa « Stratégie pour les données »[1], présentée en février 2020, l'Union européenne (UE) vise à bâtir « *un nouveau modèle doté de règles claires : un marché unique européen des données, ouvert mais souverain* »[2]. L'objectif affiché est de permettre de tirer pleinement parti du potentiel offert par les données. Ce potentiel à exploiter n'a pas pour seul horizon un marché unique de données mais il est aussi destiné à développer l'innovation et à nourrir les activités de recherche[3].

Les gigantesques gisements de données, détenus tant par le secteur public que par les acteurs privés et résultant de leurs activités respectives, représentent une formidable matière pour alimenter les recherches scientifiques en tout genre. Permettre l'accès et l'utilisation de ces données à des fins de recherche ouvre des perspectives sur des questions aussi variées que celles du climat et de la préservation de la biodiversité, du développement des activités économiques, de la santé publique, des mouvements migratoires, de la culture, de la mobilité, de l'éducation, de la criminalité, *etc*. L'exploitation de ce potentiel implique toutefois que les données soient partagées en toute confiance avec la communauté scientifique, dans le respect notamment des règles relatives à la protection des données, ainsi qu'à la propriété intellectuelle et aux secrets commerciaux.

La communauté scientifique intéressée à accéder aux données ne se limite bien évidemment pas à celle située dans les frontières de l'Union européenne. Comme on le verra dans les pages qui suivent, l'ouverture des données mise en place par le législateur européen est totalement indépendante de ces frontières : une fois acquis le principe de l'ouverture des données détenues par le secteur public des pays membres de l'UE et même de certains acteurs privés, et moyennant éventuellement le respect de certaines conditions, ces données sont à la disposition de tout intéressé de par le monde. La connaissance des ressources informationnelles rendues disponibles dans le cadre de la Stratégie européenne pour les données représente dès lors un atout non négligeable pour la communauté scientifique dans son ensemble, et singulièrement pour le monde suisse de la recherche.

1 CE, Une stratégie.

2 CE, Bâtir l'avenir.

3 CE, Une stratégie, p. 2-3 ; TOMBAL, Data Sharing by private actors, N 1 : « *as the societal value of the data held (exclusively) by some actors is enormous, allowing (some) third parties to use this data could generate immense scientific, environmental or mobility benefits for our society.* »

Les gisements de données publics et privés contiennent de nombreuses données portant sur des individus, des « données à caractère personnel »[4], mais la présente contribution est centrée sur les données non personnelles qui sont également récoltées et traitées par les administrations, les entreprises et autres acteurs privés[5].

Depuis deux décennies, avec une nette accentuation ces dernières années, l'Union européenne a veillé à l'ouverture des données détenues par le secteur public (*via* la directive *Open data*[6]), au partage volontaire de données (*via* le *Data Governance Act*[7]) ainsi que, finalement, au partage obligatoire de données (à travers le *Data Act*[8]).

La présente contribution suivra la même progression, présentant d'abord la directive 2019/1024 sur les données ouvertes et la réutilisation des données du secteur public, soit la directive *Open Data*[9] (*infra* II), pour ensuite se focaliser sur le règlement sur la gouvernance des données (*infra* III) et enfin évoquer la proposition de règlement sur les données (*infra* IV). Pour ces trois textes, le propos se focalisera sur leur impact quant à l'accessibilité des données pour la recherche.

4 Aux termes de l'article 4.1 du règlement général sur la protection des données (RGPD), une donnée à caractère personnel s'entend de « *toute information se rapportant à une personne physique identifiée ou identifiable (dénommée ‹ personne concernée ›)* ».

5 Pour les données à caractère personnel, qui sont soumises aux réglementations de protection spécifiques, il est renvoyé aux contributions de Samah Posse et Frédéric Erard dans le présent ouvrage.

6 Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, JO L 172/56, 2.6.2019, p. 56 ss (ci-après : Directive 2019/1024).

7 Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le Règlement (UE) 2018/1727, JO L 172/56, 3.6.2022, p. 1 ss (ci-après : DGA).

8 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), COM(2022) 68 final (ci-après : Proposition de règlement sur les données).

9 Cette directive étant couramment appelée la « directive *Open Data* », c'est cette appellation qui est conservée dans la suite du propos.

II. La directive 2019/1024 sur les données ouvertes et la réutilisation des données du secteur public (directive « *Open Data* »)

A. Stratégie européenne en faveur de l'ouverture des données détenues par le secteur public

Le législateur de l'Union européenne, conscient de la richesse des données détenues par le secteur public, œuvre depuis vingt ans en faveur du partage et de l'accessibilité de cette richesse informationnelle. L'année 2003 a vu l'adoption de la première directive en la matière[10], encourageant la réutilisation des données du secteur public et leur valorisation socio-économique dans le but de favoriser le développement de l'industrie européenne de contenu et des services d'information à valeur ajoutée. Ce texte n'impose pas l'ouverture des données au bénéfice des acteurs du marché et de la société. Le choix est laissé aux États membres appelés à transposer la directive, d'imposer cette ouverture ou de laisser à leurs autorités publiques la liberté d'autoriser ou non la réutilisation de leurs documents.

Si l'objectif premier visé par la directive de 2003 est de nature économique, le législateur européen a opté pour une définition de la « réutilisation »[11] des documents publics qui permet d'englober les utilisations à des fins non commerciales, ce qui couvre l'utilisation de données à des fins de recherche. La Commission européenne avait souligné dans son Livre vert précédant l'adoption de la directive, l'intérêt stratégique pour tous ceux qui désirent développer des recherches que présente l'information sur l'état de l'art dans la technique et la recherche, condensée dans les bases de données sur les brevets délivrés. Les bases de données constituées auprès de l'Office européen des brevets et des Offices équivalents au niveau national, donnent une vision globale des derniers développements dans une technique donnée. Elles permettent donc d'identifier les travaux déjà effectués et, dès lors, d'engager des budgets pour des projets de recherche et développement sur des bases réellement novatrices. La disponibilité aisée de cette information est donc capitale, d'autant que l'Office européen des brevets estime qu'en Europe, chaque année, des milliards

10 Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, JO L 345/90, 31.12.2003, p. 90 ss (ci-après : Directive 2003/98). Sur cette directive, voir not. POUPAERT/JANSSEN, p. 29-50 ; PAS/DE VUYST.

11 Aux termes de l'article 2, 4e de la directive 2003/98, la réutilisation est définie comme « *l'utilisation par des personnes physiques ou morales de documents détenus par des organismes du secteur public ou des entreprises publiques, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les documents ont été produits* ».

d'euros sont inutilement dépensés dans des travaux de recherche déjà entrepris par ailleurs. Cela dit, ainsi que relevé dans l'introduction de la présente contribution, le secteur public regorge de données en tout genre qui peuvent alimenter des recherches dans des domaines scientifiques remarquablement variés.

Les données en lien avec l'environnement ont fait l'objet d'une attention particulière qui a débouché sur la directive INSPIRE du 14 mars 2007[12] établissant une infrastructure d'information géographique dans l'Union européenne. Ce texte s'inscrit lui aussi dans une optique favorable au déploiement d'activités de recherche. Il a conduit à la mise en place d'une infrastructure en ligne permettant de mettre à disposition des organismes publics de tous les États membres ainsi que du public en général un vaste catalogue de données relatives aux politiques environnementales de l'Union européenne et aux politiques ou activités qui peuvent avoir un impact sur l'environnement[13]. Ce catalogue comprend les données sur les réseaux de transport, l'hydrographie, l'altimétrie, la géologie, la démographie, les installations industrielles et agricoles, l'occupation des sols, les données météorologiques, les données sur les sites protégés, sur l'état de l'environnement, le cadastre, *etc*.[14].

La directive de 2003 sur la réutilisation des informations du secteur public a fait l'objet de plusieurs modifications substantielles[15], ce qui a conduit le législateur européen à procéder à une refonte complète du texte. Cela a donné le jour à la directive 2019/1024, adoptée le 20 juin 2019, sur les données ouvertes et la réutilisation des données du secteur public, appelée plus couramment directive « *Open Data* »[16]. Les objectifs affirmés par le législateur européen sont ceux de favoriser une large réutilisation des informations détenues par le secteur public et obtenues à l'aide de fonds publics en instaurant le principe des données ouvertes, et de stimuler l'innovation dans les produits et services, et singulièrement l'innovation numérique intégrant l'intelligence artificielle[17]. On verra dans les paragraphes qui suivent que ces objectifs conduisent à permettre et à soutenir l'utilisation des données à des fins de recherche, que cette recherche s'effectue au sein de l'Union européenne ou ailleurs dans le monde.

---

12 Directive INSPIRE (Infrastructure for Spatial Information in the European Community) 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne

13 <https://inspire-geoportal.ec.europa.eu/> .

14 Voir annexes 1, 2 et 3 de la directive INSPIRE.

15 Voir Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public, JO L 175/1, 27.6.2013, p. 1 ss. Sur ce texte, voir KNOCKAERT.

16 Pour une analyse fouillée de cette directive, voir KNOCKAERT/MICHEL, La directive.

17 Article 1er et considérant 3 Directive 2019/1024.

B. Principe de libre réutilisation des données

La réutilisation est définie par la directive *Open data* comme étant « *l'utilisation par des personnes physiques ou morales de documents détenus par : a) des organismes du secteur public, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les documents ont été produits, à l'exception de l'échange de documents entre des organismes du secteur public aux seules fins de l'exercice de leur mission de service public ; ou b) des entreprises, à des fins commerciales ou non commerciales autres que l'objectif initial de fournir les services d'intérêt général pour lequel les documents ont été produits, à l'exception de l'échange de documents entre des entreprises publiques et des organismes du secteur public aux seules fins de l'exercice de leur mission de service public* »[18]. L'esprit de la directive de 2003 est donc conservé : tant les formes commerciales que non commerciales de réutilisation sont couvertes, ce qui englobe les usages à des fins de recherche.

Si la définition évoque la réutilisation de documents plutôt que de données, il ne faut pas y voir de réelle distinction étant donné que le *document* est défini comme « *tout contenu, quel que soit son support (papier ou forme électronique, enregistrement sonore, visuel ou audiovisuel)* »[19] et que toutes les données identifiées dans la suite de la directive (données dynamiques, données de la recherche et ensembles de données de forte valeur) sont définies comme étant des *documents*[20]. On notera que l'intitulé de la directive ajoute encore à la confusion car il mentionne la réutilisation des *informations* du secteur public[21].

Dans la lignée de la révision de la directive de 2003 réalisée en 2013, la Directive 2019/1024 maintient le principe, inséré alors, de l'obligation pour les acteurs du secteur public de rendre tous les documents qu'ils détiennent réutilisables, sous réserve de certaines exceptions[22]. Cette obligation s'impose

18 Article 2, 11e Directive 2019/1024.

19 Article 2, 6e Directive 2019/1024. Le considérant 30 apporte cette précision : « Le terme ‹ document › devrait couvrir toute représentation d'actes, de faits ou d'informations – et toute compilation de ces actes, faits ou informations ».

20 Article 2, 8e, 9e et 10e Directive 2019/1024.

21 KNOCKAERT et MICHEL relèvent également la surprenante attitude du législateur européen qui opte, dans l'intitulé de la directive, pour deux notions (« *data* » et « informations ») alors qu'il maintient le recours à l'ancienne notion de « document » pour déterminer le champ d'application de la directive (KNOCKAERT/MICHEL, La directive, p. 79).

22 Article 3 Directive 201/1024. Il est à noter que le concept de « données ouvertes/*open data* » ne correspond pas exactement à ce qu'il recouvre d'ordinaire (il « *s'entend généralement comme désignant des données présentées dans un format ouvert qui peuvent être librement utilisées, réutilisées et partagées par tous quelle qu'en soit la*

à tous les organismes du secteur public, ce qui inclut les organismes de droit public, c'est-à-dire les organismes assumant une mission d'intérêt général[23]. Grâce au considérant 43 de la directive, on perçoit que ce qui est visé par le « secteur public », c'est l'ensemble des pouvoirs étatiques. Ce considérant énonce en effet : « *La publicité de tous les documents généralement disponibles qui sont détenus par le secteur public – non seulement par la filière politique, mais également par la filière judiciaire et la filière administrative – constitue un instrument essentiel pour développer le droit à la connaissance, principe fondamental de la démocratie. Cet objectif est applicable aux institutions, et ce, à tous les niveaux, tant local que national et international*. » Pour que l'obligation de rendre les documents réutilisables s'impose, il faut que les acteurs du secteur public disposent des documents. Cela implique que les documents existent réellement. Ils ne doivent pas être créés.

Dans la version de 2019, le principe d'ouverture des données a été étendu et s'applique désormais non seulement aux documents existants détenus par des organismes du secteur public des États membres de l'UE, mais également à ceux détenus par des entreprises publiques actives dans certains domaines (dans les secteurs de l'eau, l'énergie, les transports et les services postaux)[24]. Cet élargissement du champ d'application personnel de la directive présente assurément de l'intérêt pour les activités de recherche étant donné que cela ouvre aux chercheurs l'accès à des données en matières énergétiques et des transports, matières au cœur de travaux scientifiques intenses aujourd'hui. Ces entreprises publiques ne sont toutefois pas tenues d'ouvrir d'office leurs documents à la réutilisation, la directive laissant à ces entreprises ou aux États membres la liberté d'autoriser ou non la réutilisation de ces documents[25].

Il en est de même pour les documents sur lesquels les bibliothèques, musées et archives sont titulaires de droits de propriété intellectuelle[26]. Pour cette dernière catégorie de détenteurs de documents, Manon KNOCKAERT et Alejandra MICHEL observent avec pertinence qu'« [i]*l ne faut pas perdre de vue qu'en pratique la majorité des collections des bibliothèques et des musées est constituée d'œuvres sur lesquelles des tiers détiennent des droits.* »[27] Or, ainsi qu'on le verra dans les paragraphes qui suivent, les documents pour lesquels des tiers détiennent les droits sont exclus du champ d'application de la directive. Les deux auteurs poursuivent : « *en raison de l'existence majoritaire (pour ne pas dire quasi totale) de documents avec des droits de propriété intellectuelle de tiers, les*

finalité » – consid. 16 Directive 2019/1024), même s'il s'en approche fortement. Sur ces différences, voir KNOCKAERT/MICHEL, La directive, p. 78-79 ; GERARD, p. 320.

23 Article 2, 1° et 2° Directive 2019/1024.

24 Article 1, § 1, b Directive 2019/1024.

25 Article 3, § 2 Directive 2019/1024.

26 Article 3, § 2 Directive 2019/1024.

27 KNOCKAERT/MICHEL, La directive, p. 76, n. 35.

autres établissements culturels (opéras, orchestres, théâtres, salles de concerts, châteaux, galeries d'art ou encore cinémas) n'entrent pas dans le champ d'application de la directive. »[28]

Une des importantes nouveautés introduites par la directive *Open Data* est l'ouverture de principe des données de la recherche détenues par des organismes de recherche financés sur fonds publics ou par des organismes qui financent la recherche[29]. On reviendra dans le point *infra* C sur le régime réservé désormais à ce type de données.

Le principe d'ouverture des données du secteur public à la réutilisation n'est pas absolu. Des catégories de documents font ainsi exception à la règle d'ouverture, parmi lesquels[30] :

– les documents dont la fourniture ne relève pas de la mission de service public confiée aux organismes concernés : il s'agit des produits d'information que l'organisme public aurait développés dans le cadre d'activités de type commercial (statistiques ciblées élaborées par l'Institut National des Statistiques à la demande d'un client, par exemple) ;
– les documents détenus par des entreprises publiques, dont la production ne relève pas du service d'intérêt général, ou qui sont relatifs à des activités directement exposées à la concurrence ;
– les documents sur lesquels des tiers détiennent les droits de propriété intellectuelle : ainsi, pour que les études réalisées par des tiers à la demande d'une autorité soient soumises à la législation de réutilisation, il faut que l'organisme ait prévu le transfert des droits de propriété intellectuelle à son bénéfice ;
– les documents qui ne sont pas accessibles compte tenu des règles d'accès en vigueur : il est clair que ce qu'on ne peut pas voir, on ne peut pas davantage le réutiliser[31] ;
– ou encore, les documents qui contiennent des données dont la réutilisation porterait atteinte à la protection de la vie privée et de l'intégrité de la personne concernée, en particulier au regard du droit sur la protection des données à caractère personnel ; cette exclusion ne se justifie donc pas par de pures préoccupations au regard de la législation de protection des données (le fameux RGPD essentiellement), mais intègre un élément inhabituel : l'intégrité des individus. Aucun éclairage additionnel n'est malheureusement apporté par le texte à ce propos.

28 KNOCKAERT/MICHEL, La directive, p. 76, n. 35. Ég. : KER, p. 62-64.
29 Article 1er, § 1, c) et 3, § 1 Directive 2019/1024.
30 Article 1, § 2 Directive 2019/1024.
31 DE TERWANGNE, Réutilisation, p. 142 ; POUPAERT/JANSSEN, p. 33.

Pour les documents qui ne correspondent pas à ces exceptions et qui donc sont soumis au régime général de l'ouverture de principe à la réutilisation, leur mise à disposition doit s'effectuer en principe gratuitement[32] dans tout format ou toute langue préexistants et, si possible, sous forme électronique, dans un format ouvert[33], lisible par machine, accessible, traçable et réutilisable, en les accompagnant de leurs métadonnées[34]. La mise à disposition des documents a lieu soit spontanément en ligne, à l'initiative des acteurs publics, à l'instar de ce qui est prévu pour alimenter les points d'accès uniques aux données[35] (voir *infra*), soit en réponse à des demandes individuelles émanant de « candidats réutilisateurs »[36]. Ces candidats réutilisateurs désireux d'accéder aux données pour les réexploiter peuvent provenir de tous les horizons géographiques. Le texte ne limite pas les destinataires aux personnes physiques ou morales situées dans l'UE.

On notera que les organismes du secteur public ne sont pas tenus de poursuivre la production et la conservation d'un certain type de données pour répondre à des demandes d'acteurs privés ou publics[37]. L'interruption de collecte ou de production de données peut ainsi impacter négativement des recherches longitudinales qui visent à observer un phénomène sur une période d'une certaine durée. Le chercheur ou l'organisme de recherche dépité face à la source tarie ne pourra exiger de l'organisme public que celui-ci maintienne son activité afin qu'il dispose des données pour conclure sa recherche. Les auteurs de la directive ont été conscients des désagréments et difficultés qu'une soudaine interruption de collecte ou de production de données pouvait présenter pour les réutilisateurs habituels. Il est dès lors déclaré (mais seulement dans un considérant) que « *si l'autorité compétente décide de ne plus mettre à disposition certains documents en vue de leur réutilisation ou de ne plus les mettre à jour, elle devrait rendre ses décisions publiques dans les meilleurs délais, par voie électronique chaque fois que cela est possible*. »[38]

C. Libre accès aux données de la recherche

Cela fait plusieurs décennies que l'Union européenne marque sa préoccupation en faveur de la recherche, notamment à travers ses programmes-

32 Article 6 Directive 2019/1024.
33 Format de fichier « *indépendant des plates-formes utilisées et mis à disposition du public sans restriction empêchant la réutilisation des documents* » (article 2.14 de Directive 2019/1024).
34 Article 5 Directive 2019/1024.
35 Article 9, § 2 Directive 2019/1024.
36 KNOCKAERT/MICHEL, La directive, p. 82.
37 Article 5, § 4 Directive 2019/1024.
38 Consid. 45 Directive 2019/1024.

cadres pour la recherche et le développement. Ainsi, sur une impulsion donnée par la Commission, le Conseil européen de Lisbonne a établi, au tournant du millénaire, les fondations d'un Espace Européen de la Recherche[39].

Plus récemment, le programme-cadre « Horizon Europe » pour la recherche et l'innovation pour les années 2021 à 2027 instaurait un principe d'accès ouvert immédiat aux publications et aux données[40].

Cette attention particulière se retrouve dans la directive *Open Data*, très clairement dans le régime spécifique nouveau qui est réservé aux données de la recherche.

Par « données de la recherche », il faut entendre « *des documents se présentant sous forme numérique, autres que des publications scientifiques, qui sont recueillis ou produits au cours d'activités de recherche scientifique et utilisés comme éléments probants dans le processus de recherche, ou dont la communauté scientifique admet communément qu'ils sont nécessaires pour valider des conclusions et résultats de la recherche* »[41]. Il ne s'agit donc pas des résultats de la recherche à proprement parler ni des publications scientifiques qui présentent et commentent ces résultats mais bien des données servant à démontrer ou valider le processus de recherche, données qu'il convient de « *diffuser le plus largement possible afin d'assurer l'objectivité et le sérieux de la recherche* »[42]. À titre d'illustration, le considérant 27 de la directive 2019/1024 énonce que ces données de la recherche peuvent comprendre des statistiques, des résultats d'expériences, des mesures, des observations faites sur le terrain, des résultats d'enquêtes, des enregistrements d'entretiens ou des images. Elles peuvent prendre aussi la forme de métadonnées, de spécifications ou d'autres objets numériques[43].

39 Commission européenne, Communication au Conseil, au Parlement européen, au Comité économique et social et au Congrès des régions, « *Vers un espace européen de la recherche* », 18 décembre 2000, COM(2000)6 final. Cet Espace Européen de la Recherche a vu sa structure révisée en profondeur en 2021 tandis que l'UE se dotait d'un nouveau « *Pacte pour la recherche et l'innovation en Europe* », <https://www.consilium.europa.eu/fr/policies/european-research-area/>.

40 Règlement (UE) 2021/695 du Parlement européen et du Conseil, 28 avril 2021, portant établissement du programme-cadre pour la recherche et l'innovation « Horizon Europe » et définissant ses règles de participation et de diffusion, et abrogeant les règlements (UE) 190/2013 et (UE) 1291/2013, JO L 170/1, 12.5.2021, p. 1 ss.

41 Article 2, 9e Directive 2019/1024. Voir Robin, p. 95.

42 Robin, p. 22.

43 Consid. 27 Directive 2019/1024.

La directive[44] encourage la mise à disposition par défaut des données de la recherche en invitant les États membres à adopter des politiques de libre accès[45] afin de rendre accessibles et réutilisables par quiconque, à des fins tant commerciales que non commerciales, les données résultant de la recherche. Le libre accès ne s'impose que lorsque la recherche est financée au moyen de fonds publics, ou plus précisément lorsque les données de la recherche « *sont issues d'un processus de recherche financé au moins majoritairement par des fonds publics, incluant donc la recherche partenariale (ou mixte)* »[46]. Ces politiques de libre accès concernent les organismes exerçant une activité de recherche et les organisations finançant une activité de recherche[47]. Afin d'éviter toute charge administrative, une condition a été ajoutée à celle du financement de la recherche sur fonds publics : les politiques de libre accès des données de la recherche ne s'imposent que lorsque le chercheur, l'organisme de recherche ou l'organisation finançant la recherche ont déjà rendu les données publiques par l'intermédiaire d'une archive ouverte institutionnelle ou thématique[48]. Cette condition suscite des réserves au vu des risques de contre-productivité qu'elle présente : « *suffirait-il ainsi à la communauté scientifique de ne plus rendre publiquement accessibles les données de la recherche afin de ne pas se soumettre aux obligations de la directive ?* »[49]. Les recherches financées dans le cadre du programme Horizon Europe évoqué antérieurement ne peuvent en tout cas pas échapper à la règle du libre accès car c'est devenu une condition du financement des recherches[50].

Pour décider de la mise à disposition en libre accès des données, il doit être tenu compte des exigences découlant des droits de propriété intellectuelle, de la protection des données à caractère personnel et de la confidentialité, de la sécurité et des intérêts commerciaux légitimes, en veillant à respecter le principe « *aussi ouvert que possible, mais aussi fermé que nécessaire* »[51].

La politique de libre accès aux données de la recherche présente les avantages indéniables qu'elle contribue à améliorer la qualité des recherches, à réduire

---

44 Article 10, § 1er Directive 2019/1024.

45 « *Le libre accès s'entend comme la pratique consistant à fournir gratuitement l'accès en ligne à des résultats de recherche à l'utilisateur final, sans restriction sur l'utilisation et la réutilisation au-delà de la possibilité d'exiger l'indication de l'auteur.* » (Consid. 27 Directive 2019/1024). Voir ég. la recommandation 2018/790 de la Commission.

46 ROBIN, p. 95.

47 Consid. 27 Directive 2019/1024.

48 Article 10, § 2 Directive 2019/1024.

49 KNOCKAERT/MICHEL, La directive, p. 83.

50 Pour des développements détaillés sur ces programmes, voir KNOCKAERT/MICHEL, La directive, p. 83-84.

51 Article 10, § 1er Directive 2019/1024. Une formulation plus juste du principe serait « *aussi ouvert que possible et pas plus fermé que nécessaire* » (voir ROBIN, p. 74).

les duplications inutiles, à accélérer le progrès scientifique et à lutter contre la fraude scientifique[52].

D. Mise à disposition des ensembles de données de forte valeur

Parmi les catégories de données auxquelles un sort spécifique est réservé par le législateur européen dans la directive *Open Data*, signalons les ensembles de données de forte valeur (*high value data*). Ces ensembles de données se caractérisent par leur aptitude à générer des avantages (ou « retombées positives »[53]) sociaux, économiques ou environnementaux importants et à servir au développement de services à valeur ajoutée et d'applications innovantes dont le nombre de bénéficiaires potentiels est élevé[54].

Six catégories thématiques ont d'ores et déjà été identifiées et figurent dans l'annexe I de la directive *Open Data*. Il s'agit des données géospatiales (telles que les codes postaux, les cartes nationales et locales) ; celles relatives à l'observation de la terre et à l'environnement (comme la consommation d'énergie et les images satellitaires) ; les données météorologiques (notamment les données *in situ* provenant d'instruments et de prévisions météorologiques) ; les statistiques (les indicateurs démographiques et économiques, par exemple) ; les données sur les entreprises et la propriété d'entreprises (les registres du commerce et les identifiants d'enregistrement) ; et enfin les données liées à la mobilité (telles que la signalisation routière et les voies de navigation intérieures)[55].

La Commission européenne est appelée à faire évoluer cette liste et à identifier éventuellement de nouveaux ensembles de données de forte valeur en fonction de l'évolution technologique et sociale. La directive l'invite expressément à procéder à des consultations appropriées, notamment d'experts, pour établir la liste détaillée de tels ensembles de données de forte valeur[56]. Cela a déjà débouché sur un premier règlement d'exécution adopté par la Commission fin décembre 2022[57].

52 Consid. 27 Directive 2019/1024.
53 Article 2.10 Directive 2019/1024.
54 Article 2.10 et consid. 66 Directive 2019/1024.
55 Tous les exemples proviennent du considérant 66 de la Directive 2019/1024.
56 Article 14, § 2 Directive 2019/1024.
57 Règlement d'exécution (UE) 2023/138 de la Commission du 21 décembre 2022 établissant une liste d'ensembles de données de forte valeur spécifiques et les modalités de leur publication et de leur réutilisation JO L 19/43, 20.1.2023, p. 43 ss. À propos des données environnementales reprises dans ce règlement d'exécution, voir KNOCKAERT/MICHEL, Le cadre européen, N 42.

Le régime juridique réservé aux ensembles de données de forte valeur est particulièrement favorable à l'égard des personnes intéressées à accéder à ces ensembles de données et à les réutiliser, notamment pour la recherche, étant donné que ces ensembles doivent être mis à disposition gratuitement et leur téléchargement de masse doit être possible[58]. Des exceptions à la gratuité sont toutefois admises pour les entreprises publiques si la gratuité devait entraîner une distorsion de concurrence, ainsi que pour les bibliothèques, y compris les bibliothèques universitaires, les musées et les archives. Quant aux organismes du secteur public tenus de générer des recettes pour couvrir une partie substantielle des coûts liés à l'exécution de leurs missions de service public, si la gratuité a une incidence trop importante sur leur budget, une tolérance de deux ans leur est accordée à partir de l'entrée en vigueur du règlement d'exécution de décembre 2022, pour assurer leur viabilité financière[59].

E. Mise à disposition immédiate des données dynamiques

La troisième catégorie particulière de données faisant l'objet d'un régime spécifique est celle des « données dynamiques ». Ces données se présentent sous forme numérique et font l'objet « *d'actualisations fréquentes ou en temps réel, notamment à cause de leur volatilité ou de leur obsolescence rapide* »[60]. Elles se distinguent donc des données statiques, contenues dans des ensembles essentiellement figés[61]. À titre d'exemples de données dynamiques, on citera les données environnementales, les données sur la circulation, les données satellitaires et météorologiques ou les données émanant de capteurs[62]. En matière de transports publics, de nombreuses données présentent cette caractéristique de dynamisme ou de fluidité[63]. Il en est ainsi de « *l'information en temps réel sur un déplacement donné ; des informations sur les correspondances pendant le déplacement, avec réannonce en cas de rupture ;* […] *des informations pour les réservations et achat de titres ;* […] *du signalement par les usagers des anomalies sur les équipements ; des annonces de perturbation et de reroutage proactif,* […] ».[64]

58 Article 14, § 1, al. 2 Directive 2019/1024.
59 Article 14, § 5 Directive 2019/1024.
60 Article 2, 8e Directive 2019/1024.
61 ROBIN, p. 90-91.
62 Consid. 32 Directive 2019/1024.
63 ROBIN, p. 91.
64 Comité du débat sur l'ouverture des données relatives à l'offre de transport, Ouverture des données de transport, Rapport au secrétaire d'État chargé des Transports, de la Mer et de la Pêche, 2015, p. 34-35, disponible à :<https://trafic-routier.data.cerema.fr/IMG/pdf/vf_rapport_jutand.pdf>.

Le législateur européen tenait particulièrement à faire entrer cette nouvelle catégorie de données dans le champ de la directive. Au titre des changements fondamentaux qu'il lui fallait apporter au texte de 2003/2013 afin de tirer pleinement parti du potentiel des informations du secteur public pour l'économie et la société européennes, il cite ainsi, en premier lieu, « *la fourniture d'un accès en temps réel à des données dynamiques par des moyens techniques adéquats* »[65].

Les délais de mise à disposition sont cruciaux pour les données dynamiques dont la valeur (qu'il s'agisse de valeur économique, sociale ou d'intérêt scientifique pour certains types de recherches) dépend de la mise à disposition immédiate et d'une mise à jour régulière[66]. Ces données dynamiques ont en effet pour « *finalité de nourrir un système d'analyse en temps réel* »[67]. Ces données doivent en conséquence être mises à disposition aux fins de la réutilisation « *aussitôt qu'elles ont été recueillies* »[68], sauf si cela impose un effort disproportionné au vu de la taille et des capacités financières et techniques de l'organisme détenteur des données[69]. En cas de mise à jour manuelle, la mise à disposition doit intervenir immédiatement après la modification du jeu de données[70]. Si une vérification des données dynamiques est nécessaire pour des raisons d'intérêt général (en matière de santé ou de sécurité publiques, par exemple), les données doivent être accessibles immédiatement après la vérification[71].

Enfin, la directive prévoit qu'une mise à disposition sous la forme d'un téléchargement de masse des données dynamiques doit, le cas échéant, être proposée[72].

F. Point d'accès unique aux données

Les États membres de l'Union européenne sont invités[73] à mettre en place, en coopération avec la Commission, un point d'accès unique permettant de simplifier l'accès aux ensembles de données. L'ambition est de mettre à disposition en un seul point, progressivement, des ensembles de données détenus

65 Consid. 4 Directive 2019/1024.
66 Consid. 31 Directive 2019/1024.
67 ROBIN, p. 91.
68 Article 5, § 5 Directive 2019/1024.
69 Article 5, § 6 et consid. 32 Directive 2019/1024.
70 Consid. 31 Directive 2019/1024. KNOCKAERT/MICHEL, p. 87.
71 Consid. 31 Directive 2019/1024.
72 Article 5, § 5 Directive 2019/1024.
73 Article 9, § 2 Directive 2019/1024.

par des organismes du secteur public, dans des formats accessibles, traçables et réutilisables sous forme électronique.

Un portail européen a ainsi vu le jour sur Internet[74] et est déjà une voie d'accès à de très nombreux jeux de données provenant de l'Union européenne et de ses États membres mais également de pays tiers. Certains de ces pays tiers ont une présence importante sur ce portail. Ainsi le Royaume-Uni et l'Ukraine occupent les 7e et 8e places au vu du nombre de jeux de données mis à disposition[75]. La Suisse, quant à elle, se situe à une très honorable 13e place sur 36. Elle met à disposition du public, via ce portail, près de 12'000 jeux de données. Ces données présentent une surprenante variété. On peut notamment accéder aux manuscrits numérisés provenant des bibliothèques et archives suisses, à l'indice des prix de l'offre totale (IPOT) et ses variations depuis 1914, à des données sur la migration des réfugiés juifs, aux données sur les gisements d'eau souterraine, à des enregistrements de musique et de matériel cinématographique du domaine public, aux chiffres-clés des hôpitaux suisses, à la correspondance de Thomas Mann, à l'Herbier de l'Université de Neuchâtel, ou à des informations sur des jeux vidéo indépendants créés par des développeurs ou des studios suisses...[76]

Les autres pays tiers contributeurs de la plateforme « *data.europa* » sont la Norvège, le Liechtenstein, la Moldavie et la Serbie.

Une « entité » originale parmi les contributeurs du portail européen couvre les « Océans du monde ». On peut y retrouver par exemple les aires de pépinières de morues ou la répartition géographique d'éclosion de l'églefin, une carte de l'habitat des fonds marins de l'Atlantique, ou les concentrations de glace dans l'Océan Arctique[77].

III. Le règlement sur la gouvernance des données (*Data Governance Act*)

En adoptant le 30 mai 2022 son règlement sur la gouvernance des données (plus communément appelé sous sa dénomination anglaise : *Data Governance Act* – DGA) qui est en vigueur depuis le 23 juin 2022 mais n'est d'application que depuis le 24 septembre 2023, le législateur européen a souhaité rendre davantage de données disponibles pour la réutilisation tout en

74 <www.data.europa.eu> .

75 Respectivement près de 55'000 et de 30'000 jeux de données.

76 <https://data.europa.eu/data/datasets?locale=fr&dataScope=countryData&country=countryData&country=ch&page=1&limit=10>.

77 <https://data.europa.eu/data/datasets?locale=fr&dataScope=countryData&country=countryData&country=world-ocean&page=1&limit=10>.

tenant compte des contraintes pesant sur les données. Son objectif était également de parvenir à stimuler l'innovation en facilitant le partage des données dans les domaines de la santé, de l'environnement, de l'énergie, de l'agriculture, de la mobilité, de la finance, de l'industrie manufacturière, de l'administration publique et des compétences[78].

Les activités de recherche sont donc directement concernées par le règlement DGA, étant donné que celui-ci « *ouvrira des perspectives pour l'innovation fondée sur les données et rendra les données plus accessibles à tous* »[79]. Les auteurs du texte ont d'ailleurs illustré cela dès l'entame du règlement puisque le deuxième considérant énonce que « *l'innovation fondée sur les données apportera des avantages considérables* [notamment] *en améliorant et en personnalisant la médecine, en offrant une mobilité nouvelle et en contribuant* [au] *pacte vert pour l'Europe* », trois perspectives nécessairement liées à la recherche.

S'il vise à élargir le champ des réutilisations possibles de données détenues par le secteur public, et à aller dès lors au-delà de la directive *Open Data*, le DGA ne crée pas pour autant d'obligation, pour les organismes du secteur public, d'autoriser la réutilisation de leurs données[80].

Signalons que le DGA s'adresse aux seuls organismes du secteur public. Il ne s'applique pas aux données détenues par les entreprises publiques, les radiodiffuseurs publics, les établissements culturels et les établissements d'enseignement[81].

A. Réutilisation de certaines catégories de données détenues par des organismes du secteur public

Une série de données détenues par les organismes du secteur public ne peuvent pas être partagées dans le cadre de la directive *Open Data* car elles sont protégées par des droits de tiers. C'est ainsi le cas de données à caractère personnel protégées par le RGPD (règlement général de protection des données), ou de données couvertes par des droits de propriété intellectuelle, ou de données objets de secrets commerciaux, de secrets d'affaires ou de secret professionnel, ou encore de données couvertes par le secret statistique[82].

L'objectif du législateur européen au travers de son règlement sur la gouvernance des données est de permettre les réutilisations de ces données qui n'entrent pas dans la stratégie d'ouverture de l'Union, en entourant ces réutilisations

78 Consid. 2 du DGA.
79 CE, Communiqué de presse.
80 Article 1, § 2 DGA.
81 Article 3, § 2 DGA.
82 Article 3, § 1 et consid. 6 DGA.

de garanties spécifiques. Il est précisé que c'est « *afin de faciliter l'utilisation des données par les entités privées et publiques dans le cadre de la recherche et de l'innovation en Europe,* [qu'] *il est nécessaire de fixer des conditions claires pour l'accès à ces données et leur utilisation dans l'ensemble de l'Union* »[83]. Une précision éclairante est apportée sur la notion de « recherche scientifique » dans le considérant 25 qui énonce : « *Dans ce contexte spécifique, les finalités liées à la recherche scientifique devraient s'entendre comme incluant tout type d'objectif en rapport avec la recherche, quelle que soit la structure organisationnelle ou financière de l'organisme de recherche concerné, à l'exception de la recherche menée par une entreprise ayant pour but la mise au point, l'amélioration ou l'optimisation de produits ou de services*. »

Si les données en question ne deviennent donc pas pour autant des données ouvertes, elles sont néanmoins réutilisables selon des règles spécifiques. Les organismes du secteur public ne sont pas libérés des obligations de confidentialité qui leur incombent[84]. Pour ouvrir leur porte et leurs serveurs aux réutilisateurs, et singulièrement aux chercheurs, ils devront dès lors respecter les conditions de réutilisation établies dans le règlement[85]. Les conditions appliquées concrètement aux réutilisateurs doivent être rendues publiques[86] et être non discriminatoires, transparentes, proportionnées et objectivement justifiées en ce qui concerne les catégories de données et les finalités de la réutilisation[87]. Le considérant 15 précise que les conditions de réutilisation « *devraient être conçues de manière à promouvoir la recherche scientifique afin que, par exemple, le fait de privilégier la recherche scientifique puisse en principe être considéré comme non discriminatoire* ».

Des redevances raisonnables peuvent être réclamées pour la réutilisation de données mais elles ne peuvent excéder les coûts nécessaires encourus et doivent, elles aussi, être transparentes, proportionnées, non discriminatoires et objectivement justifiées. Les organismes peuvent appliquer des frais réduits ou nuls pour encourager la réutilisation à des fins de recherche scientifique[88].

Afin de maintenir le caractère protégé des données, les organismes du secteur public qui sont sollicités pour des réutilisations de leurs données doivent anonymiser celles-ci si ce sont des données à caractère personnel, ou les agréger ou les modifier pour préserver la confidentialité des éléments couverts par le secret commercial ou pour respecter les droits de propriété intellectuelle qui

83 Consid. 6, *in fine*, DGA (c'est nous qui soulignons). Voir ég. consid. 16.
84 Article 1, § 2 DGA.
85 Il convient en outre de respecter toutes les conditions contenues dans le RGPD (article 1er, § 3 DGA). Voir KNOCKAERT/MICHEL, La directive, p. 91-92.
86 Article 3, § 1 et consid. 6 DGA.
87 Article 3, § 2 et consid. 6 DGA.
88 Article 6 DGA.

sont attachés à ces éléments[89]. Même en présence de données à caractère non personnel, il faut être prudent et le règlement invite à refuser de transmettre des données *a priori* anonymes s'il y a lieu de croire que par combinaison avec d'autres jeux de données, on pourrait aboutir à l'identification des personnes[90]. Les organismes doivent par ailleurs proposer l'accès aux données à distance dans un environnement de traitement sécurisé qu'ils contrôlent, ou, à défaut, l'accès sur place dans leurs locaux (p. ex., dans des salles de données), dans le respect de normes de sécurité élevées.[91] Enfin, il est interdit aux réutilisateurs de rétablir l'identité de toute personne concernée dont ils traitent les données[92].

Il est à signaler que pour transférer hors de l'UE des données confidentielles, non personnelles, provenant d'organismes du secteur public, il faut que l'État de destination soit reconnu par la Commission européenne comme assurant la protection de la propriété intellectuelle et des secrets d'affaires d'une manière essentiellement équivalente à la protection assurée par le droit de l'Union[93], ou que le réutilisateur qui a l'intention de transférer les données dans un pays tiers ne répondant pas à cette première condition offre lui-même des garanties contractuelles en ce sens[94]. « *Concrètement, en Suisse, la mesure concernera des entreprises ou des organismes (p. ex. instituts de recherche ou hautes écoles) qui ont accès à des données confidentielles publiées dans l'UE par des organismes du secteur public et qui souhaiteraient les transférer en Suisse*. »[95]. On ne confondra pas, même si elles sont sensiblement proches, les (futures) décisions d'adéquation relatives au transfert de données confidentielles non personnelles, des décisions d'adéquation prises par la Commission dans le cadre du RGPD, relatives au transfert de données à caractère personnel hors de l'UE.

B. Services d'intermédiation

Selon le législateur européen, les services d'intermédiation de données « *sont appelés à jouer un rôle essentiel dans l'économie des données, notamment en soutenant et en promouvant les pratiques volontaires de partage de données entre les entreprises, ou en facilitant le partage de données* […]. *Ils pourraient devenir un outil facilitant l'échange de quantités substantielles de données pertinentes*. »[96]. En publiant sa proposition de texte qui allait devenir

89 Article 5, § 3, a DGA.
90 Consid. 15 DGA.
91 Article 5, § 3, b et c DGA.
92 Article 5, § 5 DGA.
93 Article 5, § 12 DGA.
94 Article 5, § 10 DGA. Une hypothèse spécifique de transfert avec le consentement du détenteur de droits est également prévue à l'article 5, § 9.
95 DETEC/DFAE/DFF/DEFR, p. 16.
96 Consid. 27 DGA.

le DGA, la Commission européenne avait signalé que l'objectif poursuivi était d'établir les règles d'une nouvelle gouvernance européenne des données appelée à remplacer le modèle de plateformes dirigé par les grandes entreprises technologiques[97].

Le règlement encadre la reconnaissance et la mise en place de ces nouveaux acteurs, les fournisseurs de services d'intermédiation de données, afin d'établir un modèle basé sur la confiance et garantissant aux personnes et aux organismes le contrôle de leurs données. Ces fournisseurs sont des intermédiaires neutres mettant en relation soit des détenteurs de données avec des utilisateurs potentiels, soit des sujets de données désireux de mettre à disposition leurs données à caractère personnel, avec des utilisateurs potentiels[98].

Ces services d'intermédiation vont pouvoir jouer un rôle déterminant pour donner forme à l'altruisme en matière de données qui repose sur des intermédiaires pour générer la confiance (voir la section suivante).

C. Altruisme en matière de données/Partage volontaire de données

Le DGA encourage la mise à disposition de données à des fins d'altruisme, c'est-à-dire un partage volontaire des données pour le bien commun.

Cette forme d'altruisme est définie par le règlement comme étant « *le partage volontaire de données fondé sur le consentement donné par les personnes concernées* [(c.-à-d. des individus)] *au traitement de données à caractère personnel les concernant, ou l'autorisation accordée par des détenteurs de données* [(c.-à-d. des acteurs privés ou publics[99])] *pour l'utilisation de leurs données à caractère non personnel sans demander ni recevoir de contrepartie qui aille au-delà de la compensation des coûts qu'ils supportent lorsqu'ils mettent à disposition leurs données*, *pour des objectifs d'intérêt général prévus par le droit national, le cas échéant, par exemple les soins de santé, la lutte contre le changement climatique, l'amélioration de la mobilité, la facilitation du développement, de la production et de la diffusion de statistiques officielles, l'amélioration de la prestation de services publics, l'élaboration des politiques*

97 CE, Executive Summary. Eg. ROBIN, p. 40, n. 38.

98 Article 10 DGA.

99 La définition que donne l'article 2, 8° DGA du détenteur de données est plus précise puisqu'elle vise « *une personne morale, y compris des organismes du secteur public et des organisations internationales, ou une personne physique qui n'est pas une personne concernée pour ce qui est des données spécifiques considérées, qui, conformément au droit de l'Union ou au droit national applicable, a le droit d'octroyer l'accès à certaines données à caractère personnel ou non personnel* ».

publiques ou la recherche scientifique dans l'intérêt général »[100]. Il est donc question d'altruisme en matière de données lorsque des personnes, des organismes publics ou des entreprises donnent leur consentement ou leur autorisation pour mettre à disposition les données personnelles ou non personnelles qu'ils génèrent, en vue de l'utilisation de ces données dans l'intérêt public. Le législateur épingle parmi les objectifs d'intérêt public la recherche scientifique dans l'intérêt général. La mise à disposition doit en outre se faire sans contrepartie[101].

À titre d'exemple de ce type d'altruisme, on peut évoquer le partage volontaire de données relatives à la protection de l'environnement qui pourrait permettre d'identifier les actions prioritaires à entreprendre pour faire face à la déforestation, à la perte de biodiversité ou à la gestion des déchets dangereux[102]. L'altruisme pourrait aussi conduire des entreprises à partager leurs informations sur la qualité de l'air et sur les rejets de matières polluantes, ou les agriculteurs adeptes du « *smart farming* » à partager les données récoltées via divers capteurs (stations météorologiques, capteurs d'humidité, scanners de sol, capteurs de culture, *etc.*)[103]. La plateforme *Smart Citizen* illustre bien à quoi peut conduire l'« altruisme des données » : cette plateforme permet le partage par les citoyens des données sur les niveaux de bruit et de pollution dans leur maison, collectées par le biais de capteurs. Le rassemblement de ces données permet aux chercheurs de cartographier le bruit et la qualité de l'air. L'app allemande *Corona-Datenspende-App*, quant à elle, a collecté durant la pandémie du COVID-19 des données (fréquence cardiaque, température corporelle, pression artérielle, habitudes de sommeil) à partir de bracelets de fitness et de montres intelligentes. Grâce à l'analyse de ces données, les chercheurs ont pu identifier à un stade précoce les points chauds possibles du COVID-19.

Aux termes de l'article 16 du règlement, le législateur européen incite les États membres à élaborer des politiques nationales concernant l'altruisme en matière de données. Toute entité engagée dans cet altruisme doit pouvoir demander à être enregistrée comme « organisation altruiste en matière de données reconnue dans l'Union » dans un registre commun tenu par la Commission européenne[104]. Les conditions pour figurer dans ce registre sont toutefois plutôt strictes[105]. Il doit s'agir d'entités publiques ou privées à but non lucratif qui poursuivent un objectif d'intérêt général et qui agissent par le biais d'une

100 Article 2, 16° DGA (c'est nous qui soulignons).
101 Sans contrepartie sauf la compensation des coûts de la mise à disposition de leurs données (article 2, 16° DGA).
102 CE, Une stratégie, p. 26-27 ; TOMBAL, Data sharing, N 4.
103 Human Technology Foundation/L'Exploratoire Sopra Steria Next, p. 29-34 ; TOMBAL, Data sharing, N 4 ; Everis Benelux, p. 43.
104 Article 19 DGA. Voir ég. TOMBAL, Data sharing, N 7.
105 TOMBAL, Data sharing, N 6.

structure juridiquement indépendante et fonctionnellement distincte[106]. L'organisation altruiste en matière de données ne peut utiliser les données pour des objectifs autres que ceux d'intérêt général pour lesquels la personne concernée ou le détenteur des données ont autorisé le traitement[107].

Selon l'analyse très pertinente de Thomas TOMBAL, le mécanisme d'« altruisme des données », du fait de sa nature purement volontaire, devra tenir compte de trois défis pour parvenir à se développer. « *Premièrement, il ne fonctionnera que si sa mise en œuvre concrète génère une confiance entre tous les acteurs concernés et si leurs craintes quant à l'utilisation abusive des données (par les concurrents) sont apaisées, ce qui n'est pas acquis à la lumière de scandales tels que celui de Cambridge Analytica. Deuxièmement, les motivations (non financières) des personnes concernées, des détenteurs de données, des réutilisateurs de données et des organisations altruistes en matière de données à s'engager dans un tel mécanisme devront être identifiées et encouragées. Troisièmement, les organisations altruistes en matière de données devront créer des mécanismes de financement pour assurer leur pérennité tout en restant (financièrement) indépendants* »[108].

D. Création des Espaces européens communs de données

À l'origine du texte du règlement et dans le contexte de la Stratégie européenne pour les données, la Commission européenne a plaidé en faveur de la libre circulation sécurisée des données avec les pays tiers, sous réserve des exceptions et des restrictions en matière de sécurité publique, d'ordre public et d'autres intérêts légitimes.[109]

« *Afin que cette vision devienne réalité* »[110], c'est-à-dire en vue de réaliser cette libre circulation des données au-delà des frontières, un ensemble de domaines ou de thématiques ont été identifiés pour lesquels des Espaces européens communs de données ont été ou seront mis en place par la Commission européenne, permettant le partage et la mise en commun de données[111].

Ainsi, dans un premier temps, les dix domaines ou thématiques stratégiques suivants ont été proposés : la santé, l'agriculture, l'industrie manufacturière,

106 Article 18 DGA.
107 Article 21, § 2 DGA.
108 TOMBAL, Data sharing, N 8.
109 Consid. 2 DGA.
110 Consid. 2 DGA.
111 Voir pour une explication du concept d'espace européen commun de données et des règles de fonctionnement de ces espaces, ainsi que pour la présentation d'un inventaire des espaces européens communs de données, Commission Staff Working Document on Common European Data Spaces, 23 février 2022, SWD(2022) 45 final.

l'énergie, la mobilité, les services financiers, l'administration publique, les compétences, la science ouverte et le pacte vert. Deux autres domaines ont déjà été ajoutés : les médias et le patrimoine culturel. L'objectif final est que les espaces de données forment ensemble un espace européen (UE) unique des données.

Les espaces européens communs de données visent à rendre les données qu'ils hébergent traçables, accessibles, interopérables et réutilisables, c'est-à-dire répondant aux principes FAIR pour les données. Ils doivent par ailleurs garantir un niveau élevé de cybersécurité[112].

IV. La proposition de règlement sur les données (*Data Act*)

Le législateur européen poursuit son action en vue de permettre toujours davantage d'accéder à et de réutiliser les données, dans un but semblable à celui déjà avancé pour les deux textes précédemment analysés, de « *stimul*[er] *le développement d'un marché des données concurrentiel*, [d'] *ouvr*[ir] *des perspectives pour l'innovation fondée sur les données et* [de] *rendr*[e] *les données plus accessibles à tous* »[113]. Les nouvelles règles en préparation sont appelées à augmenter drastiquement le volume de données disponibles en vue de leur réutilisation. Après les données détenues par le secteur public et par les entreprises publiques, les données couvertes par des obligations de secret ou d'accès restreint, et les données spontanément partagées, la Commission européenne s'attaque cette fois à deux nouveaux types de données : les données générées par l'utilisation des dispositifs et objets connectés ; et les données détenues par le secteur privé qui sont nécessaires pour faire face à des circonstances exceptionnelles[114].

La proposition de règlement sur les données[115] vise à régler les problèmes juridiques, économiques et techniques à l'origine de ce que les auteurs du texte percevaient comme une grave sous-utilisation des données visées. Loin de la philosophie d'altruisme en matière de données qui imprégnait le DGA, laissant aux détenteurs de données la liberté d'opter pour le partage de celles-ci, le règlement sur les données entend mettre en place une obligation de partage[116].

112 Consid. 2 DGA.
113 CE, Communiqué de presse.
114 Voir les réflexions à la base de la volonté de développer un partage de données B2G pour répondre à un intérêt public : High-Level Expert Group on Business-to-Government Data Sharing.
115 Proposition de Règlement sur les données.
116 Sur l'impact que ce texte en projet pourrait avoir pour la Suisse, voir DETEC/DFAE/DFF/DEFR, p. 17-18.

A. Données générées par l'utilisation de dispositifs et objets connectés (*Internet of Thing data*)

À la différence de l'achat d'un bien ou d'un produit « traditionnel » pour lequel on devient propriétaire de toutes les pièces et accessoires dès qu'on a acquis le bien en question, l'achat d'un produit connecté, comme une voiture ou un appareil domestique intelligent, dont l'usage génère de multiples données, conduit la plupart du temps au recueil de ces données exclusivement par le fabriquant du produit. Il est en outre souvent difficile de savoir qui peut faire quoi avec ces données. La proposition de règlement répond à ces deux situations problématiques en prévoyant un droit d'accès gratuit de l'utilisateur aux données et une obligation de transparence à son égard[117].

Ainsi, le règlement sur les données[118] imposera, lorsqu'il sera adopté, que les données générées au moyen d'objets, de machines ou d'appareils intelligents soient directement accessibles (par défaut) à l'utilisateur du dispositif connecté et que leur accès ne soit pas limité au fabricant. L'utilisateur pourra demander que les données relatives à son usage du produit ou dispositif connecté soient transmises à un tiers (droit à la portabilité)[119] ou les lui transmettre lui-même.

Il est à noter que ces règles et obligations contenues dans le projet de règlement s'appliqueront également à toute entreprise établie dans un État hors UE mais active sur le marché intérieur de l'Union. En effet, le texte devrait s'appliquer « *à tous les fournisseurs, qui offrent des produits, des services ou des données à des clients dans les États membres, ou qui reçoivent des données, indépendamment du lieu de leur établissement* »[120].

Cette portabilité des données générées par l'utilisation de dispositifs ou d'objets connectés, qui vise en premier lieu à empêcher la mainmise monopolistique sur les données par les fabricants, dans le but de favoriser le développement de services concurrents notamment de services de réparation et d'entretien[121], permettra éventuellement aussi d'alimenter des recherches, surtout si les données sont agrégées à partir de plusieurs utilisateurs. Ainsi, par exemple, les données

---

117 Voir article 3 de la proposition de règlement sur les données.

118 Voir article 4 de la proposition de règlement sur les données.

119 Voir article 5 de la proposition de règlement sur les données. Le droit à la portabilité envisagé ici viendrait en complément de l'article 20 du RGPD qui établit un droit à la portabilité des données à caractère personnel pour les personnes concernées (personnes physiques). « *Ce droit au partage des données aurait une portée beaucoup plus large que le droit à la portabilité prévu par le RGPD, puisqu'il serait accordé aux particuliers comme aux entreprises et couvrirait les données personnelles et non personnelles*. » (MADIEGA).

120 DETEC/DFAE/DFF/DEFR, p. 18.

121 Thomas TOMBAL voit dans cette portabilité spécifique un « *embryon de partage de données B2B à des fins de durabilité* » (TOMBAL, N 29 ss. C'est nous qui traduisons)

émanant de certains véhicules connectés pourraient être rassemblées dans les mains d'organismes de recherche pour contribuer aux recherches sur la circulation routière ou en matière d'accidentologie.

Le texte en projet[122] prévoit que le tiers sélectionné par l'utilisateur pour recevoir l'accès à ou la transmission des données devrait indemniser le fabricant pour les coûts liés à l'accès aux données qu'il lui octroie, c'est-à-dire aux dispositions techniques permettant de mettre les données à disposition, telles que les interfaces de programmation d'applications (API).

B. Obligation de mettre les données à disposition en raison d'un besoin exceptionnel

Le règlement sur les données en projet vise à obliger les entreprises privées à mettre leurs données à disposition du secteur public dans des situations exceptionnelles d'intérêt public élevé[123]. Aux termes de l'article 14 de ce texte, intitulé « *Obligation de mettre les données à disposition en raison d'un besoin exceptionnel* », « [s]*ur demande, un détenteur de données met des données à la disposition d'un organisme du secteur public ou d'une institution, d'un organe ou d'un organisme de l'Union démontrant l'existence d'un besoin exceptionnel d'utiliser les données demandées*. ». Cette disposition précise en outre qu'elle ne s'applique pas aux petites et microentreprises[124].

La proposition de règlement oblige donc les détenteurs de données à mettre les données qu'ils détiennent à la disposition du secteur public sur demande dans trois scénarios dans lesquels un « besoin exceptionnel d'utiliser les données » peut être établi. Signalons d'emblée que la notion de « besoin exceptionnel » n'est pas définie dans le projet de règlement[125] qui se contente d'en donner pour exemples la santé, le climat et les incidents graves de cybersécurité[126]. La protection de l'environnement, à tout le moins la lutte contre la dégradation de celui-ci à un point pouvant impacter gravement les conditions de vie, mériterait de figurer dans le texte final du règlement[127].

122 Voir. article 9 proposition de règlement sur les données.

123 Pour une analyse de la question du partage obligatoire de données B2G, voir TOMBAL, Business-to-government, p. 9-10 ; TOMBAL, Data sharing, N 14 à 25 ; COLANGELO, p. 22-23.

124 Pour une critique de cette exclusion, voir DREXL *et al*., p. 49.

125 Certains auteurs déplorent l'approche trop abstraite du « besoin exceptionnel » dans la proposition de règlement : COLANGELO, p. 22 ; TOMBAL, Data sharing, N 16.

126 Considé. 60 proposition de règlement sur les données. Voir KNOCKKAERT/MICHEL, p. 95.

127 TOMBAL, Data sharing, N 16.

Dans le premier scénario, un besoin exceptionnel est réputé exister quand les données demandées sont nécessaires pour *réagir* face à une urgence publique[128]. Dans le second scénario, il y a un besoin exceptionnel lorsque les données sont nécessaires pour *prévenir* une urgence publique ou pour *rétablir* la situation après une urgence publique (dans ce cas, la demande de données doit avoir une durée et une portée limitées)[129]. Enfin, dans un troisième scénario, on admet le besoin exceptionnel si l'absence de données empêche l'organisme public de s'acquitter d'une mission d'intérêt public explicitement prévue par la loi et s'il n'est pas possible d'obtenir les données autrement (via le marché) ou en temps utiles (via la loi) ou si cette voie de la réquisition des données réduit substantiellement la charge administrative pesant sur les détenteurs de données[130].

Dès lors que les données sont nécessaires pour répondre à une urgence publique, elles devront être fournies sans délai et gratuitement. Dans d'autres situations – pour prévenir ou surmonter une urgence publique, ou pour remplir une mission d'intérêt public imposée par la loi – le détenteur des données peut demander une compensation financière couvrant les coûts liés à la mise à disposition des données pertinentes, augmentés d'une marge raisonnable[131].

Ce mécanisme de réquisition possible de données entre les mains de détenteurs privés peut présenter un intérêt pour des activités de recherche. En effet, l'article 21 du projet de règlement prévoit une possibilité de réutilisation pour des finalités scientifiques et statistiques des données obtenues. Selon cette disposition, un organisme du secteur public ou une institution ayant reçu l'accès à des données pour répondre à un besoin exceptionnel a le droit de partager les données reçues avec des particuliers ou des organismes en vue de mener des travaux de recherche scientifique ou des analyses compatibles avec la finalité pour laquelle les données ont été demandées. Les particuliers ou les organismes à qui les données sont transmises doivent agir dans un but non lucratif ou dans le cadre d'une mission d'intérêt public qui leur a été confiée. Les organismes sur lesquels des entreprises commerciales ont une influence déterminante ne peuvent bénéficier de cette possibilité de recevoir des données par cette voie, dans la mesure où cela pourrait conduire à donner à ces entreprises un accès préférentiel aux résultats des recherches.

---

128 Article 15 (a) proposition de règlement sur les données. L'urgence publique est définie à l'article 2 (10) comme : « *une situation exceptionnelle ayant une incidence négative sur la population de l'Union, d'un État membre ou d'une partie de celui-ci, entraînant un risque de répercussions graves et durables sur les conditions de vie ou la stabilité économique, ou la détérioration substantielle d'actifs économiques dans l'Union ou les États membres concernés*. »

129 Article 15 (b) proposition de règlement sur les données.

130 Article 15 (c) proposition de règlement sur les données.

131 Article 20 proposition de règlement sur les données.

V. Conclusion

En développant sa Stratégie pour les données, l'Union européenne a placé les données personnelles et non personnelles au cœur de son action, déterminée à jouer un rôle de premier plan dans une « société fondée sur les données »[132]. Les mesures réglementaires prises ou encore en voie d'élaboration dans le cadre de cette Stratégie visent à « libérer le potentiel économique et sociétal des données »[133]. Si cette action de l'UE est inévitablement axée sur le poids des données dans le développement économique, c'est donc aussi l'impact sociétal des données qui est pris en compte. À ce titre, la recherche scientifique figure au premier rang des domaines appelés à bénéficier des actions législatives de l'Union en matière de données.

Consciente que « [l]*a valeur des données tient à leur utilisation et réutilisation* »[134], la Commission européenne a veillé à favoriser considérablement la disponibilité des données pour le bien public. « *Les données générées par le secteur public […] devraient être disponibles pour le bien commun en faisant en sorte, par le recours à un accès préférentiel, que ces données soient utilisées par des chercheurs* […]. *Les données provenant du secteur privé peuvent également apporter une contribution significative au bien public*. »[135]. L'action du législateur européen s'est en conséquence portée sur l'incitation au partage de données, volontaire ou obligatoire, en vue de permettre la réutilisation des données.

Trois textes législatifs donnent forme à cette incitation au partage : la directive *Open Data* de 2019, le règlement sur la gouvernance des données (le DGA) de 2022 et le dernier texte encore en voie d'élaboration et d'adoption par le Parlement européen et le Conseil, le règlement sur les données (le *Data Act*). Ces textes sont particulièrement favorables à la mise à disposition d'un ensemble colossal de données au bénéfice de la recherche, et singulièrement de la recherche dans l'intérêt général. Ainsi, les données détenues par les organismes du secteur public, celles dans les mains de certaines entreprises publiques, les données de la recherche détenues par des organismes de recherche financés sur fonds publics, les ensembles de données de forte valeur, les données dynamiques, les données couvertes par des obligations de secret ou d'accès restreint mais ouvertes à la réutilisation sous conditions, les données spontanément partagées par leurs détenteurs, les données générées par l'utilisation des dispositifs et objets connectés (l'*Internet of Things*) et communiquées par les utilisateurs et les données transmises par le secteur privé aux organismes publics pour faire

132 CE, Communiqué de presse.
133 CE, Communiqué de presse.
134 CE, Stratégie, p. 7.
135 CE, Stratégie, p. 8.

face à des besoins exceptionnels, toute cette fabuleuse manne informationnelle est désormais disponible pour les chercheurs de l'intérieur ou de l'extérieur de l'Union européenne, ou le sera dans un futur proche.

Cela dit, cette évolution législative suscite une dernière réflexion.

Une partie des données citées dans les lignes qui précèdent ne seront partagées que si leurs détenteurs y consentent ou en prennent l'initiative. Or, le passé a montré que pour que la directive sur la réutilisation des données du secteur public de 2003 ait véritablement de l'effet, il a fallu passer – en 2013 – de l'invitation à favoriser l'ouverture des ressources informationnelles du secteur public à l'obligation de la réaliser. L'écoulement d'une décennie avait permis de voir qu'il ne fallait pas trop compter sur une action spontanée des acteurs publics. La version réécrite en 2019 de cette directive, si elle reprend l'obligation de partage des données pour les organismes du secteur public, ne prévoit par ailleurs qu'une simple incitation à l'ouverture pour les entreprises publiques, les bibliothèques, les musées et les archives. De la même façon, le DGA ne fait qu'inviter à l'« altruisme des données » les acteurs publics ou privés. Il n'est pas dit que ces détenteurs de données seront davantage motivés que les acteurs de la décennie précédente pour mettre leurs données à disposition d'autrui. Là où les chances d'y assister sont les plus grandes et réalistes est sans doute lorsque le partage poursuit un objectif de recherche et se fait au bénéfice du monde scientifique œuvrant à l'intérêt général. On sera donc attentif dans les années qui viennent à mesurer l'efficacité des textes européens sur ce point, en assistant, on l'espère, au déploiement d'un véritable partenariat altruiste donnant vie aux rêves contenus dans la directive *Open data* et le DGA.

Quant aux obligations (et non plus seulement incitations) de partage, prévues dans la directive et dans le futur *Data Act*, elles ne profiteront au bien commun que si la société – au sein de l'Union européenne et en-dehors – saisit les occasions qui lui sont offertes d'exploiter le potentiel des données mises à disposition. À présent que l'encadrement juridique de cette mise à disposition est en place ou en passe de l'être incessamment, le défi se situe désormais sur le plan de la communication à propos de ces ressources. Les chercheurs mais aussi les acteurs de la société et du marché doivent prendre conscience des trésors informationnels qui leur sont accessibles.

VI. Bibliographie

A. Littérature/Doctrine

Giuseppe Colangelo, European Proposal for a Data Act: A First Assessment, CERRE Assessment Paper, 2022 disponible : <https://cerre.eu/wp-content/uploads/2022/07/200722_CERRE_Assessment-Paper_DataAct.pdf> ; **Cécile de Terwangne**, Réutilisation des informations du secteur public : la directive 2003/98 enfin totalement transposée en droit belge, Revue du Droit des Technologies de l'Information nº 32, 2008, p. 142 ss ; **Josef Drexl/Carolina Banda/Begoña Gonzalez Otero/Jörg Hoffmann/Daria Kim/Shraddha Kulhari/Valentina Moscon/Heike Richter/Klaus Wiedemann**, Position Statement of the Max Planck Institute for Innovation and Competition on the Commission's Data Act Proposal, 2020 disponible : <https://www.researchgate.net/publication/361400603_Position_Statement_of_the_Max_Planck_Institute_for_Innovation_and_Competition_of_25_May_2022_on_the_Commission%27s_Proposal_of_23_February_2022_for_a_Regulation_on_Harmonised_Rules_on_Fair_Access_to_and> (cité : Drexl *et al.*) ; **Everis Benelux**, Study on data sharing between companies in Europe – Case studies, Study for the European Commission, 2018, disponible : <https://publications.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en> ; **Loïc Gerard**, Réutilisation des données du secteur public : la transposition de la Directive 2013/37/UE par la loi du 4 mai 2016, A&M nº 4, 2016, p. 320 ss ; **High-Level Expert Group on Business-to-Government Data Sharing**, Towards a European strategy on business-to-government data sharing for public interests – Final report, 2020, disponible : <https://ec.europa.eu/digital-single-market/en/news/experts-say-privately-held-data-available-european-union-should-be-used-better-and-more> ; **Human Technology Foundation/L'Exploratoire Sopra Steria Next**, Le data altruisme : Les données au service de l'intérêt général, disponible : <https://www.soprasteria.fr/docs/librariesprovider2/sopra-steria-fr-documents/notindexdocuments/rapport-htf---sopra-steria-next---data-altruisme_version-digitale.pdf?Status=Master&sfvrsn=bfc6c6dc_15> ; **Caroline Ker**, Réutilisation des informations du secteur public : la transposition de la directive 2013/37/UE, Revue du Droit des Technologies de l'Information, 2016, p. 62 ss ; **Manon Knockaert**, La réutilisation des informations du secteur public : l'open data et les organismes publics, JT nº 6739, 2018, p. 613-621 ; **Manon Knockaert/Alejandra Michel**, La Directive (UE) 2019/1024 et la réutilisation des informations du secteur public : un pas de plus vers un espace européen commun des données, R.T.D.Eur., 2023, p. 71-95 (cité : Knockaert/Michel, La directive) ; **Manon Knockaert/Alejandra Michel**, Le cadre européen de l'information environnementale, *in* Hervé Jacquemin/Amélie Lachapelle (éds), Numérique et développement durable : obstacles et opportunités pour le droit, Bruxelles, 2023, p. 219-254 ; **Tambiama Madiega**, European Parliamentary Research Service, Briefing EU Legislation in Progress, The data act, 2022, disponible : <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733681/EPRS_BRI(2022)733681_EN.pdf> ; **Johan Pas/Bruno De Vuyst**, Re-Establishing the Balance between the Public and the Private Sector: Regulating Public Sector Information Commercialization in Europe, Journal of Information Law and Technlogy (JILT), 2004, disponible : <http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_2/pasanddevuyst/> ; **Nathalie Poupaert/Kathleen Janssen**, « La directive du 17 novembre 2003 concernant la réutilisation des informations du secteur public », Revue du Droit des Technologies de l'Information nº 19, 2004, p. 29-50 ; **Agnès Robin**, Droit des données de la recherche. Science ouverte, innovation, données publiques, Collection Création Information Communication, Bruxelles, 2022 ;

Thomas TOMBAL, Data sharing by private actors as an avenue for more sustainability, *in* Hervé JACQUEMIN/Amélie LACHAPELLE (éds), Numérique et développement durable : obstacles et opportunités pour le droit, Bruxelles, 2023, p. 219-254 (cité : TOMBAL, Data sharing) ; **Thomas TOMBAL**, Business-to-Government data sharing for environmental purposes, Network Industries Quarterly, 24(3), p. 7-11, disponible à : <https://www.network-industries.org/wp-content/uploads/2022/10/Business-to-government-data-sharing-for-environmental.pdf> (cité : TOMBAL, Business-to-government) ; **Thomas TOMBAL**, *Imposing Data Sharing Among Private Actors: A Tale of Evolving Balances*, Alphen aan den Rijn, Wolters Kluwer, Innovation Law Series nº 48, 2022 ; **Thomas TOMBAL**, The rationale for compulsory B2B data sharing and its underlying balancing exercises, Revue du Droit des Technologies de l'Information nº 84, 2021, p. 5-26.

B. Documents officiels

Commission européenne, Communiqué de presse, Règlement sur les données : la Commission propose des mesures en faveur d'une économie des données équitable et innovante, 2022 (cité : CE, Communiqué de presse) ; **Commission européenne**, Staff Working Document on Common European Data Spaces, 23 février 2022, SWD(2022) 45 final ; **Commission européenne**, Une stratégie européenne pour les données, COM(2020)66 final, 2020 (cité : CE, Une stratégie) ; **Commission européenne**, Executive Summary of the Impact Assessment Report accompanying the Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), SW(2020)296 final, 2020 (cité : CE, Executive summary) ; **Commission européenne**, Bâtir l'avenir numérique de l'Europe, disponible à : <https://digital-strategy.ec.europa.eu/fr/policies/data> (cité : CE, Bâtir l'avenir) ; **Commission européenne**, Recommandation (UE) 2018/790 du 25 avril 2018 relative à l'accès aux informations scientifiques et à leur conservation, JO L 134/12, 31 mai 2018, p. 1 ss (cité : CE, recommandation 2018/790) ; **Commission européenne**, Communication au Conseil, au Parlement européen, au Comité économique et social et au Congrès des régions, « Vers un espace européen de la recherche », COM(2000)6 final, 2000 ; **DETEC/DFAE/DFF/DEFR**, La Suisse et la stratégie numérique de l'Union européenne 2023, disponible : <https://www.eda.admin.ch/missions/mission-eu-brussels/fr/home/dossiers-prioritaires/digital.html> ; **European Commission**, Directorate-General for Communications Networks, Content and Technology (2018), Scaria, E., Berghmans, A., Pont, M. et al., Study on data sharing between companies in Europe – Final report, Publications Office, disponible à : <https://data.europa.eu/doi/10.2759/354943> ; **Parlement européen**, Communiqué de presse, Data Act : MEPs back new rules for fair access and use of industrial data, 2023.