Collection lausannoise
CEDIDAC

Sylvain Métille
(éditeur)

L'informatique en nuage

Stämpfli Editions

Sommaire

© Stämpfli Editions SA Berne

Cloud et territoire

SUZANNE VERGNOLLE
Docteure en droit, Maître de conférences au Conservatoire national des arts et métiers (Cnam)

Table des matières

© Stämpfli Editions SA Berne

I. Introduction

A. Observations générales

« *N'oublie pas que chaque nuage, si noir soit-il, a toujours une face ensoleillée, tournée vers le ciel*. » Cette incitation à la réflexion proposée par Friedrich Wilhelm Weber nous rappelle que toute perception est une question de point de vue. En fonction de la perspective, chacun y voit ce qu'il veut y voir, ignorant parfois qu'une autre position, donc une autre perspective, est possible.

Les nuages informatiques sont-ils si différents des nuages météorologiques ? Après tout, ils présentent bel et bien certaines caractéristiques communes : ils peuvent être larges ou petits, attendus ou redoutés, proches ou lointains. Parfois, ils entraînent la foudre et lorsqu'elle frappe, par son électricité ou par une cyberattaque, les humains sont souvent dévastés !

En droit, l'apparente volatilité du nuage informatique a parfois généré quelques doutes ou incompréhensions sur les enjeux territoriaux liés à cette technologie. Fort heureusement, les informaticiens n'ont pas manqué de rappeler aux juristes que : « *there is no cloud, it's just someone else's computer* », soulignant ainsi le principe de matérialité et de territorialité de l'infrastructure technique existante derrière le *cloud*.

B. Le « *Cloud* » : brèves observations conceptuelles

L'informatique en nuage, équivalent français de *cloud* ou *cloud computing*, fait référence à « *l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau* »[1]. En d'autres termes, le *cloud* est une infrastructure informatique virtualisée fournissant des services que les utilisateurs peuvent exploiter depuis n'importe quel lieu du monde. Le *cloud* repose donc fondamentalement sur une délocalisation des traitements ainsi que sur une externalisation des compétences[2]. En confiant leurs données ou leurs infrastructures à des entreprises plus compétentes et expertes qu'elles, les clients peuvent alors mieux se concentrer sur leurs propres services. C'est ce qui explique la variété des offres de *cloud computing* parmi lesquelles figurent trois modèles de services (SaaS[3], PaaS[4],

1 CNIL, site Internet, page « Définition de Cloud Computing ».
2 MONTAVON, p. 459.
3 *Software as a Service*, pouvant être traduit par « logiciel à la demande ».
4 *Platform as a Service,* pouvant être traduit par « plateforme-service ».

© Stämpfli Editions SA Berne

IaaS[5]) et trois modèles de déploiement (public, privé, hybride)[6]. Le choix du modèle dépend des besoins du client, notamment en termes d'architecture informatique, de gouvernance, et de gestion des risques.

En pratique, le *cloud* présente de nombreux avantages. D'abord, il offre une meilleure utilisation des ressources, particulièrement avec le déploiement des *clusters*, lesquels adaptent l'infrastructure utilisée en fonction des besoins du client. Cette meilleure utilisation des ressources techniques se transforme souvent en économies financières : non seulement des économies d'échelle sont réalisées mais surtout, seuls les services utilisés par le client sont facturés. Ensuite, les infrastructures de *cloud* de bonne qualité présentent souvent un meilleur niveau de sécurité que celui existant dans les infrastructures autonomes. En externalisant leurs besoins à des fournisseurs de confiance, les petites et moyennes entreprises bénéficient de technologies de meilleur niveau que celles qu'elles pourraient développer en interne. De plus, les organisations se déchargent des tâches de maintenance et de mise à jour des systèmes informatiques, et bénéficient des certifications réglementaires détenues par leurs fournisseurs. Enfin, le *cloud* offre également une plus grande mobilité pour le client puisque les données sont accessibles depuis n'importe quelle machine connectée au réseau.

Ces avantages ne doivent pas cacher les risques liés à l'usage de cette technologie, tels que la perte de contrôle ou de données, le manque d'isolation entre les données, les pannes du système et du réseau…[7] Surtout, dès lors que l'usage est délocalisé, il n'est pas certain que les serveurs du fournisseur de *cloud* se situent sur le même territoire que leurs clients. Des problèmes d'application territoriale du droit peuvent alors surgir. Le territoire et le droit entretiennent en effet des liens profonds et anciens.

C. Le territoire : fondement de la souveraineté de l'État

La notion de « territoire » de l'État s'est progressivement séparée de l'idée de « possession du sol » par le seigneur qui a longtemps prévalu pendant le Moyen Âge[8]. À partir du XVI[e] siècle, le territoire va apparaître comme l'un des fondements essentiels de l'État, notamment avec les Traités de Westphalie signés en 1648. La notion de territoire devient alors la pierre angulaire du droit international.

5 *Infrastructure as a Service*, pouvant être traduit par « infrastructure à la demande ».
6 GREVET, p. 10 s.
7 PFPDT, Explications.
8 CARREAU/MARRELLA, p. 52.

© Stämpfli Editions SA Berne

Le territoire marque les limites géographiques où s'exerce exclusivement l'autorité, c'est-à-dire la compétence de l'État. En dehors de ces limites, l'État n'a pas de compétence et il ne peut donc pas légitimement intervenir. Ce principe est rappelé par de nombreuses règles, notamment l'article 3 alinéa 1 du Code pénal suisse, lequel limite son applicabilité « *à quiconque commet un crime ou un délit en Suisse* ». Bien sûr, des exceptions existent afin de garantir la cohérence et l'utilité de ce principe, mais les frontières du territoire caractérisent bel et bien la compétence étatique de principe[9].

La notion de territoire est souvent rapprochée de celle de souveraineté. Cette dernière est classiquement définie comme la capacité des États à imposer des règles sur leur territoire et à interagir avec leurs pairs. Cela signifie non seulement que la compétence de l'État sur son territoire est pleine et exclusive, mais aussi qu'il n'existe pas de subordination d'un État par rapport aux autres[10]. Les limites de la souveraineté d'un État ainsi que sa capacité à édicter des règles juridiques, sont donc largement liées aux démarcations territoriales. Les caractéristiques du *cloud* rendent parfois complexe l'appréhension de la compétence territoriale ainsi que son application.

D. Le *cloud* et le territoire : quelles interactions ?

Puisque le *cloud* est un outil reposant principalement sur Internet, il n'est pas inutile de rappeler la caractéristique principale de ce dernier : il s'agit d'un ensemble de réseaux sans délimitation territoriale[11]. En étant accessible partout dans le monde, Internet a largement contribué à redéfinir l'application territoriale des règles juridiques ainsi que la compétence juridictionnelle.

Pourtant, en dépit de son apparente volatilité et de son absence de rattachement territorial, Internet repose bel et bien sur des infrastructures techniques et matérielles. Les menaces pesant sur la rupture des câbles sous-marins ainsi que les enjeux écologiques liés aux fermes de serveurs en sont des témoins. Il en va de même pour le *cloud.* Les interruptions de services de l'entreprise *Amazon Web Services* (AWS) en 2017 avaient en effet entraîné de fortes perturbations sur de nombreux services et sites marchands et mis en évidence la réalité matérielle existante derrière le *cloud*.

De nombreux enjeux de compétences découlent de l'utilisation du *cloud.* Par exemple, comment déterminer le droit applicable aux données d'une entreprise suisse, dont l'informatique est gérée depuis la France, avec des serveurs *cloud* situés en Belgique, disposant d'une infrastructure de secours aux États-Unis ?

9 MÜLLER, p. 307.
10 KRANZ, p. 413 ss.
11 GOLDSMITH, p. 475 ; SCHERRER, p. 474.

© Stämpfli Editions SA Berne

Est-ce uniquement le droit suisse ? Probablement pas. Seulement un autre des droits des États impliqués ? Non plus. En réalité, le droit applicable à ces données est certainement un assemblage des différentes règles juridiques des pays offrant un rattachement plus ou moins direct avec les différents acteurs. Le juriste doit alors effectuer une vérification minutieuse de la compatibilité de ces règles entre elles afin de s'assurer de leur cohérence ainsi que de la conformité de son organisation aux règles nationales. La question de la conformité est d'autant plus importante lorsque les données envoyées et conservées dans le *cloud* sont des données personnelles[12]. Dans ce cas, aux principes juridiques d'ores et déjà applicables au *cloud* tels que ceux relatifs aux obligations liées à la coopération pénale s'ajoute également la réglementation spéciale du droit des données personnelles, menant à des vérifications techniques et juridiques ainsi qu'à l'insertion de dispositions contractuelles impératives[13].

L'objectif de la présente contribution n'est pas de proposer une réponse juridique exhaustive en lien avec une situation particulière. Il est plutôt d'ébaucher quelques-unes des principales problématiques en lien avec le *cloud* et le territoire. À cet effet, il sera proposé d'étudier les interactions entre ces deux thèmes, mais aussi d'élargir les perspectives à d'autres sujets liés, tels que ceux de souveraineté ou d'extraterritorialité. Pour ce faire, il s'agit, dans un premier temps, de s'intéresser aux enjeux liés au *cloud* dans le territoire (II.) pour ensuite voir, dans un second temps, les enjeux liés au *cloud* au-delà du territoire (III.).

II. Le *cloud* dans le territoire

A. Observations introductives

L'espoir d'un développement numérique ouvert et décentralisé offrant un renouvellement des modes de gouvernance et de répartition des pouvoirs s'étiole progressivement pour laisser place à une centralisation croissante des services en ligne. Quelques multinationales américaines et chinoises se partagent aujourd'hui la majorité du « gâteau » numérique. Les enjeux de gouvernance liés à cette centralisation ne sont pas uniquement théoriques mais bel et bien politiques et géostratégiques. Depuis plusieurs années, la tendance actuelle des registres décentralisés (souvent dénommés « Web 3 ») cherche à prendre le contre-pied de cette centralisation. Par ailleurs, un nombre croissant d'États développent des stratégies favorables à une souveraineté dans l'environnement numérique (B). Certains États européens, dont la France et la Suisse, tentent

12 Sur les exigences de la protection des données, voir la contribution de FISCHER/PITTET dans cet ouvrage ; BOURGEOIS/MOINE.

13 ANCELLE/FERDJANI, p. 140.

© Stämpfli Editions SA Berne

ainsi de développer des *cloud* souverains (C), alors que d'autres États, tels que la Chine ou la Russie, ont imposé l'hébergement des données sur leur territoire aux opérateurs actifs dans leur juridiction (D).

B. L'aspiration à une « souveraineté numérique »

1. Observations introductives

L'expression « souveraineté numérique » renvoie à l'application des principes de souveraineté au domaine des technologies de l'information et de la communication. L'aspiration à une souveraineté numérique suppose de s'intéresser aux différents acteurs impliqués dans l'outil numérique : de la construction des composants électroniques, à la localisation des machines, en passant par les logiciels exécutés sur celles-ci, chacune de ces étapes génèrent des enjeux de souveraineté[14]. L'aspiration à une souveraineté numérique peut donc être générale (2) ou ciblée (3).

2. Une aspiration générale

Comme le remarquait le mathématicien et député français Cédric VILLANI dans un rapport sur l'intelligence artificielle, « *rien qu'en France, 80 % des visites vers les 25 sites les plus populaires sur un mois sont captés par les grandes plateformes américaine*s »[15]. Affinant ce constat, des sénateurs français relevaient que la situation géopolitique actuelle place l'Europe dans une situation délicate face à la prédominance des acteurs américains, parfois concurrencés par certains acteurs chinois[16]. Les sénateurs remarquaient d'ailleurs que le continent européen avait, jusqu'à présent, adopté une attitude plutôt défensive à l'égard de ces grands services en ciblant la défense de certaines valeurs, telles que la protection des données personnelles[17].

Face à ce constat, des voix s'élèvent de plus en plus fort pour encourager une vision plus ambitieuse de la souveraineté numérique et pour mettre en place des infrastructures numériques garantissant une véritable autonomie européenne[18]. D'autres voix n'hésitent pas à rappeler que les subventions publiques ne suffiront pas à poser les bases d'une souveraineté et que les causes du retard se trouvent dans des facteurs plus fondamentaux, tels que les visions sociales

14 FITZJEAN Ó COBHTHAIGH, p. 16.
15 VILLANI, p. 27.
16 MONTAUGE/LONGUET, p. 16.
17 *Ibid.*
18 Voir par exemple GHERNAOUTI/AGHROUM, p. 81.

© Stämpfli Editions SA Berne

et culturelles de la technologie et du numérique. Conciliant ces deux approches, le rapport sénatorial français[19] considère qu'une politique ambitieuse de souveraineté doit s'inscrire dans trois directions :

– *celle des infrastructures*, à savoir le déploiement sur le territoire européen ou national d'infrastructures numériques ;
– *celle politique,* c'est-à-dire le développement d'une politique industrielle identifiant les secteurs technologiques essentiels dans lesquels investir ; et enfin
– *celle des écosystèmes*, à savoir la mise en place de moyens humains et financiers favorisant l'émergence de virtuoses numériques européens.

Des stratégies générales et ambitieuses sont donc proposées par les États européens afin de stimuler le développement d'un modèle alternatif et souverain[20]. À ces stratégies générales s'ajoutent également certaines aspirations ciblées.

3. Des aspirations ciblées

Pour l'actuelle Présidente de la Commission européenne Ursula VON DER LEYEN, « *il est peut-être trop tard pour reproduire des géants du numérique, mais il n'est pas trop tard pour atteindre la souveraineté technologique dans certains secteurs technologiques critiques* »[21]. Ainsi, plutôt que de tenter d'imiter les succès passés, il faudrait faire des choix stratégiques pour garantir un futur technologique ambitieux et respectueux des valeurs européennes.

Selon cette approche, certains secteurs clés doivent être privilégiés, au rang desquels figurent les technologies liées à la « *blockchain, au calcul informatique de pointe, à l'informatique quantique, ainsi qu'aux algorithmes et aux outils permettant l'usage et le partage des données* »[22]. Il est assez clair que certaines de ces technologies entretiennent un lien avec le *cloud*.

Constatant que l'informatique en nuage se produit actuellement principalement dans certains grands centres de données, la Commission européenne compte sur une inversion de cette tendance d'ici 2025. Selon l'institution, 80 % des données devraient être traitées par des appareils intelligents plus proches de l'utilisateur, une tendance connue sous le nom de « *edge computing* ». Une telle

19 MONTAUGE/LONGUET, p. 119.
20 Ces stratégies incluent notamment le développement d'infrastructures souveraines telles que le *cloud* souverain ou de politiques publiques favorables aux nouveaux entrants sur le marché numérique telles que celles proposées dans le *Digital Markets Act*.
21 VON DER LEYEN, p. 13.
22 VON DER LEYEN, p. 13.

© Stämpfli Editions SA Berne

inversion offrirait des perspectives intéressantes en termes de souveraineté et permettrait sans doute des investissements stratégiques pour préparer l'avenir.

Ces stratégies technologiques sont complétées par une politique réglementaire effervescente. Des textes en lien avec le *cloud* tels que ceux liés à la circulation des données[23] ou à la cybersécurité[24] ont été rapidement adoptés, et de nombreux autres textes sont en cours de négociation.

La stratégie européenne est encore plus précise et ambitieuse en matière de *cloud* « souverain ».

C. Les tentatives de *Cloud* souverain

En tant qu'infrastructure, le *cloud* se révèle un outil essentiel de toute stratégie de souveraineté numérique. C'est pourquoi plusieurs pays tels que la France, la Suisse ou l'Allemagne ont pour ambition de développer des *cloud* dits souverains. Le *cloud* souverain est défini comme un modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur des données par un service de *cloud* sont physiquement réalisés dans les limites du territoire national par une entité de droit national et en application des lois et normes nationales[25]. Une telle définition surprend puisqu'il est désormais reconnu que le droit national s'applique non seulement aux entités de droit national mais aussi aux entités étrangères ayant un rattachement avec le territoire national. Par exemple, la loi fédérale sur les cartels prévoit explicitement qu'elle « *est applicable aux états de fait qui déploient leurs effets en Suisse, même s'ils se sont produits à l'étrange*r »[26]. L'article 3 al. 1 de la nouvelle Loi fédérale de protection des données (nLPD[27]) reprend ce principe de l'effet, en tant que concrétisation particulière du principe de territorialité[28]. Même si l'objectif du *cloud* souverain va bien au-delà d'une réponse purement juridique, il est regrettable de voir une mauvaise identification de l'un de ses enjeux principaux.

23 Règlement 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, JO L 303 du 28 novembre 2018, p. 59.

24 Règlement 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications, JO L 151 du 7 juin 2019, p. 15.

25 Ministères français de l'intérieur et de la culture, Note d'information du 5 avril 2016.

26 Article 2 de la loi fédérale du 6 octobre 1995 sur les cartels (LCart), RO 1996 546.

27 Loi fédérale du 25 septembre 2020 sur la protection des données (nLPD), FF 2020 7397.

28 ROSENTHAL/STUDER, p. 37.

© Stämpfli Editions SA Berne

D'autant que les acteurs nationaux, dès qu'ils ont un rayonnement à l'international, seront également soumis à des droits étrangers[29].

Plusieurs initiatives de *cloud* souverain essaiment en Europe. Elles sont les témoins de la volonté politique d'améliorer la souveraineté nationale en matière de données et de réduire au minimum la dépendance des pays aux prestataires internationaux de services en nuage publics[30]. Dès janvier 2010, le Premier ministre français regrettait que les entreprises nord-américaines « *dominent ce marché, qui constitue pourtant un enjeu absolument majeur* […] *pour la souveraineté de nos pays* »[31]. Son souhait était alors de développer « *un partenariat public-privé grâce aux fonds du programme pour les investissements d'avenir* ». Deux ans plus tard, l'État français investissait 150 millions d'euros dans deux projets de *cloud* (*Numergy* et *Cloudwatt*) qui ont peiné à atteindre leurs objectifs et à trouver leur public. Face à ces difficultés, *Numergy* fut placé en redressement judiciaire, puis fut racheté par *SFR* en 2016, et *Cloudwatt* a fermé ses portes en janvier 2020. Cet échec cuisant n'a pas découragé les représentants politiques qui ont continué d'insister sur la nécessité d'un *cloud* français ou européen en février 2020[32], lequel s'est matérialisé avec le projet *GAIA-X*. Initialement lancé autour de 22 entreprises françaises et allemandes, il associe, depuis novembre 2020, plus de 180 entreprises, notamment les grandes figures (étrangères) du *cloud*, telles *Alibaba*, *Amazon*, *Google*, *Microsoft*, et du logiciel, comme *Oracle*, *Palantir* ou *Salesforce*. D'importants problèmes de gouvernance au sein du projet ont été dénoncés par la société civile. D'ailleurs, en novembre 2021, l'entreprise française *Scaleway*, un des membres fondateurs de l'initiative, a annoncé son retrait en raison de la présence jugée trop importante des acteurs étrangers.

Si *GAIA-X* s'est récemment orienté vers un rassemblement des acteurs du *cloud* sous une même initiative, le rêve d'un *cloud* souverain persiste. La Conférence « Construire la souveraineté numérique de l'Europe » de février 2022 en est une preuve supplémentaire. Douze États membres de l'Union y ont manifesté leur volonté de contribuer au « *projet important d'intérêt européen commun (PIIEC), afin de renforcer nos investissements et notre autonomie stratégique en matière de cloud et d'edge computing* », avec un financement à hauteur de 7 milliards d'euros[33]. L'articulation entre *GAIA-X* et ce nouveau projet

29 Voir développements III, C.
30 Conseil fédéral, Communiqué du 16 avril 2020.
31 Premier ministre français, Discours du 18 janvier 2010.
32 Ministre de l'économie et Commissaire européen au marché intérieur, Déclarations du 7 février 2020.
33 Ministère français de l'Europe et des affaires étrangères, Ministère français de l'économie et Secrétariat d'État français chargé de la transition numérique, Communiqué conjoint du 7 février 2022.

© Stämpfli Editions SA Berne

n'apparaît pas très claire et des doutes subsistent quant à la bonne allocation des fonds publics dans ce domaine.

De son côté, le Conseil fédéral avait décidé de faire examiner, en avril 2020, « *la nécessité, la conception, l'utilité et la faisabilité d'un nuage informatique suisse (« Swiss Cloud »)* »[34]. Publié en décembre 2020, le rapport d'évaluation concluait que « *la nécessité d'un « Swiss Cloud » sous forme d'infrastructure de droit public et comme clé du succès de la place économique suisse n'est pas démontrée* », mais que « *la demande est forte concernant un label « Swiss Cloud » proposant un cadre adapté et des lignes directrices pour une utilisation compétente et sécurisée des services en nuage* »[35]. Sans plus attendre, la Confédération a publié quelques semaines plus tard un appel d'offres pour des services d'informatique en nuage d'une valeur de 110 millions de francs, lequel a fait l'objet d'importantes critiques de certains acteurs locaux l'ayant qualifié de contre-productif et excluant les firmes suisses[36]. Sans grande surprise, l'appel d'offres fut remporté par cinq géants du *cloud*, quatre américains (*Amazon*, *IBM*, *Microsoft* et *Oracle*) et un chinois (*Alibaba*). Toutefois, et de manière surprenante, *Google* ne faisait pas partie des acteurs américains sélectionnés. L'entreprise écartée avait intenté un recours qui fut rejeté par le Tribunal administratif fédéral[37]. Plusieurs concurrents suisses ont réitéré leurs critiques sur le choix de la Confédération et ont dénoncé le renforcement de la dépendance à l'égard des grands fournisseurs de *cloud* étrangers.

À ces projets de *cloud* souverains s'ajoutent également d'autres initiatives telles que celles liées aux lois imposant la localisation des données.

D. Les lois imposant la localisation des données sur leur territoire

Depuis le début des années 2010, plusieurs pays ont adopté des lois exigeant que certaines données (personnelles, commerciales, ou financières) soient collectées, traitées ou conservées sur leur territoire. Les mesures vont d'une simple obligation de conserver physiquement les données dans le pays d'origine à une restriction, voire à une prohibition, de les transférer vers des pays tiers. Parmi les États ayant adopté de telles lois figurent notamment la Chine, l'Inde, l'Indonésie, la Russie ou encore le Vietnam[38]. Les arguments

34 Conseil fédéral, Communiqué du 16 avril 2020.
35 Rapport « Swiss Cloud », décembre 2020, p. 30.
36 Office fédéral des constructions et de la logistique, Appel d'offre du 7 décembre 2020, nº 1136861.
37 TAF, arrêt B-3238/2021 du 18 octobre 2021.
38 CORY/DASCOLI, p. 27 s. ; CHANDER/LÊ, p. 682 s.

© Stämpfli Editions SA Berne

justifiant de telles obligations diffèrent en fonction des pays, mais se résument souvent à une prétendue meilleure sécurité ou protection des données, à une sauvegarde de la souveraineté nationale, ainsi qu'aux besoins d'accès par les enquêteurs dans le cadre d'enquêtes[39]. Si ces arguments sont parfaitement recevables et sont de nature à justifier une politique juridique imposant certaines limites en matière de circulation des données, ils peuvent aussi se révéler comme un miroir distordant d'objectifs politiques distincts. Certains de ces pays utilisent en effet ces lois pour permettre une surveillance de leurs citoyens et affaiblir les opinions politiques dissidentes.

Du fait de sa structure technique, le *cloud* se prête, en principe, plutôt mal aux obligations de localisation des données. En effet, les *clouds* sont accessibles depuis n'importe quel lieu et les serveurs peuvent être localisés dans le monde entier. Certaines obligations, telles que celles liées à la résilience, encouragent d'ailleurs les fournisseurs de *cloud* à effectuer des copies des données dans des serveurs situés sur plusieurs territoires. Pourtant, et en dépit de ces difficultés, les fournisseurs de *cloud* ont diversifié leurs offres afin d'offrir des services localisés dans certaines régions identifiées dans le contrat de *cloud*[40]. Les fournisseurs ouvrent des *data centers* (centres de données) dans de nombreuses régions du monde, non seulement en réponse aux obligations liées à la localisation des données, mais aussi pour être territorialement proches de leurs clients (et ainsi garantir des temps d'accès aux données réduits).

Dans tous les cas, il semble que ces obligations légales de localisation se diffusent de plus en plus largement, sans toutefois que leurs effets réels soient toujours convaincants pour la protection des personnes et de leurs données.

Pour autant, il reste fréquent que le *cloud* se trouve au-delà du territoire du client. Dans ce cas, d'autres difficultés juridiques peuvent alors survenir.

III. Le *Cloud* au-delà du territoire

A. Observations introductives

Il est courant de penser que ce qui est hors de notre portée est difficile à contrôler. Pour mieux connaître et contrôler les risques liés aux choix technologiques effectués par les entreprises, les autorités nationales ont imposé des règles encadrant les transferts de certaines données en dehors de leurs frontières (B). Il arrive aussi que des États adoptent des règles afin de se réserver

39 PANDAY/MALCOLM, p. 515 s.

40 Par exemple, *Amazon* (AWS), *Cloudflare*, *Google*, *Microsoft* (*Azure*) offrent la possibilité de choisir spécifiquement les régions dans lesquelles les clients souhaitent que leurs données soient conservées.

© Stämpfli Editions SA Berne

des accès aux données, et cela quel que soit le territoire sur lequel les données se trouvent (C).

B. Les règles encadrant les transferts de données au-delà du territoire

La plupart des lois réglementant les traitements de données personnelles ont encadré les transferts de données en dehors de leurs territoires. Par exemple, la loi française relative à l'informatique et aux libertés de 1978[41], la Convention 108 du Conseil de l'Europe de 1981[42] ou la LPD de 1992[43] reconnaissaient déjà de tels principes. La directive européenne de 1995 sur la protection des données avait, quant à elle, dédié un chapitre entier aux transferts des données en dehors des frontières de l'Union. Le principe consacré était celui de la confiance entre les États membres, matérialisé par la libre circulation des données sur le territoire européen, et celui de la défiance pour les États tiers, matérialisé par des restrictions juridiques interdisant en principe les transferts en dehors des frontières européennes. Ces transferts n'étaient permis que dans des cas clairement définis, notamment si « *le pays tiers en question assure un niveau de protection adéquat* » ou si le responsable du traitement, situé dans le pays tiers, « *offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes* »[44]. Ces principes ont été repris par le Règlement européen sur la protection des données[45] et se retrouvent aussi dans d'autres lois nationales de protection des données, telles que la LPD[46]. Ces règles ont un impact important pour les acteurs du *cloud* qui devront faire des choix informés avant de décider de l'ouverture de nouveaux serveurs sur d'autres territoires.

41 Art. 24 de la loi 78-17 relative à l'informatique, aux fichiers et aux libertés (France) du 6 janvier 1978.

42 Chapitre III de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Conseil de l'Europe) du 28 janvier 1981.

43 Art. 6 de la Loi fédérale du 19 juin 1992 sur la protection des données (LPD), FF 1988 II 421.

44 Art. 25 s. de la Directive 95/46 du Parlement européen et du Conseil du 25 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23 novembre 1995, p. 31.

45 Art. 44 s. du Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 119 du 4 mai 2016, p. 1.

46 Art. 6 LPD.

© Stämpfli Editions SA Berne

D'apparence assez stricte, la mise en œuvre de ces règles s'est révélée plutôt favorable aux traitements transfrontaliers[47]. Dès 2000, la Commission européenne a ainsi reconnu les États-Unis comme un territoire présentant un niveau de protection adéquat[48] permettant ainsi d'effectuer des transferts vers ce pays. Les experts en protection des données savent que cette décision d'adéquation (*Safe Harbor*), ainsi que celle qui l'a remplacée (*Privacy Shield*), ont été successivement annulées par la Cour de justice de l'Union européenne en 2015[49] et en 2020[50], générant une grande insécurité juridique pour les entreprises américaines se fondant sur ce mécanisme juridique de transfert. Les accords suisses avec les États-Unis (*Safe Harbor* et *Privacy Shield*) ont subi un sort similaire.

En mars 2022, la Commission européenne et les États-Unis ont toutefois annoncé avoir trouvé un nouvel accord de principe pour justifier les flux de données vers les États-Unis sur le fondement d'une nouvelle décision d'adéquation (*Trans-Atlantic Data Privacy Framework*). Bien que le texte juridique n'ait pas été rendu public à ce jour, la principale nouveauté du cadre juridique proposé est liée à la reconnaissance d'une voie de recours sur le territoire américain[51]. L'annonce de cet accord a été accueillie très favorablement par les grands acteurs américains du *cloud,* particulièrement *Google* et *Microsoft*. Ces instruments juridiques sont importants puisqu'ils témoignent d'une relation de confiance entre les pays et contribuent à une meilleure sécurité juridique pour les acteurs internationaux. Pour autant, l'indulgence européenne ne doit pas se transformer en complaisance, et il sera essentiel que la Commission européenne s'assure non seulement du respect des principes par les entreprises situées aux États-Unis, mais aussi de la mise en place de mécanismes de contrôle stricts sur le territoire américain[52].

En sus de ces obligations liées aux données personnelles, d'autres secteurs d'activité posent également certaines contraintes en cas de transferts internationaux. Par exemple, le secteur bancaire est strictement régulé en Suisse, et des règles spécifiques sont applicables aux banques et aux sociétés d'assurance lorsqu'elles utilisent des prestataires externes. Dans une circulaire de 2018[53], l'Autorité fédérale de surveillance des marchés financiers (FINMA) a introduit

47 Pour certains textes, telle que la Convention 108, leur objet était précisément d'organiser la circulation des données entre les territoires offrant des protections adéquates.
48 Commission européenne, décision 2000/520 du 26 juillet 2000.
49 CJUE, affaire C-362/14, du 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner*, ECLI:EU:C:2015:650.
50 CJUE, affaire C-311/18, du 16 juillet 2020, *Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems*, ECLI:EU:C:2020:559.
51 Commission européenne, Trans-Atlantic Data Privacy Framework, 15 mars 2022.
52 Voir dans ce sens, EDPB, Statement 01/2022, 6 avril 2022.
53 FINMA, Circulaire 2018/3 remplaçant FINMA, Circulaire 2008/7.

© Stämpfli Editions SA Berne

des recommandations en cas d'externalisation. Selon cette circulaire, les transferts de données à l'étranger ne sont autorisés que si l'entreprise (le client) peut « *expressément garantir qu'elle-même, sa société d'audit ainsi que la FINMA peuvent exercer et faire appliquer leurs droits de regard et d'examen* ». Cela passe notamment par le fait de garantir, à tout moment, un accès aux informations nécessaires depuis la Suisse. Cela ne devrait pas poser de problème particulier puisqu'un tel accès délocalisé est justement l'une des particularités des services de *cloud*. Pour autant, certains commentateurs pourraient qualifier ces accès comme une forme d'application extraterritoriale du droit suisse. Il arrive ainsi que les autorités de certains pays s'arrogent un pouvoir d'accès aux données situées en dehors de leur territoire.

C. Les règles octroyant des accès aux données au-delà du territoire (*CLOUD Act*, *e-evidence*)

La mondialisation des échanges et la normalisation des transferts de biens et de personnes ont engendré d'importantes évolutions dans le domaine juridique. En principe, comme nous l'avons vu, le critère utilisé pour déterminer la compétence législative et juridictionnelle est celui de la localisation matérielle. Cette localisation peut notamment être celle du sujet de droit, celle du client utilisateur ou celle du fournisseur de *cloud.* Chaque situation pouvant présenter des particularités, il faudra donc être attentif à la compétence territoriale et à l'application des dispositions impératives de chaque territoire.

Dans le domaine pénal, l'articulation entre les différents droits nationaux applicables s'est rapidement révélée complexe. La massification des flux internationaux de données a en effet créé de nouvelles difficultés pour les enquêteurs. Ces derniers souhaitent souvent accéder à des preuves localisées à l'étranger et dispersées à travers plusieurs États, ce qui rend particulièrement difficile leur reconstitution. Il est effectivement de plus en plus fréquent que les enquêteurs aient besoin d'accéder à des preuves situées sur d'autres territoires, comme les informations liées à un compte d'utilisateur ou les courriels d'une personne. Afin de permettre de tels accès, un nombre croissant de pays ont signé, à partir des années 1970, des traités bilatéraux et multinationaux d'entraide judiciaire (les *Mutual Legal Assistance Treaties,* MLAT). Ces traités fournissent un cadre juridique en matière d'accès et d'utilisation des preuves situées sur un autre territoire. Bien que nécessaires, ces traités se sont révélés trop complexes dans leur mise en œuvre et souvent inadaptés à l'ère numérique[54]. L'utilisation généralisée du *cloud* dont la caractéristique est de proposer des services transfrontières a augmenté la frustration des autorités d'enquête qui doivent, le plus

[54] SWIRE/HEMMINGS/VERGNOLLE, p. 324 s.

© Stämpfli Editions SA Berne

souvent, passer par des procédures juridiques longues et complexes alors même qu'un accès à distance est possible.

Par ailleurs, les fournisseurs de services se sont parfois retrouvés dans des situations juridiques inextricables. D'un côté, le droit de l'État dans lequel leur client se trouve empêchait la divulgation de données à un État tiers, sans passer par les mécanismes de la coopération judiciaire. De l'autre, le droit de l'État de leur siège social leur imposait de collaborer avec les autorités d'enquête nationale, en dehors des règles de la coopération judiciaire. Plusieurs affaires, notamment liées à *Yahoo!*[55] ou *Microsoft*[56], ont illustré l'étendue de ces difficultés. Dans les deux cas, les autorités nationales (belges et américaines) avaient respectivement requis *Yahoo!* et *Microsoft* de leur communiquer des informations stockées sur des serveurs basés à l'étranger (respectivement aux États-Unis et en Irlande). Les deux entreprises avaient contesté ces réquisitions en demandant aux autorités nationales de passer par les mécanismes de l'entraide judiciaire[57]. *Yahoo!* avait été condamné à une amende d'un montant de 44'000 euros en Belgique pour ne pas avoir communiqué les informations aux autorités belges. Quant à l'affaire *Microsoft*, elle a conduit le Congrès américain à adopter le *Clarifying Lawful Overseas Use of Data Act* (également connu sous l'acronyme *CLOUD Act*) en mars 2018[58].

Le *CLOUD Act* a eu deux apports principaux. D'abord, il a ouvert la possibilité pour les États d'adopter des procédures simplifiées de coopération judiciaire internationale, plus adaptées au monde numérique[59]. Ensuite, il a reconnu explicitement la compétence des autorités américaines, dans le cadre d'enquêtes pénales ou administratives diligentées pour des infractions graves, d'accéder à des données, et ce quel que soit le lieu où celles-ci sont conservées (sur ou en dehors du territoire américain)[60]. Les demandes d'accès peuvent être adressées aux personnes soumises à la compétence américaine. Selon une jurisprudence constante, les juridictions américaines interprètent cette notion de compétence selon deux niveaux :

– une compétence générale, typiquement lorsque l'organisation a son siège social ou a été constituée aux États-Unis ;

55 Cour de cassation belge, 1er décembre 2015, P.13.2082.N.
56 U.S. Court of Appeals, Second Circuit, 14 juillet 2016, *Microsoft Corporation v United States of America*, 138 S. Ct. 1186 (2018).
57 VERGNOLLE, p. 216 s. Voir aussi TF, arrêt 6B_216/2020 du 1er novembre 2021.
58 BERENGAUT/GOODLOE.
59 SWIRE/DASKAL. Voir aussi la page du site du Department of Justice intitulée *Cloud Act Resources.*
60 18 U.S.C. § 2713.

© Stämpfli Editions SA Berne

– une compétence spéciale, laquelle requiert une analyse factuelle afin de déterminer si l'organisation a suffisamment de liens avec les États-Unis[61].

La compétence spéciale laisse une place importante à l'interprétation et génère une certaine incertitude quant à l'étendue exacte des pouvoirs reconnus aux autorités d'enquête américaines vis-à-vis d'entreprises étrangères[62]. En pratique, il semble que la compétence spéciale sera reconnue dans de nombreux cas dès lors que les juridictions américaines ont déjà reconnu qu'un « simple acte » en lien avec les États-Unis permet de reconnaître une telle compétence, tant qu'il crée « une connexion substantielle »[63]. Selon une lecture littérale de ces critères, il est donc parfaitement envisageable qu'un fournisseur de *cloud* suisse ou européen ayant une présence aux États-Unis puisse être soumis à ces règles et soit obligé de fournir les données situées en Suisse mais accessibles depuis le territoire américain. Il sera alors particulièrement difficile pour le fournisseur de *cloud* de réconcilier cette obligation avec l'interdiction posée par l'article 271 du Code pénal suisse, lequel prévoit que « *celui qui, sans y être autorisé, aura procédé sur le territoire suisse pour un État étranger à des actes qui relèvent des pouvoirs publics* […] *sera puni d'une peine privative de liberté* […] *ou d'une peine pécuniaire* ». D'autant qu'aux demandes des autorités pénales peuvent également s'ajouter les accès par les services de renseignements.

Bien entendu, le *CLOUD Act* prévoit des critères encadrant les motifs pour lesquels ces demandes peuvent être effectuées ainsi que les standards permettant de justifier de tels accès[64]. Il demeure que ce texte a apporté d'importantes incertitudes et a généré une certaine défiance à l'égard des autorités américaines.

Les États-Unis ne sont pas le seul pays ayant des règles produisant des effets au-delà de ses frontières territoriales[65]. Certaines dispositions du Règlement européen sur la protection des données ont également été qualifiées comme ayant des effets extraterritoriaux[66]. Ce texte a d'ailleurs été suivi très rapidement d'une proposition de règlement européen relatif aux preuves électroniques (projet « *e-evidence* »[67]), dont les dispositions sont similaires à celles du *CLOUD Act*[68]. Introduite en 2018, la proposition de règlement est toujours en cours de négociation.

61 BERENGAUT/GOODLOE.
62 DAVIS/GUNKA, p. 52 s. Pour plus de précisions, voir Department of Justice, White Paper, p. 8.
63 U.S. Supreme Court, *Burger King Corp.* c. *Rudzewicz*, p. 475 s.
64 SWIRE/DASKAL.
65 DAVIS/GUNKA, p. 55 s. ; TRIMBLE, p. 3.
66 HERT/CZERNIAWSKI, p. 231.
67 Commission européenne, Proposition de Règlement 2018/0108 du 17 avril 2018 relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale.
68 BISMUTH, p. 681.

© Stämpfli Editions SA Berne

L'utilisation croissante des services numériques et du *cloud* renouvelle la conception de la compétence territoriale. Il y a fort à parier que les États vont continuer de se reconnaître la possibilité d'accéder non seulement aux données situées matériellement sur leur territoire, mais également à celles qui sont accessibles depuis leur territoire.

IV. Observations conclusives

Si le territoire a longtemps marqué les contours de la délimitation de la compétence des États, le numérique semble avoir remis en cause, ou du moins renouvelé, cette vision traditionnelle. Il est vrai que la structure du *cloud*, notamment du fait de ses rattachements multiterritoriaux, a tendance à éprouver la définition statique du territoire. Le *cloud* et le territoire entretiennent donc des rapports complexes.

Pour préserver leur souveraineté, les États ont adopté des mesures politiques et législatives pour rétablir une territorialisation du numérique et des données. Ces mesures présentent de nombreuses limites, et des problèmes d'articulation entre les différentes normes nationales existent. Certains États ont en effet édicté des règles qui s'imposent aux entreprises et entrent parfois en contradiction avec celles d'autres États. Les entreprises se retrouvent alors dans des situations inextricables dans lesquelles, quelle que soit leur action, elles seront en violation du droit d'au moins un État.

Dès lors, il faut se demander si la technique ne peut pas contribuer à apporter quelques pistes de simplification. Actuellement, des entreprises mettent en place du chiffrement des données de bout en bout, c'est-à-dire non seulement lors du transport des données mais aussi lorsqu'elles se trouvent dans le *cloud.* Ces entreprises conservent ainsi sur leurs serveurs des données chiffrées pour lesquelles elles n'ont pas les clés de déchiffrement. Elles sont donc incapables de déchiffrer les données ou de les communiquer en clair à des tiers. Avec les développements dans le domaine du chiffrement homomorphe, il sera bientôt possible d'effectuer, dans le *cloud*, des traitements plus complexes sur ces données chiffrées, garantissant ainsi une meilleure confidentialité et sécurité des données[69]. De telles solutions diminuent le nombre de droits applicables puisque le nombre de personnes ayant accès aux données en clair est moins élevé, réduisant donc nécessairement le nombre de personnes auxquelles des réquisitions peuvent être adressées. Une difficulté persiste : celle de savoir sur quel territoire le client va conserver les clés de déchiffrement dès lors que le droit de cet État trouvera à s'appliquer.

[69] BRADLEY.

© Stämpfli Editions SA Berne

Si les doutes entourant les questions juridiques relatives au *cloud* et au territoire laissent parfois penser que le nuage est noir, il ne faut pas oublier qu'une de ses faces reste orientée vers le soleil et que des solutions pourront toujours être trouvées.

V. Bibliographie

A. Littérature

Juliette Ancelle/Karim Ferdjani, Les contrats informatiques, *in* Alexandre Richa/Damiano Canapa (éds), Droit et économie numérique, CEDIDAC, 2021, vol. 73, p. 131 ss ; **Matthieu Bourgeois/Marion Moine**, CLOUD COMPUTING. – Cloud et protection des données à caractère personnel, JurisClasseur Communication, Fascicule 961, 1er mai 2020 ; **Alexander Berengaut/Katherine Goodloe,** Reaching for the CLOUD, *in* Global Data Review, 2019 ; **Régis Bismuth**, Le Cloud Act face au projet européen e-evidence : confrontation ou coopération ?, *in* Revue critique de droit international privé, 2019, p. 681 ss ; **Jeremy Bradley**, The (r)Evolution of FHE, *in* Zama, 2022 ; **Dominique Carreau/Fabrizio Marrella**, Droit international, Pedone, 2012 ; **Anupam Chander/Uyên Lê**, Data nationalism, *in* Emory Law Journal, 2015, vol. 64, p. 677 ss ; **Nigel Cory/Luke Dascoli,** How barriers to cross-border data flows are spreading globally, what they cost, and how to address them, Information Technology & Innovation Foundation, 2021 ; **Frederick Davis/Charlotte Gunka,** Perquisitionner les nuages – *CLOUD Act,* souveraineté européenne et accès à la preuve dans l'espace pénal numérique, *in* Revue critique de droit international privé, 2021, p. 43 ss ; **Alexis Fitzjean Ó Cobhthaigh,** Le cloud et la souveraineté numérique dans le nouveau monde, *in* Revue pratique de la prospective et de l'innovation, 2021, nº 1, p. 16 ss ; **Solange Ghernaouti/Christian Aghroum**, Cyber-résilience, risques et dépendances : pour une nouvelle approche de la cyber-sécurité, *in* Sécurité et stratégie, 2012, vol. 4, p. 74 ss ; **Jack Goldsmith**, The Internet and the Abiding Significance of Territorial Soveriegnty, *in* Indiana Journal of Global Legal Studies, 1998, vol. 5, p. 475 ss ; **Nicolas Grevet**, Le *cloud computing* : évolution ou révolution ? Pourquoi, quand, comment et surtout faut-il prendre le risque ?, Mémoire de recherche, Cergy-Pointoise, 2009 ; **Paul de Hert/Michal Czerniawski**, Expanding the European data protection scope beyond territory : Article 3 of the General Data Protection Regulation in its wider context, *in* International Data Privacy Law, 2016, vol. 6, p. 230 ss ; **Jerzy Kranz**, Notion de souveraineté et le droit international, *in* Archiv des Völkerrechts, vol. 30, nº 4, 1992, p. 411 ss ; **Michael Montavon,** L'externalisation du traitement de données dans le *cloud*, *in* Cyberadministration et protection des données, Schultess, 2021, p. 457 ss ; **Jérémie Müller**, For et droit pénal applicable au *cloud computing*, *in* ForumPoenale, Stämpfli, 2013, p. 306 ss ; **Jyoti Panday/Jeremy Malcolm,** The political economy of data localization, *in* The open journal of sociopolitical studies, 2018, vol. 4, p. 511 ss ; **Isabelle Scherrer**, Internet, un réseau sans frontière ? Le cas de la frontière franco-belge, *in* Annales de géographie, 2005, nº 645, p. 471 ss ; **David Rosenthal/Samira Studer,** La nouvelle loi sur la protection des données, *in* Jusletter, 16 novembre 2020 ; **Peter Swire/Jennifer Daskal,** Frequently asked questions about the U.S. CLOUD Act, 2019 ; **Peter Swire/Justin Hemmings/Suzanne Vergnolle**, A mutual legal assistance case study : the United States and France, *in* Wisconsin International Law Journal, 2017, vol. 34, p. 324 ss ; **Marketa Trimble**, Extraterritorial

© Stämpfli Editions SA Berne

Enforcement of National Laws in Connection with Online Commercial Activity, *in* John ROTHCHILD (éd), Research handbook on electronic commerce law, Edward Elgar, 2016 ; **Suzanne VERGNOLLE**, Understanding the French criminal justice system as a tool for reforming international legal cooperation and cross-border data requests, *in* Data Protection, Privacy and European Regulation in the Digital Age, University Press of Helsinki, 2016, p. 205 ss.

B. Documents officiels

CNIL, « Définition de Cloud Computing », <https://www.cnil.fr/fr/definition/cloud-computing> (*consulté le 5 juin 2022*) ; **Commission européenne**, Trans-Atlantic Data Privacy Framework, mars 2022, <https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf> (*consulté le 5 juin 2022*) ; **Conseil Fédéral**, Communiqué « Le Conseil Fédéral commande une étude sur la faisabilité d'un « Swiss Cloud » », 16 avril 2020 ; **Commission européenne**, Décision 2000/520 du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique ; **Département fédéral des finances, UPIC,** Rapport sur l'évaluation des besoins d'un nuage informatique suisse (« Swiss Cloud »), décembre 2020 ; **Department of Justice (DOJ),** White Paper, Promoting Public Safety, Privacy, and the Rule of Law Around the World : The Purpose and Impact of the CLOUD Act, avril 2019 ; **Department of Justice (DOJ),** CLOUD Act Resources, <https://www.justice.gov/dag/cloudact> (*consulté le 5 juin 2022*) ; **EDPB**, Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework, 6 avril 2022 ; **FINMA,** Circulaire 2018/3 sur les externalisations dans le secteur des banques, des entreprises d'assurance et de certains établissements financiers au sens de la LEFin, entrée en vigueur le 1er avril 2018 ; **Ministère français de l'Europe et des affaires étrangères, ministère de l'économie, des finances et de la relance et secrétariat d'État chargé de la transition numérique et des communications électroniques sur la souveraineté numérique de l'Union européenne**, Communiqué conjoint du 7 février 2022 ; **Ministre français de l'économie et des finances et Commissaire européen au marché intérieur, sur la souveraineté numérique et la stratégie industrielle de l'Union européenne,** Déclarations du 7 février 2020 ; **Ministère français de l'intérieur et de la culture,** Note d'information du 5 avril 2016 relative à l'informatique en nuage (*cloud computing*) ; **Franck MONTAUGÉ/Gérard LONGUET,** Rapport sur la souveraineté numérique, Sénat Français, no 7, 2019 ; **Préposé fédéral à la protection des données et à la transparence (PFPDT)**, Explications concernant l'informatique en nuage (*cloud computing*) ; **Premier ministre français** François Fillon, Discours sur le thème du très haut débit et l'économie numérique, Vélizy, 18 janvier 2010 ; **Cédric VILLANI**, Donner un sens à l'intelligence artificielle. Pour une stratégie nationale européenne, 2018 ; **Ursula VON DER LEYEN**, A Union that strives for more. My agenda for Europe, Political guidelines for the next European Commission 2019-2024, 2019.

© Stämpfli Editions SA Berne

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

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

© Stämpfli Editions SA Berne · 2022
www.staempfliverlag.com

Print ISBN 978-3-7272-4456-8

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

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

printed in
switzerland

© Stämpfli Editions SA Berne