Souveraineté numérique : étude pluridisciplinaire pour la Suisse

Benhamou, Yaniv; Bernard, Frédéric; Durand, Cédric

Collaborators: Ribeiro Pedrosa, Helena

Digital Law Center
www.digitallawcenter.ch

UNIVERSITÉ DE GENÈVE
FACULTÉ DE DROIT

Souveraineté numérique

Etude pluridisciplinaire pour la Suisse

Benhamou Yaniv, Bernard Frédéric, Durand Cédric

Genève, le 31 janvier 2023

Souveraineté numérique

Etude pluridisciplinaire

* Prof. Benhamou Yaniv, Droit du numérique / UNIGE
Prof. Bernard Frédéric, Droit public / UNIGE
Prof. Durand Cédric, Économie politique / UNIGE
Avec la collaboration de Mme Helena Ribeiro Pedrosa

Genève, 20 janvier 2023

* **Yaniv BENHAMOU** est professeur associé en droit du numérique (propriété intellectuelle et protection des données) à la Faculté de droit / Digital Law Center de l'Université de Genève. **Frédéric BERNARD** est professeur ordinaire à la Faculté de droit (département de droit public) de l'Université de Genève. **Cédric DURAND** est professeur associé à la Faculté des sciences de la société (département d'histoire, économie et société) de l'Université de Genève. **Helena RIBEIRO PEDROSA** est assistante de recherche au Digital Law Center. Ils remercient vivement M. Marc-Olivier BUSSLINGER ainsi que les expert·e·s suivant·e·s qui ont été interviewé·e·s: Prof. Nicolas BAYA LAFFITE, Prof. Edouard BUGNION, Prof. Jean-Pierre HUBAUX Prof. Diego KUONEN, Prof. Tobias METTLER, Prof. Sophie WEERTS. Cette étude a été réalisée sur mandat de la Conférence latine des directrices et directeurs du numérique (CLDN).

Table des matières

Synthèse (*Executive Summary*)

Cette analyse est une étude pluridisciplinaire de la souveraineté numérique (en particulier sous l'angle socio-économique et juridique) qui vise à formuler des recommandations (*Policies*) à l'attention des autorités suisses des différents échelons et à contribuer aux réflexions stratégiques (y compris dans le contexte du débat sur un *cloud* souverain). Cette étude offre aussi des pistes de réflexions qui pourraient contribuer au débat général en Suisse et à l'étranger. Au-delà de la Suisse, les spécificités de la Confédération (e.g. fédéralisme et compétences distribuées, partenariats public-privé) font de son écosystème un laboratoire intéressant en matière de souveraineté numérique. Les enjeux sont traités de façon transversale, en particulier sous l'angle socio-économique et juridique, et sur la base de l'état de l'art (desk based-research) et d'entretiens. L'étude n'a enfin aucune prétention d'exhaustivité mais uniquement de poser quelques enjeux sélectionnés afin de contribuer aux réflexions stratégiques.

S'agissant de la définition de la souveraineté numérique, celle-ci est entendue ici sous l'angle de ses différentes composantes, dont principalement la "souveraineté technologique" et la "souveraineté des données". Elle est définie comme la capacité des autorités à maintenir leur autonomie stratégique, soit à pouvoir utiliser et contrôler de manière autonome les biens matériels et immatériels et les services numériques qui impactent l'économie, la société et la démocratie. Il est recommandé de prioriser certains domaines, en particulier la souveraineté des données, puisque ce domaine semble être prioritaire pour les citoyen·ne·s et tous les domaines ne pouvant être appréhendés simultanément à court terme.

L'étude observe aussi que le numérique redéfinit la notion de "territoire" en "souveraineté sur les réseaux" composée de plusieurs strates (physique, logique et données), l'État pouvant exercer une souveraineté exclusive sur la 1ère strate (physique) et une souveraineté limitée sur les 2ème et 3ème strates (logique et données) dépourvues de limites spatiales clairement définies. Le degré de souveraineté s'appréciera selon la capacité de l'État à contrôler chaque strate, laquelle dépendra notamment de la localisation des données ou de l'accès aux données, de la nature et de l'étendue des liens du prestataire de services avec l'État en question. Les stratégies politiques et réglementaires peuvent par ailleurs porter sur les différents acteurs de l'écosystème numérique (public, industrie, société civile).

Sous l'angle des enjeux socio-économiques, l'étude analyse les dépendances de la Suisse à l'égard des trois strates (matérielles, logicielles, données) et du point des différents acteurs (public, industrie, société civile). Elle conclut que la Suisse dispose de solides atouts dans le domaine du numérique mais qu'il convient d'être vigilent sur certains points, en particulier du fait que l'activité numérique grand public et la propriété intellectuelle sont concentrées en main de quelques entreprises (avec des effets sur la vie privée, l'action publique et le développement économique). Elle décrit aussi un dilemme autonomie-sophistication : les dépendances exposées augmentent proportionnellement à l'intensité des usages des TIC. L'analyse souligne encore que la souveraineté n'est pas uniquement spatiale mais aussi temporelle, c'est-à-dire en termes de faculté d'anticipation et de temps dont dispose une autorité pour réagir à une situation nouvelle.

Sur cette base, il est **recommandé** de faire une évaluation du degré de criticité des différents usages du numérique au sein et hors des administrations, ce afin de guider l'action publique en matière de souveraineté numérique. Cette évaluation du degré de criticité permet de distinguer quatre cas impliquant des mesures distinctes, suivant que les usages soient : *(i)* peu critiques et simples (zone bleue), *(ii)* complexes mais peu critiques (zone orange), *(iii)* critiques mais simples (zone verte), *(iv)* critiques et complexes (zone rouge). Dans ce dernier cas, lorsqu'une solution locale même coûteuse est inaccessible, réduire le risque passe par des mesures de protection (e.g. résidence des données), une sélection et une diversification des fournisseurs ou la recherche de coopération permettant d'exercer une souveraineté partagée. Par ailleurs, lorsqu'un fournisseur est sis en Suisse mais qu'il appartient à un groupe étranger pouvant le contraindre à prendre des décisions contraires aux intérêts de la Suisse, la puissance publique pourrait être amenée à prendre des participations actionnariales dans les entités résidentes dont elle dépend pour des services critiques et ce de manière à disposer d'un regard interne sur les enjeux qui intéressent directement sa souveraineté.

Sous l'angle des enjeux juridiques, l'étude analyse les principales composantes de la souveraineté numérique, soit la souveraineté des données et la souveraineté technologique, ainsi que la cyberadministration et la cybersécurité. Les territoires et les acteurs sont également analysés mais de façon transversale. L'étude rappelle l'importance de la **cyberadministration**. L'Etat doit pouvoir décider si et comment numériser ses processus et ses services de façon autonome, ce dans le respect des principes de fédéralisme, de légalité et des marchés publics. La souveraineté numérique peut en effet aussi signifier ne pas numériser certains services (p.ex. pour des raisons de sécurité et/ou sobriété). Sur cette base, il est **recommandé** de planifier en continu la transformation numérique, en analysant soigneusement le besoin d'adapter ou d'édicter les bases légales nécessaires et le droit des marchés publics (e.g. libellé des appels d'offres ou procédures de gré-à-gré). Il est aussi recommandé de clarifier quelle autonomie cantonale subsiste. Dans le doute, on pourrait considérer qu'il existe une autonomie (ou souveraineté) cantonale au nom du principe de la primauté du droit fédéral et de subsidiarité.

La **souveraineté des données** est encadrée par des lois pouvant avoir un effet extra-territorial (e.g. RGPD, *Cloud Act,* LPD) et des règles de transfert des données à l'étranger allant d'une libre circulation des données vers une exigence de localisation des données ou des serveurs. Sur cette base, il est **recommandé** que les autorités analysent la compatibilité des lois étrangères avec la souveraineté suisse avant de les appliquer et la possibilité de conférer aux lois suisses un effet extra-territorial. Lors du transfert de données à l'étranger, il convient de procéder à une évaluation des risques et d'aménager les rapports contractuels en conséquence, cas échéant de privilégier une solution locale en présence de données ou d'infrastructures critiques.

La **souveraineté technologique** passe par une politique d'innovation qui inclut des mesures étatiques (juridiques, économiques et techniques), lesquelles supposent d'évaluer soigneusement quelles sont les technologies critiques (KET) auxquelles avoir accès et les lois de protection des données. Sur cette base, il est **recommandé** de privilégier une coopération européenne et internationale (au lieu de mesures protectionnistes). S'agissant des mesures étatiques, il est recommandé de privilégier des mesures de soutien complémentaires (e.g. contrats-types, certifications, sensibilisation et formation) à des mesures législatives majeures. Il est aussi recommandé d'améliorer les compétences des utilisateurs publics et privés et de garder une maîtrise la plus totale (e.g. in-sourcer) la transformation numérique des activités régaliennes (*cyberadministration*) (e.g. identification e-ID et signature électronique).

La **cybersécurité** est un élément clé dans une société numérique, qui passe par des moyens technologiques résilients, une préparation adéquate, la mise en place de contrats adaptés et des processus de contrôle de conformité (*compliance*). Sur cette base, il est **recommandé** de mettre en place des contrats avec les fournisseurs de TIC incluant des TOMs. Il est aussi recommandé de s'assurer d'un cadre légal clair, ce qui plaide pour le suivi des recommandations du NCSC et des mesures incitatives ou contraignantes en assurant leur respect. A l'international, il serait intéressant de rechercher des solutions pour protéger les civils en cas de cyberattaques étatiques, de soumettre les entreprises technologiques aux règles de droit humanitaire et de développer des solutions de type ambassades de données (*Data-Embassies*).

I. Introduction et définitions

1. Objectifs et délimitations

La présente étude est une étude pluridisciplinaire sur les enjeux de la souveraineté numérique principalement destinée aux décideur·euse·s politiques et stratégiques suisses, réalisée sur mandat des cantons de Genève et de Vaud. L'objectif est d'aider les autorités des différents échelons (Confédération, cantons, communes) à faire des choix stratégiques en matière de souveraineté numérique. Plus spécifiquement, l'étude a un objectif double : poser un cadre d'analyse interdisciplinaire de la souveraineté numérique (objectif principal) et offrir un cadre et un contexte à l'étude d'opportunité d'un cloud souverain comme à d'autres projets ultérieurs (objectif secondaire)[1]. Cette étude offre enfin des pistes de réflexions qui pourraient contribuer au débat général en Suisse et à l'étranger. Au-delà de la Suisse, les spécificités de la Confédération (e.g. fédéralisme et compétences distribuées, partenariats public-privé) font de son écosystème un laboratoire intéressant en matière de souveraineté numérique[2].

Les enjeux de souveraineté numérique étant transversaux, il est important de les traiter sous l'angle des différentes disciplines (e.g. droit, économie, sociologie, histoire, géopolitique, des sciences informatiques). A cette fin, l'étude a été réalisée par une équipe pluridisciplinaire de 3 chercheurs, en particulier Prof. Yaniv Benhamou (droit du numérique et protection des données), Prof. Frédéric Bernard (droit administratif) et Prof. Cédric Durand (économie politique) avec l'aide de Mme Helena Ribeiro Pedrosa (chercheuse au Digital Law Center). Il est précisé que le sujet est extrêmement vaste et concerne toutes les dimensions de la société numérique. L'étude se limite aux disciplines représentées (socio-économiques et droit), même si elle tient compte des enjeux techniques, en particulier de l'étude technique sur le *cloud* souverain mandatée par le canton de Vaud. L'étude n'a ainsi aucune prétention d'exhaustivité mais uniquement de poser quelques enjeux sélectionnés afin de contribuer aux réflexions stratégiques. Cette étude pluridisciplinaire, de même que celle sur les enjeux techniques du *cloud* souverain s'inscrivent dans les travaux de la Conférence latine des directrices et des directeurs du numérique (CLDN).

2. Contexte

La souveraineté numérique suppose que l'État, l'économie et la société maîtrisent en continu leur transformation numérique, soit si et quelles informations numériser en vue de leur réutilisation[3]. En effet, seules les entités maîtrisant leurs actifs numériques, voire les TIC[4] peuvent envisager d'être souveraines numériquement[5]. Si les États possèdent indéniablement une maîtrise technique dans ce domaine – comme le montre notamment la mise au point de l'application SwissCovid – ce sont souvent les **acteurs privés qui maîtrisent les TIC**. On pense non seulement aux acteurs économiques dominants sur le marché (e.g. GAFAM et BHATX) qui décident du sort des données[6], voire s'arrogent des

[1] Voir DFF/UPIC, Rapport Swiss Cloud et DIGITAL SWISS, Stratégie suisse numérique 2023 (site web) : Ces 2 rapports font du recours au Cloud et de la souveraineté numérique une priorité et concluent à un besoin de clarification des notions (e.g. terminologie, degrés de souveraineté) et du cadre légal (e.g. pour réduire les risques d'accès aux données par des tiers, tels que les autorités étrangères).

[2] Pour une analyse de l'UE, cf. MOGHIOR, mettant en avant la difficulté à trouver un consensus en raison de la nature décentralisée des institutions et de l'hétérogénéité des États membres ; BRUNESSEN, rappelant l'importance d'une politique transversale et d'encadrer l'économie de la donnée et des plateformes. L'exemple suisse pourrait être ainsi, toutes proportions gardées, un autre exemple d'institutions décentralisées dont les pays voisins pourraient s'inspirer, avec ses mécanismes de gouvernance et de consensus.

[3] Pour la définition de la transformation numérique, cf. TAN et al., p. 1.

[4] Les TIC et les données sont des actifs numériques qui constituent des facteurs d'influence sur les indicateurs d'innovation et de compétitivité de l'économie nationale. Ils sont par ailleurs vecteurs de valeurs et de normes.

[5] La transformation numérique est un processus qui comporte différentes étapes, à savoir une phase de planification, une phase de mise en œuvre et une phase de contrôle, voir *infra* II.2.a. ; Pour l'importance de la transformation numérique comme préalable à la souveraineté numérique, voir SECO, Économie numérique (site web) ; DFF, Administration numérique (site web) ; SECO, Digitalisation des PME en Suisse: un enjeu central (site web) ; CHANCELLERIE FÉDÉRALE, Suisse numérique (site web).

[6] E.g. via leurs conditions générales d'utilisation. Voir TÜRK et références : "*[fixer] les conditions les conditions générales d'utilisation de services en ligne devenus indispensables, [développer] les algorithmes, [décider] de supprimer des contenus, de fermer le profil d'un utilisateur, de conserver ou de vendre les données personnelles dont elles assurent le stockage*".

prérogatives étatiques[7], mais aussi aux acteurs non-dominants sur le marché qui créent des dépendances avec d'autres opérateurs[8]. Les acteurs économiques acquièrent alors un **pouvoir normatif** de fait dans le cyberespace[9].

Face à l'émergence de nouveaux rapports de force, les milieux politiques emploient fréquemment le concept de souveraineté numérique dans leurs discours dans le but de restaurer la centralité de l'État-nation[10]. Ce concept n'est toutefois **pas encore clarifié** et peine à trouver une réelle consécration politique, rendant difficile toute cohérence aux niveaux décisionnel et opérationnel. Alors que ce concept doit trouver une place dans un contexte politique et réglementaire fragmenté, la prolifération rapide d'initiatives en matière de souveraineté numérique complexifie la délimitation du concept et des pouvoirs des entités fédérales, cantonales, et communales.

On songe aussi aux **enquêtes** qui visent à saisir comment la notion de souveraineté numérique est perçue par les différents acteurs. Par exemple, une enquête européenne conclut que 80% des entreprises européennes se disent dépendantes de prestataires étrangers[11]. Ces conclusions sont confirmées par les témoignages d'expert·e·s que nous avons collectés dans le cadre de cette étude[12]. En particulier, les expert·e·s concluent que tous les pays, dont la Suisse, sont dépendants de technologies étrangères, de sorte que des mesures protectionnistes doivent être évitées au profit d'une analyse stratégique des dépendances et d'une politique publique nuancée en matière de souveraineté numérique. Parmi les mesures permettant de renforcer la souveraineté numérique, les expert·e·s soulignent la nécessité d'une volonté politique commune de transformation numérique[13], la sensibilisation des décideur·euse·s politiques et de la population[14] (e.g. via des mesures éducatives, telles que *data literacy,* et la promotion de "valeurs souveraines")[15]. Dans le cadre des marchés publics, le critère du prix devrait aussi être relativisé en faveur de critères de souveraineté numérique. La régulation des technologies doit prendre en compte les réalités techniques (e.g. risques et impacts technologiques, opérationnels et juridiques) ainsi que le caractère intrinsèquement global et l'influence de l'industrie qui relativise le caractère territorial du numérique et érode la souveraineté numérique.

On songe aussi aux différents **modèles** qui visent à quantifier la souveraineté numérique sur la base d'indicateurs (e.g. composantes, valeurs et objectifs stratégiques)[16]. Ces modèles varient toutefois selon

---

[7] E.g. en rendant les États dépendants de leurs services avec des monnaies virtuelles ou des techniques fiables d'authentification. Voir COTTIER, Privatisation, N 8 ; TÜRK et références ; BELLI ; JÄGER.

[8] Les dépendances ont plusieurs dimensions pour l'industrie, elles peuvent être notamment opérationnelles (effectuer ses services dans les temps), économiques (contrôle et tirer les bénéfices de la chaîne de valeur), légales (sujettes ou non aux lois extra-territoriales), liées aux données, politiques, militaires. Cf. BOUNIE.

[9] TÜRK et références ; POHLE/THIELE, p. 6ss ; SEIFRIED/BERTSCHEK, p. 10ss.

[10] Cf. FALKNER et al. ; Voir aussi AUFRECHTER/KLOSSA, indiquant que le concept de souveraineté numérique sert aussi de prétexte à un protectionnisme économique, en référence à un rapport du gouvernement américain de 2021.

[11] Cf. SEIFRIED/BERTSCHEK, p. 39ss : Dans le cadre de l'enquête, les entreprises ont également été interrogées sur leur sentiment de dépendance vis-à-vis des fournisseurs/partenaires étrangers dans six domaines technologiques. Pour la notion de dépendance, cf. n. 8 et 69.

[12] Les expert·e·s suivant·e·s ont été interviewé·e·s : Prof. Edouard BUGNION, Prof. Diego KUONEN, Prof. Tobias METTLER, Prof. Jean-Pierre HUBAUX Prof. Sophie WEERTS et Prof. Nicolas BAYA LAFFITE. Il est précisé que les auteurs ont également contacté plusieurs expertes (également dans un souci de représentativité) mais qu'ils n'ont pas pu recevoir de retour sur ce rapport. Les conclusions qui suivent sont une synthèse des différents entretiens. Le questionnaire sur la base duquel les entretiens ont été conduits figure en annexe 3 (Questionnaire).

[13] En effet, sans changement de culture et sans volonté politique commune des décideur·euse·s politiques, la transformation numérique est précipitée, sans la confiance de la population et sans sécurité des infrastructures et des données (e.g. manque d'interopérabilité, failles de sécurité).

[14] Ce afin d'envisager des solutions technologiques intègres, dignes de confiance et adaptées aux besoins stratégiques.

[15] A ce titre, Prof. Jean-Pierre HUBAUX souligne que "*d'énormes progrès techniques ont été réalisés au cours des vingt dernières années pour permettre à un client de protéger les données stockées sur un cloud auquel il ne fait pas entièrement confiance. Ces progrès techniques se fondent sur deux approches. La première, baptisée "trusted executed environment", permet d'établir sur les serveurs cloud des zones de stockage et de calcul auxquels le fournisseur de service cloud n'a pas accès. La seconde se fonde sur le chiffrement. Ainsi, le client peut chiffrer ses données sensibles avec ses propres clés cryptographiques avant de les stocker dans le cloud*".

[16] Quelques exemples (non-exhaustifs) peuvent d'ores et déjà être évoqués comme base de réflexion : une étude de KALOUDIS tente d'élaborer une ébauche d'index de souveraineté numérique, en regroupant plusieurs index en matière de souveraineté et de numérisation. L'UE utilise le Digital Economy and Society Index (DESI) sur la base d'indicateurs de numérisation de l'économie et de la société concernant le capital humain, la connectivité, l'intégration des technologies numériques, et les services publics numériques. L'index de souveraineté technologique se base sur certains domaines spécifiques (l'intelligence artificielle, le *big data*, le *cloud computing*, les semi-conducteurs, la robotique, l'internet des objets, le calcul haute performance, les télécommunications avancées et la cybersécurité), mais il convient toutefois de noter que ces indicateurs ont été élaborés selon les enjeux actuels de développement économique de l'UE. Les capacités technologiques des États membres sont, quant à elles, mesurées à l'aide de certains indicateurs (les contributions à la recherche, aux brevets et aux normes, le nombre d'entreprises et de professionnels de la technologie, les parts de marché des entreprises, les investissements en capital-risque dans ces technologies, l'adoption des technologies, leurs positions sur les réglementations et la coopération de l'UE, leur engagement dans les forums technologiques

le pays et/ou l'entité concernés. Par exemple, le modèle *Digital dependency index* analyse la souveraineté numérique en référence à la vulnérabilité économique d'un État vis-à-vis de l'étranger et en référence aux 3 indicateurs : TIC fabriquées à l'étranger, services d'infrastructures et de données ainsi que propriété intellectuelle venant de l'étranger[17]. Par ailleurs, aucun modèle de ce type n'existe en Suisse pour le moment[18]. La volonté des acteurs politiques sera donc déterminante pour développer ou appliquer un modèle à la Suisse.

On notera enfin que, s'il est logique que la Suisse se positionne en matière de souveraineté numérique, le mouvement de souveraineté numérique peut contribuer à davantage de méfiance du public et des autorités vis-à-vis de certaines entreprises privées et de certains gouvernements et avoir des effets négatifs. Par exemple, il peut conduire à la fragmentation d'internet[19], freiner l'innovation (p.ex. développement des technologies, telles que le web3)[20] et le partage des données au service du bien commun[21].

3. Définitions

Les termes de "souveraineté numérique" ne bénéficient à ce jour **d'aucune définition harmonisée** aux niveaux international et national. Plusieurs tentatives de définition ont toutefois émergé, notamment dans le monde académique. Les notions *(a)*, les composantes *(b)* et les territoires *(c)* en jeu seront analysés, afin de mieux cerner les contours de ce concept et de poser des jalons terminologiques.

a) Notions

Une première approche consiste à définir les deux termes qui composent la notion. Le **"numérique"** se réfère aux technologies, infrastructures, données et contenus utilisant des techniques de calcul électronique ainsi qu'à leurs conséquences sur la société, la culture et les processus[22]. La **souveraineté** se réfère au territoire d'un État, soit à l'acteur souverain qu'est la nation (i.e. souveraineté externe) et qui a le monopole sur les règles de droit et la force publique (e.g. police ou justice) (i.e. souveraineté interne)[23]. Cette approche classique de la souveraineté, appliquée à l'ère numérique, se réfère donc aux compétences étatiques en matière de numérique (e.g. cybersécurité, protection des données, exercice

internationaux, leur participation à la recherche et au développement européens, leurs contributions aux initiatives technologiques internationales de l'UE et les résultats de sondages sur le soutien public au développement technologique). Voir KALOUDIS, Index, p. 8ss ; COMMISSION EUROPÉENNE, Digital Economy and Society Index (DESI) 2022 (site web) ; PUGLIERIN/ZERKA, p. 5ss.

[17] Cf. LU/MAYER : Les 3 indicateurs sont les suivants : (1) produits et services TIC fabriqués et fournis par des fournisseurs basés à l'étranger (mesurable par la part des importations dans les statistiques du commerce extérieur), (2) infrastructures d'information, soit les écosystèmes ou plateformes numériques et dispositifs connectés contrôlés et/ou fournis par des entreprises étrangères (mesurable par les parts de marché), et (3) propriété intellectuelle, soit les brevets de technologies numériques détenus par des entreprises étrangères (mesurable par les statistiques de délivrance de brevets).

[18] Seuls des index isolés évaluant notamment le développement numérique et l'usage des TIC peuvent être identifiés. Voir *infra* II.1.

[19] DIPLOFOUNDATION concluant que la fragmentation d'internet peut être évitée, notamment en renforçant la confiance du public dans l'utilisation d'internet, en adoptant des standards (e.g. IPv6 et IDNs), en clarifiant l'impact des nouvelles lois sur l'architecture d'internet et en renforçant la collaboration internationale pour des normes et standards internationaux et pour une coordination entre États et organisations internationales (p.ex. ICANN, UIT et IGF). Cf. DIPLOFOUNDATION, Balancing digital sovereignty and the splinternet (event report), Internet Governance Forum, 2022.

[20] Ces exigences font également référence à la "souveraineté des données" ; Concernant l'impact de la souveraineté numérique sur les technologies *blockchain*, voir GANNE, not. p. 45 et 101 ; De manière plus générale, voir CORY/DASCOLI : "*The number of data-localization measures in force around the world has more than doubled in four years. In 2017, 35 countries had implemented 67 such barriers. Now, 62 countries have imposed 144 restrictions*.").

[21] On peut songer aux barrières au partage des données de santé pendant la crise covid-19. A ce propos. cf. l'article précurseur de HARARI Yuval, The World After Coronavirus, *in* Financial Times, 20 mars 2020.

[22] COUTURE/TOUPIN, p. 2306 ; Au-delà de l'aspect purement technique, on peut en effet considérer le numérique comme incluant la numérisation des processus de l'État, internes et externes (*digital in governement* et *e-governance*) et plus généralement la gestion des implications juridiques, économiques et sociales de la transformation numérique (*governance in a digital world*). Voir *infra* III.2.a.

[23] Cf. art. 2 Charte ONU ; POHLE/THIEL, p. 49 ; ALCAUD : dans une approche philosophique, "*la souveraineté appartient au peuple, entendu comme l'ensemble des citoyens. Chacun d'eux est ainsi détenteur d'une parcelle de souveraineté. Dans cette logique, les citoyens ont une relation étroite avec la politique, et ils donnent à leur représentant un mandat "impératif""*. ; INTERNET SOCIETY distingue 3 aspects de la souveraineté : (i) la capacité d'un État d'exercer son pouvoir et son contrôle sur un peuple et les ressources d'un territoire donné ; (ii) indépendamment des influences extérieures ; (iii) la capacité des individus et des communautés d'agir de façon autonome. Cf. INTERNET SOCIETY, Navigating Digital Sovereignty and its Impact on the Internet, décembre 2022.

des fonctions régaliennes)[24]. Cette approche classique est toutefois critiquée du fait qu'elle ne tient pas compte des nouveaux rapports de force exercés par les acteurs non-étatiques (e.g. utilisateurs internet ou opérateurs de plateformes) qui font émerger *de facto* de nouvelles formes de territoires[25].

La souveraineté numérique est par ailleurs souvent définie sous l'angle **technologique** qui distingue parfois trois degrés de souveraineté (élevé, moyen et faible) pour chaque étape du cycle de vie d'un système numérique et d'une donnée[26]. Au-delà de la définition technologique et vu que les différentes disciplines mettent en exergue différents enjeux, il est intéressant de définir la notion d'un point de vue **pluridisciplinaire**, en particulier des sciences sociales et du droit. Ceux-ci distinguent généralement les notions de "souveraineté numérique" et "d'autonomie stratégique". L'**autonomie stratégique** se réfère à la capacité d'un État ou d'une organisation à décider et à agir de façon autonome et sur le long terme sur les aspects numériques essentiels de son économie, sa société et sa démocratie[27].

Alors que la souveraineté d'un État est devenue indissociable de la technologie, l'autonomie stratégique vise les moyens pour l'atteindre[28]. Elle se concentre sur la capacité de l'État de contrôler les TIC et les données. Cette définition semble plus précise et mieux délimitée que la notion de "souveraineté numérique", en particulier car elle permettrait d'éviter les controverses juridiques liées à la reconnaissance de la "souveraineté" des acteurs non-étatiques ou supranationaux[29].

b) Composantes

La **souveraineté numérique** inclut **plusieurs composantes**, dont principalement la "souveraineté technologique" et la "souveraineté des données"[30]. Elle intervient dans toutes les facettes de la vie numérique, en particulier dans le choix des infrastructures techniques (e.g. antennes de téléphonie mobile, réseaux de fibre optique), des logiciels utilisés et du mode de stockage des données.

La **souveraineté technologique** se réfère au contrôle sur les *hardwares*, les *softwares*, les infrastructures et les services numériques ("sous-composantes")[31]. Elle implique une certaine capacité d'un Etat et de ses opérateurs économiques à innover et à s'engager dans le développement technologique, notamment au moyen de politiques publiques d'innovation, du développement de *softwares* ou d'infrastructures

---

[24] NORODOM, p. 21ss : Les contextes politico-économiques peuvent toutefois créer des approches divergentes de ce même concept par des entités étatiques. Une vision "libérale" s'oppose traditionnellement à une vision plus "autoritaire" et "protectionniste" de la souveraineté numérique.

[25] COUTURE/TOUPIN, p. 2308ss ; FABIANO, p. 272 ; ROGUSKI, p. 1 ; CELESTE, p. 13ss ; POHLE/THIEL, p. 4ss : à ce titre, la notion antagoniste de "souveraineté du cyberespace" a émergé par le biais de la Déclaration d'indépendance du Cyberespace (John Barlow, 1996). Dans ce manifeste cyber-exceptionaliste, l'absence de régulation gouvernementale sur Internet dans le cyberespace est prônée, du fait que les juridictions étatiques seraient dans l'impossibilité de traiter les cas ayant lieu dans le cyberespace, de déterminer les responsables et de fonder leurs jugements sur des lois suivant les évolutions technologiques. Une évolution en faveur d'une approche multipartite de la souveraineté s'est toutefois développée, afin de mettre en place une autorégulation décentralisée, incluant les acteurs non-étatiques [e.g. Internet Governance Forums (IGF), Internet Corporation for Assigned Names and Numbers (ICANN)], et de développer des normes communes, consensuelles et inclusives. ; COUTURE/TOUPIN, p. 2319 : certaines études en matière de "*indigenous digital sovereignty*" visent également à remettre en question les dimensions coloniales et impériales de la souveraineté, telle que conçue dans une "vision classique" du droit international public.

[26] KAGERMANN et al. p. 13 ; COUTURE/TOUPIN, p. 2313 ; POHLE/THIELE, p. 6ss ; KALOUDIS, Index, p. 16.

[27] MOEREL/TIMMERS, p. 8 et références : "*the capabilities and capacities to decide and act autonomously on essential aspects of the longer-term future in the economy, society and democracy*" ; TAN et al., p. 4 et références : Dans le même sens, l'UE décrit la souveraineté numérique comme "*the ability to shape the digital transformation in a self-determined manner with regard to hardware, software, services, and skills. Being digitally sovereign does not mean resorting to protectionist measures or doing everything yourself. Being digitally sovereign means, within the framework of applicable law, making sovereign decisions about the areas in which independence is desired or necessary*". Le Ministère fédéral allemand de l'économie et de l'énergie la définit comme "*the possibility of independent self-determination by the state and by organisations' with regard to the 'use and structuring of digital systems themselves, the data produced and stored in them, and the processes depicted as a result*" ; DANET/DESFORGES, p. 179ss ; SCHMITZ/SEIDL, p. 12.

[28] CHRÉTIEN/DROUARD, p. 15ss ; DANET/DESFORGES, p. 184 ; MOEREL/TIMMERS, p. 8.

[29] La notion "d'autonomie stratégique" semble donc remplacer celle de "souveraineté étatique" dans un contexte démocratique et libéral, par exemple dans les politiques européennes qui visent un marché unique de plus en plus géopolitisé et numérisé. Cf. MOEREL/TIMMERS, p. 8 et DANET/DESFORGES, p. 180 ; A ce titre, SCHMITZ/SEIDL proposent d'examiner cette problématique notamment sous le prisme des difficultés à concevoir et à mettre en œuvre des politiques visant à accroître l'autonomie stratégique et la souveraineté numérique de l'Europe, étant donné la dépendance omniprésente à l'égard de la capacité et de la coopération du secteur privé. Cf. SCHMITZ/SEIDL, p. 31.

[30] Certaines recherches abordent aussi d'autres dimensions de la souveraineté, telles que la "souveraineté des réseaux", "souveraineté de l'information", "souveraineté des plateformes et des infrastructures". On ajoutera encore la "souveraineté économique" et la "souveraineté énergétique" vues les problématiques actuelles géopolitiques respectivement énergétique et de développement durable. Cf. not. KAGERMAN et al. ; POHLE/THIEL ; SEIFRIED/BERTSCHEK ; TAN et al. ; CAPGEMINI, The journey to cloud sovereignty, 2022 ; Voir aussi SWISS DATA ALLIANCE, 2, indiquant que "souveraineté numérique" a plusieurs connotations et que la "souveraineté des données" est centrale.

[31] FABIANO, p. 272 ; BERTANI et al., p. 7.

autonomes, tout en respectant les normes sécurité et les réglementations[32]. Pour analyser la souveraineté technologique, certaines autrices et auteurs proposent d'abord d'identifier les technologies essentielles ("*key enabling technologies*", KET) qui créent des dépendances, avant d'analyser le champ d'action décisionnel et opérationnel de l'entité en vue d'une utilisation souveraine[33].

Pour l'État, la souveraineté technologique passe par la mise en place d'une **infrastructure numérique** publique et parapublique autonome et respectueuse des réglementations locales, ainsi que l'élaboration de stratégies et de politiques de transformation numérique de l'administration publique (dont des services publics à destination de la population, *cyberadministration*)[34]. Cela passe aussi par un **volet sécuritaire** et défensif afin de lutter contre la cybercriminalité et de protéger les infrastructures nationales critiques[35]. Cela passe enfin par l'élaboration d'une **politique industrielle** destinée à stimuler l'innovation et renforcer les compétences locales en matière de TIC[36].

La **souveraineté des données** désigne le droit et la capacité des individus et des organisations (administration, industrie, société civile) à contrôler et à utiliser de manière autodéterminée les données[37]. Elle implique donc un contrôle sur les données personnelles et non-personnelles stockées et traitées, dont les droits d'accès (sur une base contractuelle ou technologique)[38]. La souveraineté des données (contrôle sur les données) est devenue centrale dans une société ultra-connectée vus les enjeux de sécurité et de confidentialité[39]. Elle consiste particulièrement en la tentative par les États d'assujettir les flux de données à leurs réglementations, voire leurs juridictions nationales[40]. Les données étant des actifs stratégiques, les États cherchent également à minimiser les ingérences étrangères sur les données étatiques ou privées, sensibles ou stratégiques (e.g. par des méthodes d'espionnage). Dans un but de protection contre les activités de renseignement et d'attractivité de la place économique suisse, le concept de "*cloud suisse*" a notamment émergé dans les milieux politiques[41], concept qui a évolué ensuite vers la notion de "*cloud souverain*" (qui pose la question de savoir si l'on peut rester souverain lorsque l'on utilise un *cloud* qui est en partie ou en totalité localisé hors de Suisse).

Le **Cloud souverain** peut être ainsi défini comme un environnement de *cloud computing* contrôlé, déployé et/ou géré localement au sein d'une seule juridiction. L'idée est que l'organisation utilisatrice garde un contrôle sur les données, systèmes et applications. Les exigences varient selon le degré de

---

[32] Cf. *infra* III.3 ; COUTURE/TOUPIN, p. 2317 ; Dans son rapport, AWK définit la souveraineté technologique comme "*la capacité d'autodétermination d'une entité (légale) en ce qui concerne tout le cycle de vie d'un système numérique – de la conception à l'utilisation et au décommissionnement – et des données qui sont traitées et stockées ainsi que des processus qu'ils représentent*". ; En Allemagne, huit couches technologiques ont été identifiées à titre de champs d'action en matière de souveraineté technologique : (0) Matières premières et biens intermédiaires, (1) Composants, (2) Infrastructures de communication (3) Infrastructure à la demande (IaaS), (4) Plateforme service (PaaS), (5) Espaces de données, (6) Technologies logicielles, et (7) le système juridique et de valeurs. Voir KAGERMAN et al., p. 10.

[33] CHRÉTIEN/DROUARD, p. 23ss ; MAURER et al. ; ILLGNER, p. 8 ; KALOUDIS, Action plan, p. 7ss, rappelant qu'il convient aussi de tenir compte de l'accès aux matières premières et aux connaissances nécessaires et mettant en évidence six étapes pour identifier les KET (1) Définition des KET en étroite collaboration entre la politique, la recherche et l'industrie, (2) Développement des KET et coopération correspondante de la recherche et de l'industrie, au niveau national, européen et international, (4) Capacité à évaluer la technologie et son intégration dans les écosystèmes existants en mettant l'accent sur la fiabilité et la sécurité, (5) Évaluation des risques également des chaînes d'approvisionnement, (6) Transparence des architectures de systèmes, des interfaces associées, de l'échange et du stockage des données, et (7) Choix des technologies, architectures et fournisseurs. A titre de KET, les technologies suivantes peuvent notamment être envisagées : la construction de câbles sous-marins, le routage des données localisé sur le territoire, les systèmes nationaux de courrier crypté, le stockage territorial et local des données, y compris pour les services de *cloud*, ou les technologies de cryptage propres.

[34] Cf. *infra* III.4 ; POHLE, p. 14 ; CRESPI et al., p. 349 : La souveraineté technologique est définie comme "*the ability of a country (or a group of countries) to generate autonomously technological and scientific knowledge or to use technological capabilities developed outside through the activation of reliable partnerships*". Précisons que, selon nous, le choix de ne pas numériser est aussi un choix valide dans une perspective de "souveraineté étatique", qui est certes plus coûteuse et moins efficace, mais plus sécuritaire.

[35] Cf. *infra* III.5 ; POHLE, p. 14 ; POHLE/THIELE, p. 55.

[36] *Ibid*.

[37] Cf. *infra* III.2 ; GOLLIEZ, p. 83 ; CELESTE, p. 7 ; KALOUDIS, Action plan, p. 6.

[38] On distingue parfois trois axes de souveraineté des données : l'utilisation des données non personnelles au plus grand nombre possible d'acteur·ice·s ("*open data*"), l'utilisation de données personnelles par les personnes concernées ("*my data*") et le partage des données sensibles entre entreprises et administrations dans le respect de conditions strictes ("*shared data*"). Voir GOLLIEZ, p. 83.

[39] Cf. *infra* III.5 ; TAN et al., p. 2.

[40] COUTURE/TOUPIN, p. 2312 ; concernant l'extraterritorialité des lois, voir *infra* III.3.a. A ne pas confondre avec la notion de "*data residency*".

[41] DFF/UPIC, Rapport Swiss Cloud, p. 22ss : dans le cadre de l'étude Swiss cloud, les expert·e·s ont mis l'accent, en cas de besoin de protection spécifique, sur la satisfaction des caractéristiques suivantes : "*(1) le fournisseur est majoritairement en mains suisses et ne dépend pas économiquement d'autres pays dans lesquels il exerce son activité, (2) les données sont traitées uniquement en Suisse, (3) il n'existe pas d'obligation de communiquer les données à des tiers autres que des membres du système judiciaire suisse, dans le cadre de la protection juridique correspondante et (4) l'organisation est soumise au droit suisse et a son for en Suisse*".

contrôle : pour certains, le prestataire, les données, les systèmes et/ou les applications doivent être gérés localement ; pour d'autres, il suffit que les données soient inaccessibles depuis l'étranger. Il existe ainsi différents degrés de souveraineté selon les 3 composantes suivantes : *(i)* souveraineté des données (contrôler qui détient et accède aux données) indépendamment de leur localisation ou moyennant le stockage des données sur un seul territoire (*résidence des données*), *(ii)* souveraineté opérationnelle (contrôler les opérations sur les services, dont la continuité des opérations et la conformité réglementaire), *(iii)* souveraineté technique (exécuter soi-même les opérations sans dépendre d'un fournisseur)[42]. Stratégiquement, il est ainsi recommandé de définir les objectifs et le degré de souveraineté souhaité sur la base de ces 3 composantes ainsi que de les évaluer continuellement selon ses besoins et les développements.

c) Territoires (strates)

Les technologies évoluent dans un contexte de réseau mondial de communications interconnectées dépourvu de territoires géographiques bien définis (ou de limites spatiales)[43]. On glisse donc d'une approche de "souveraineté territoriale" vers une notion de "souveraineté sur les réseaux"[44].

Ces réseaux (nouvelles formes de territoires) sont composés de **plusieurs strates** sur lesquelles l'État peut exercer son autorité : (1) **strate physique** (composants TIC et capacités techniques localisées sur un territoire spatial) (2) **strate logique** (codes et normes régissant les composants TIC, rendant possibles l'échange d'informations entre eux) et (3) **données** circulant sur les réseaux[45]. Le degré de souveraineté s'appréciera selon la capacité de l'État à contrôler chaque strate, laquelle dépendra notamment de la localisation des données ou de l'accès aux données, de la nature et de l'étendue des liens du prestataire de services avec l'État en question[46]. L'État peut exercer une souveraineté **exclusive sur la 1ère strate** (physique) et une souveraineté **limitée** sur les 2ème et 3ème strates (logique et données) qui sont dépourvues de limites spatiales[47].

Ce rapport définit la souveraineté numérique comme le développement d'une autonomie stratégique en matière de numérique. Il s'agit du droit et de la capacité des entités politiques à pouvoir utiliser et contrôler de manière autonome (i.e. de manière indépendante et/ou autodéterminée) les biens matériels et immatériels et les services numériques qui impactent significativement la démocratie, l'économie et la société.

---

[42] CAPGEMINI, The journey to cloud sovereignty, 2022 : ce rapport parle de *continuum* de cloud souverain et distingue plusieurs catégories de cloud (du moins au plus souverain): *(i) Public Cloud* (sans prestataires locaux et sans restriction quant aux juridictions depuis où les services sont déployés), *(ii) Hybrid Cloud* (sans prestataires locaux mais avec des centres de calculs préalablement approuvés), *(iii) Cloud open source* (pour les logiciels et/ou les composants d'origine étrangère), *(iv)* Cloud privé (i.e. prestataires et données purement locaux), *(v)* Cloud totalement privé (*full in-house private cloud*) (i.e. prestataires, données et composantes locaux).

[43] COTTIER, Cyberespace, p. 205ss ; ROGUSKI, p. 5 : la localisation des composants du réseau est généralement imperceptible pour les utilisateur·ice·s du cyberespace, de sorte que la notion de territoire s'en trouve modifiée ; SAVIN, rappelant que la notion de territorialité (spatiale) n'est plus adaptée aux réalités des platetormes qui sont globales.

[44] VATANPARAST considérant que les lois glissent aussi du principe de territorialité vers l'extra-territorialité et tentent de "reterritorialiser" les données avec des exigences de localisation des serveurs et responsables du traitement, de sorte que l'on peut parler "d'élasticité de la souveraineté" consistant pour une juridiction d'étendre son pouvoir sur le transfert des données ; CHAPDELAINE/MCLEOD ROGERS, considérant que le concept de souveraineté numérique consiste pour une juridiction de promouvoir les intérêts individuels et collectifs de ses citoyen·ne·s localement et globalement.

[45] Cf. ROGUSKI, p. 5, présentant ces nouvelles formes de territoires à 3 strates (strates physiques, sociales et logiques) et à 5 strates (strates géographique, physique, logique, des cyberpersonnes et des personnes) ; OPEN SYSTEMS INTERCONNECTION (OSI) Model, distinguant 7 strates (physique, liaison de données, réseau, transport, session, présentation et application). Cf. aussi DUCHEINE, p. 458 et GOLDMAN, p. 17-1 ; SHEIKH, p. 6, distinguant 7 strates (ressources, chips, réseau, cloud, intelligence, application, objets connectés).

[46] *Ibid*.

[47] Ce sous réserve d'une nationalisation du cyberespace (e.g. Chine et Russie). Concrètement la "strate logique" touche notamment à l'attribution des adresses IP et des noms de domaine, ainsi qu'à l'administration des serveurs racine du DNS. Actuellement, ces aspects sont autorégulés par l'ICANN, qui fonctionne sur un modèle multipartite. Voir ROGUSKI, p. 10ss.

d) Acteurs

En vue du développement d'une autonomie stratégique en matière de numérique, les stratégies politiques et réglementaires peuvent porter sur les différents acteurs de l'écosystème numérique, en particulier les entités étatiques publiques et parapubliques, l'industrie et la société civile, chacune exerçant des rôles différents et représentant des leviers de gouvernance et de régulation[48].
Les **entités publiques et parapubliques** sont les premières actrices concernées. Les États cherchent à étendre leur autorité et leur champ d'action sur les actifs numériques (i.e. TIC et données), soit à exercer leur souveraineté dans ses dimensions interne et externe[49]. De par les fonctions régaliennes et régulatrices de l'État, les acteurs publics et parapublics jouent un rôle clé dans la protection des infrastructures étatiques ou critiques, de la population et de l'industrie[50].

L'**industrie** a aussi un rôle déterminant dans l'autonomie stratégique d'un État, du fait que les entreprises technologiques influencent l'innovation et génèrent des compétences[51]. Elles sont par ailleurs allocatrices de ressources numériques, voire détentrices d'une souveraineté de fait[52].

La **société civile** constitue un levier de gouvernance et de régulation incontournable au sein d'un système démocratique. En effet, de par ses choix politiques et économiques (e.g. exercice de droits citoyens, formation, choix d'utilisation et de consommation), elle façonne les fondements et l'avenir numérique d'une nation[53].

On parle de "souveraineté faible" lorsque ces questions sont menées par le secteur privé (e.g. sous forme d'auto-régulation) et de "souveraineté forte" lorsqu'elles sont prises en charge par l'État en vue de la sauvegarde de la sécurité nationale (e.g. sous forme d'une réglementation stricte)[54]. On parle aussi de souveraineté interne, lorsque les règles et la politique se concentrent sur les processus internes et de souveraineté externe lorsqu'elles sont tournées vers l'international[55].

---

[48] COUTURE/TOUPIN, p. 2317 ; TÜRK et références ; LEWIS, p. 3 ; POHLE, p. 14 ; GUEHAM, p. 12. ; POHLE/THIEL, p. 8 ; CONNOLLY et ROSSI et al. et références. Il convient de déterminer le(s) modèle(s) de gouvernance du numérique pertinent(s) en déterminant notamment la légitimité et la transparence des processus de régulation, puis la responsabilité des acteurs. A ce sujet, voir WEBER R.
[49] Cf. *supra* I.3.a.
[50] FABIANO, p. 270 ; TAN et al., p. 5.
[51] Cf. *infra* II et III.3.c.
[52] Cf. *infra* II. Du fait que les *Big Tech* entrent en relation avec d'autres États et imposent leur gouvernance sur le cyberespace avec une population déterminée (les internautes), certains auteurs considèrent qu'elles remplissent les critères traditionnels de souveraineté et influencent le paysage géopolitique. Cf. BLANDIN-OBERNESSER, p. 95ss ; COTTIER, Privatisation, N 8. Pour la souveraineté de fait, il suffit de songer aux deux exemples suivants : (1) la collecte de statistiques sociales (e.g. données de mobilités d'Apple ou résultats de recherche sur Google) rend possible le déploiement d'une action régulatrice classiquement attribuée à l'action publique, par exemple dans les contextes de crise (e.g. alerte Google sur smartphone en cas de situation d'urgence dans une zone géographique) ou en termes d'encadrement de la liberté d'expression (e.g. modération des contenus sur les réseaux sociaux). (2) La collecte et l'analyse automatisée de données en quantité massive permettent d'anticiper les comportements des individus, et ainsi d'orienter les comportements individuels. Cf. ROUVROY/BERNS, DURAND et ZUBOFF.
[53] Cf. *infra* II, III.2 et 3. Concernant l'émergence d'une souveraineté individuelle dans le cyberespace, voir BOIZARD.
[54] Voir COUTURE/TOUPIN, p. 2313 et POHLE/THIELE, p. 6ss ; La souveraineté forte se manifeste souvent par une volonté offensive, voire autoritaire, de territorialiser l'écosystème numérique et de créer une forme d'autarcie numérique. Elle est souvent associée aux risques de balkanisation d'Internet et d'isolationnisme d'un État. Elle peut par ailleurs autant accentuer la protection des individus que les réprimer, ce qui dépendra des buts politiques menés. Voir CELESTE, p. 6, POHLE, p. 6 et KALOUDIS, Action plan, p. 7 ; Concernant les dérives autoritaires des politiques en matière de "souveraineté numérique", voir CHANDER/SUN, p. 283ss.
[55] BENDIEK/STÜRZER, distinguant entre la souveraineté interne et externe ; SWISS DATA ALLIANCE, appréhendant la "souveraineté numérique" sous l'angle international et se demandant comment la Suisse peut promouvoir ses objectifs (approche positive) et se prémunir des interventions d'autres acteurs (approche négative).

4. Initiatives en matière de souveraineté numérique

La souveraineté numérique fait l'objet de nombreuses initiatives, tant à l'international *(a)*, qu'à l'étranger *(b)* et en Suisse *(c)*.

a) International

Sans entrer dans le détail, on rappellera ici que la souveraineté numérique est devenue un enjeu majeur à l'échelle internationale, sachant que les différentes approches de souveraineté numérique participent à une fragmentation d'internet, ce qui peut freiner l'innovation (e.g. développement des technologies, telles que le web3)[56] et le partage des données au service du bien commun[57], et que certains appellent à renforcer la collaboration internationale afin de nuancer ces risques de fragmentation[58].

b) Etranger

Les initiatives en matière de souveraineté numérique varient selon les régions et les Etats. On peut identifier trois approches de souveraineté numérique : la 1ère centrée sur la liberté d'entreprise (e.g. aux États-Unis), la 2ème sur le contrôle des données et des technologies par l'État (e.g. en Chine), la 3ème centrée sur l'individu (e.g. dans l'UE)[59].

Les **États-Unis** ont une approche de la souveraineté numérique qui peut être qualifiée de "privée", où la liberté d'entreprise et la protection de la propriété intellectuelle prévalent et où le discours de souveraineté numérique est perçu comme une entrave au commerce et à l'innovation[60]. Les États-Unis prévoient toutefois plusieurs réglementations pour encadrer l'activité des entreprises (e.g. le FSA pour pallier les limites du *Fourth Amendment* et le *US Cloud Act* pour pallier la délocalisation des données d'entreprises américaines)[61]. Il existe aussi des projets législatifs en vue de réguler les géants du numérique (e.g. *Tech Antitrust Bill, White House Principles for Enhancing Competition and Tech Platform Accountability*)[62]. Il existe par ailleurs des stratégies de numérisation de l'administration, de l'économie et de la société qui visent à stimuler l'innovation et à améliorer les services étatiques (e.g. avec un usage sécurisé des données par les citoyen·ne·s)[63].

---

[56] Pour l'impact des restrictions au transfert des données, voir CORY/DASCOLI, indiquant que les mesures de localisation des données ont doublé en 4 ans à travers le monde. En 2017, 35 pays prévoyaient de tells restrictions, contre 62 aujourd'hui. ; Concernant l'impact de la souveraineté numérique sur les technologies *blockchain*, voir GANNE, p. 101.

[57] On peut songer aux barrières au partage des données de santé pendant la crise covid-19. A ce propos, voir l'article précurseur de HARARI Yuval, The World After Coronavirus, *in* Financial Times, 20 mars 2020.

[58] DIPLOFOUNDATION, *op. cit.*, concluant que la fragmentation d'internet peut être évitée, notamment en renforçant la confiance du public dans l'utilisation d'internet, en adoptant des standards (e.g. IPv6 et IDNs), en clarifiant l'impact des nouvelles lois sur l'architecture d'internet et en renforçant la collaboration internationale pour des normes et standards internationaux et pour une coordination entre États et organisations internationales (e.g. ICANN, UIT et IGF) ; INTERNET SOCIETY considère que les politiques de souveraineté numérique affectent le fonctionnement d'internet et recommandent aux décideurs et décideuses politiques de procéder à des analyses d'impact d'internet (*Internet Impact Assessment*) comme mesures de leur stratégie numérique. Cf. INTERNET SOCIETY, *op. cit.*

[59] Cf. DETEC/DFAE, p. 35, résumant ces 3 approches à propos d'une politique nationale de données. ; INTERNET SOCIETY, *op. cit.* ; Cf. BENDIEK/STÜRZER, distinguant 2 modèles de souveraineté numérique, entre des modèles de souveraineté numérique dits "ouverts" caractérisés par une distribution du pouvoir entre une multitude d'acteurs (e.g. États-Unis, Europe) et "fermés" caractérisés par une centralisation du pouvoir sur le numérique (e.g. Chine). Pour d'autres juridictions, voir ERGAS/BRANIGAN (Australie), YEN (Taïwan), YUGUCHI (Japon).

[60] Alors que le "discours de souveraineté" est souvent absent dans les situations où l'autorité est incontestée – ce qui correspond le mieux à la définition substantielle de la souveraineté – le discours de la souveraineté apparaît plus fortement lorsque l'autorité est faible. Voir COUTURE/TOUPIN, p. 2310 et CHANDER/SUN, p. 283.

[61] Le *Fourth Amendment* permet aux autorités judiciaires américaines d'accéder aux données stockées sur le territoire des États-Unis, dans le cadre d'une procédure judiciaire. Le *US Cloud Act*, de par son effet extraterritorial, permet aux mêmes autorités de demander aux entreprises états-uniennes la production des données en leur possession et situées à l'étranger. Voir CHANDER/SUN, p. 283ss.

[62] Voir notamment NYLEN Leah, Tech Antitrust Bill Threatens to Break Apple, Google's Grip on the Internet, *in* Bloomberg, 26 juillet 2022 ; SHEPARDSON David / BOSE Nandita, White House unveils principles for Big Tech reform, *in* Reuters, 8 septembre 2022 ; KOLLER Rodolphe, La Maison blanche énonce des principes pour protéger les utilisateurs sans règlementer l'IA, *in* ICTJournal, 5 octobre 2022.

[63] Dans cette optique, les buts visés sont de permettre aux citoyen·ne·s américains de mieux exploiter les données gouvernementales pour stimuler l'innovation à travers la nation et améliorer la qualité des services pour le peuple américain, s'assurer qu'ils saisissent l'opportunité d'acquérir et de gérer des appareils, des applications et des données intelligents de manière sûre, sécurisée et efficace, puis libérer le pouvoir des données et être prêt à fournir et à recevoir des informations et des services numériques à tout moment, en tout lieu et sur tout appareil. Voir FEDERAL TRADE COMMISSION, Digital Government Strategy (site web) ; U.S. DEPARTEMENT OF STATE, Digital Government Strategy (site web) ; U.S. DEPARTEMENT OF COMMERCE, Digital Strategy (site web) ; U.S. AGENCY INTERNATIONAL DEVELOPMENT, Digital Strategy

La **Chine** a une approche de la souveraineté numérique qui peut être qualifiée de "centralisée", où le contrôle des données par l'État prévaut[64]. La stratégie numérique vise par ailleurs une souveraineté d'internet et un statut de puissance numérique et industrielle (e.g. *Great Firewall*, *Digital Silk Road*)[65]. La Chine semble par ailleurs privilégier une gouvernance multilatérale au multipartisme[66]. Par exemple, elle renforce des grands projets d'infrastructures, des collaborations de recherche dans des domaines stratégiques (e.g. 6G, circuits intégrés, intelligence artificielle) et les normes chinoises (e.g. flux de données transfrontaliers, lutte contre les monopoles, yuan numérique et protection de la vie privée)[67].

L'**UE** a une approche de souveraineté numérique qui peut être qualifiée de "centrée sur l'individu", où l'autonomie individuelle et les droits humains sont centraux (e.g. vie privée, liberté d'expression)[68]. La souveraineté numérique est principalement envisagée dans le renforcement des capacités européennes "indigènes", en particulier dans ses dimensions d'infrastructures et de plateformes *cloud* (appelées aussi "*cloud souverain*")[69] ainsi que dans le développement de la cybersécurité et de l'intégrité des données[70]. L'efficacité du *cloud souverain* est toutefois relativisée par la portée extraterritoriale de lois étrangères (e.g. *US Cloud Act*)[71]. Au niveau stratégique, elle se concentre sur l'intelligence artificielle d'une part et les données d'autre part[72]. Au niveau réglementaire, elle vise à créer des normes permettant l'émergence de standards globaux (e.g. RGPD à effets extra-territoriaux) et de limiter l'accès au marché européen pour les entreprises non européennes (p.ex. en contrôlant l'accès aux données)[73]. Au niveau national, plusieurs États membres (e.g. Allemagne, France) suivent la même approche centrée sur le modèle social national et les valeurs européennes (liberté, tolérance et solidarité), certains ayant une réelle politique de souveraineté numérique[74]. De manière générale, on observe enfin que l'UE pousse à s'émanciper de la technologie étrangère en créant des "champions" européens, tandis que des pays plus petits ou plus libéraux veulent bénéficier des meilleures technologies disponibles.

Factsheet (site web) ; OFFICE OF MANAGEMENT AND BUDGET / CDO COUNCIL / GENERAL SERVICES ADMINISTRATION, Federal Data strategy (site web).

[64] DETEC/DFAE, p. 35; NANNI, p. 2342.

[65] SHI-KUPFER/OHLBERG, p. 15ss ; HONG/GOODNIGHT, p. 8 ; CHANDER/SUN, p. 295ss ; CREEMERS, p. 110ss ; ROBERTS et al., p. 19.

[66] CHANDER/SUN, p. 295ss.

[67] *Ibid* : ces réglementations s'inspirent de règles internationales et étrangères. ; WU Yi, Understanding China's Digital Economy: Policies, Opportunities, and Challenges, *in* China Briefing, 11 août 2022.

[68] BAISCHEW et al., p. 63ss ; CELESTE, p. 8ss ; BARRINHA/CHRISTOU, p. 362, indiquant que le concept de souveraineté numérique est apparu pour la 1ère fois expressément dans le domaine de la cybersécurité, en particulier dans la stratégie européenne de décembre 2020 sur la cybersécurité.

[69] Comme exemple de cloud souverain européen, on mentionnera le projet Gaïa-X lancé en 2020 et dont le 1er catalogue dévoilé fin 2022 propose 176 services cloud fédérés et certifiés par un label, divisé en trois niveaux, dont le dernier garantit une immunité aux législations non-européennes à portée extra-territoriale. Comme projets de certification, on mentionnera la certification cloud (EUCS) délivrée par l'ENISA ou "*SecNumCloud* " délivrée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), garantissent un niveau de cybersécurité, la localisation et le traitement des données dans l'UE, ainsi que l'immunité à l'extra-territorialité des lois étrangères. Le projet Gaia-X fait l'objet de critiques du fait de la possible participation d'acteurs extra-européens, américains et chinois, jusqu'au sein de son conseil d'administration. Cf. LUZEAUX ; BÜCHEL/ENGELS ; BAUR, p. 19ss ; RAMOS et al. (Étude Greenberg Traurig), rappelant que lorsque les données sont hébergées et traitées dans l'UE, le "risque Cloud Act" ne peut être évité qu'en ayant aucune relation ou contact avec une entreprise américaine (e.g. avec une filiale américaine) ou, si elle a une relation d'entreprise avec une entreprise basée aux États-Unis, la société américaine ne doit pas avoir la possession, la garde, le contrôle ou la responsabilité de l'entité européenne. Rappelant aussi que, en termes d'organisation de l'entreprise selon la certification "*SecNumCloud*", le siège statutaire, administration centrale et principal établissement du prestataire doivent être établis au sein d'un État-membre de l'UE et le capital social et les droits de vote dans la société du prestataire ne doivent pas être, directement ou indirectement individuellement détenus à plus de 24 %, et collectivement détenus à plus de 39 %, par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement au sein d'un État non-membre de l'UE.

[70] TAN et al., p. 4.

[71] A ce sujet, voir RAMOS et al. (Étude Greenberg Traurig).

[72] Parmi les nombreux documents, cf. Annexe 1 (Tableaux) – Figure 14 pour des exemples de réglementations européennes ; PARLEMENT EUROPÉEN, Une stratégie numérique pour l'Europe ; COMMISSION EUROPÉENNE, Communication de la Commission au parlement européen, au Conseil, au Comité économique et social européen et au Comité, des régions, Une stratégie européenne pour les données, COM(2020) 66 final, Bruxelles, 19 février 2022 ; BURWELL/PROPP, p. 11, définissant les données et l'IA comme l'élément vital de la souveraineté numérique (*Lifeblood of Digital Sovereignty*).

[73] BURWELL/PROPP, p. 15.

[74] Par exemple, l'Allemagne et la France sont soucieuses de développer des compétences indigènes dans des domaines technologiques pertinents afin de faire contrepoids aux fournisseurs non européens et investissent dans certains domaines stratégiques (matériel (infrastructures et hardware), logiciels (applications et software), intelligence artificielle, cybersécurité, des plateformes numériques et des données). Pour l'Allemagne, voir BMWK, Façonner la transition numérique ; SEIFRIED/BERTSCHEK, p. 6ss ; LAMBACH/OPPERMANN, p. 7ss ; WEBER H., p. 155ss ; BURGFRIED/RECKERT-LODDE, p. 10 ; Pour la France, WOOD et al., p. 11 ; BAISCHEW et al., p. 63ss ; AUFRECHTER/KLOSSA, p. 11, rappelant qu'en 2006 déjà le Président Chirac a appelé les Européens à développer une capacité indigène de recherche d'informations pour répondre au "défi mondial posé par Google et Yahoo" et que dès 2010 le gouvernement français tirait la sonnette d'alarme sur la perte de souveraineté face aux entreprises technologiques étrangères.

c) Suisse

Comme vu précédemment, la souveraineté numérique intervient dans toutes les facettes de la vie numérique, en particulier dans le choix des infrastructures techniques (e.g. antennes de téléphonie mobile, réseaux de fibre optique) et des logiciels utilisés et du mode de stockage des données[75]. De manière générale, la question de la souveraineté s'inscrit dans les réflexions de transformation numérique de l'administration et, plus largement, celle de la société[76].

En Suisse, des politiques publiques du numérique ont déjà été envisagées, sans que la souveraineté numérique ou l'autonomie stratégique n'ait été clairement définie[77]. La Suisse étant un État fédéral, les réflexions sur la souveraineté numérique sont conduites à tous les niveaux des collectivités publiques. Au niveau fédéral, la réflexion sur la souveraineté numérique fait l'objet d'un nombre important de documents stratégiques[78]. Par ailleurs, de nombreux cantons et communes se sont aussi dotés d'outils de politique numérique[79], auxquels il convient d'ajouter les discussions qui se tiennent au niveau intercantonal[80]. Enfin, des réflexions sont menées dans d'autres cercles tels que le monde académique[81] et la société civile[82].

La difficulté de résoudre les différents enjeux de la souveraineté numérique peut être illustrée au moyen d'un cas concret, celui de l'infrastructure de données en nuages et des réflexions sur l'opportunité de créer une infrastructure helvétique.

Initialement, le Conseil fédéral avait lancé la réflexion sur l'opportunité de la création d'un nuage sous forme "d'infrastructure technique indépendante de droit public de nuage" (*Swiss cloud* ou *cloud souverain*)[83]. A l'issue de ce processus, cette stratégie a été très largement écartée, sauf pour certains domaines sensibles (telle que la mobilité en réseau)[84], au profit d'un renforcement du cadre légal[85]. Ultérieurement, ce dernier point a également fait l'objet d'une atténuation, la nécessité de créer un système de certification pour les services en nuage ayant été niée en raison de l'absence de besoin concret de réglementation et des systèmes de certification déjà existants[86].

---

[75] Voir *supra* I.2.b

[76] Cf. CONSEIL FÉDÉRAL, Message du 29 janvier 2020 sur le programme de la législature 2019 à 2023, FF 2020 1709, notamment p. 1767 : "*L'attrait que la Suisse présente pour les entreprises et la société dépend en grande partie de l'efficacité avec laquelle les prestations de l'État sont fournies. Aussi, pour répondre aux exigences d'aujourd'hui, les administrations publiques doivent-elles utiliser davantage les technologies numériques*".

[77] Il convient toutefois de distinguer les politiques publiques du numérique de la souveraineté numérique du fait que les premières sont déterminantes pour bâtir ou renforcer les capacités d'autonomie stratégique, sans que l'autonomie stratégique ne soit nécessairement clairement définie. Lorsque le concept de souveraineté numérique est évoqué, il se traduit par des discours ou politiques protectionnistes et autarciques en lien avec les dépendances des acteurs Suisses. La notion de dépendance concerne avant tout les données structurelles nécessaires à la puissance publique pour exercer ses prérogatives dans les domaines régaliens, économiques et concernant la protection des droits individuels et collectifs des citoyen·ne·s. Elle se réfère à "*la mesure dans laquelle les acteurs d'un pays donné doivent s'appuyer sur des technologies numériques contrôlées par des entités étrangères pour exercer des activités numériques*". Voir MAYER/LU, p. 5.

[78] Cf. Rapports du CONSEIL FÉDÉRAL, Stratégie suisse numérique 2023 ; Stratégie informatique de la Confédération 2020-2023, avril 2020 ; Stratégie informatique de la Confédération 2020-2023, avril 2020, Rapport sur l'évaluation des besoins d'un nuage informatique suisse ("Swiss Cloud"), septembre 2022) ; Cyberadministration, juillet 2020 ; Stratégie de politique extérieure numérique 2021–2024, novembre 2020 ; Rapport sur la création d'espaces de données fiables, sur la base de l'autodétermination numérique adopté le 30 mars 2022. Le gouvernement fonde sa compétence sur les articles 5 et 14 de l'OIAF, abrogée et remplacée dans l'intervalle par l'OTNI. La compétence du Conseil fédéral est dorénavant ancrée à l'art. 13 OTNI.

[79] A titre d'exemples, à Genève, la politique numérique pour Genève, p. 37ss et sur Vaud, la stratégie numérique, p. 35ss (les 2 documents rappellent l'importance de la souveraineté numérique). Pour des exemples de rang communal, à Genève, voir le Plan directeur de la transformation numérique 2021-2025. A Lausanne, voir les Lignes directrices relatives à la transformation numérique.

[80] Voir par exemple PRIVATIM, qui "*cherche, par l'échange d'informations continu, à favoriser la coopération entre les cantons, les communes et la Confédération*" et "*se veut l'interlocuteur des autorités et du public dès qu'il s'agit de protection des données*". Voir aussi la CLDN qui a mené à la présente étude.

[81] Ainsi, l'Université de Genève a mis sur pied au printemps 2022 un Groupe de réflexion "Souveraineté numérique de l'UNIGE". Celui-ci s'est déjà réuni à trois reprises et a notamment réfléchi à la rédaction d'une Charte de bonnes pratiques.

[82] Voir par exemple la SWISS DATA ALLIANCE, qui regroupe des entreprises, des associations professionnelles, des organisations de la société civile, des institutions de recherche et des individus pour établir une politique des données en Suisse orientée vers l'avenir.

[83] Cf. DFF/UPIC, Rapport Swiss Cloud, p. 4, observant au passage que la pratique numérique a changé au point de donner la priorité à la solution en nuage (*cloud first*) par rapport à une solution de stockage localisée. A noter que d'autres gouvernements (e.g. français) préconisent aussi la doctrine du cloud first (ou "cloud par défaut" ou "cloud au centre"). Cf. GOUVERNEMENT FRANÇAIS, Stratégie nationale pour le cloud, 2 novembre 2021.

[84] Cf. Rapport postérieur sur la création d'un espace de données fiables du DETEC/DFAE, p. 41.

[85] Cf. DFF/UPIC, Rapport Swiss Cloud, p. 32.

[86] CHANCELLERIE FÉDÉRALE, Informatique en nuage (site web).

Toutefois, ces orientations stratégiques ne font pas l'unanimité au sein des autorités politiques fédérales, comme le montre le fait qu'en septembre 2021, une initiative parlementaire identique déposée au sein des deux Chambres de l'Assemblée fédérale demandait la création d'une infrastructure numérique souveraine (*cloud souverain*) pour renforcer la cybersécurité et la souveraineté suisse[87]. En février 2022, la Commission de la politique de sécurité du Conseil national a décidé de lui donner suite, tandis qu'en août 2022, son alter ego du Conseil des États a pris la position inverse[88].

Outre les orientations stratégiques, la question du respect du cadre juridique applicable oriente l'ensemble des discussions[89]. **Une première question**[90] porte sur **l'exigence d'une base légale** qui permettrait la délégation de la gestion des données des individus nécessaires à des fins administratives[91]. C'est en raison de doutes sur l'existence d'une base légale suffisante que le TF a récemment renvoyé au TAF le dossier de l'adjudication de marchés de *cloud* à des prestataires privés dont une partie des centres de données sont situés à l'étranger[92]. Dans ce cadre, la question de l'accès en tout temps aux données se pose et recevra une réponse différente selon si celles-ci sont stockées exclusivement en Suisse, à l'étranger avec une copie en Suisse ou exclusivement à l'étranger[93].

Une **deuxième question**[94] est de savoir si le recours à des services *cloud* respecte les exigences de la nLPD. Sur ce point, les autorités publiques en Suisse ont émis des opinions divergentes. Ainsi, le PFPDT a estimé dans une prise de position du 13 mai 2022 que le recours au cloud M365 (pour des services *Outlook* et *Teams*) pour la Caisse suisse d'assurance-accidents (SUVA) est contraire à la LPD même si les données sont hébergées en Europe au motif qu'il existe un risque résiduel que les autorités américaines accèdent aux données sur la base du *US Cloud Act* (**approche fondée sur le risque zéro**)[95]. A l'inverse, le **Conseil d'État zurichois** a estimé dans une décision du 30 mars 2022 que le recours au *cloud* M365 pour l'administration cantonale zurichoise est licite au motif que le risque est faible lorsque des mesures additionnelles sont prises (**approche fondée sur le risque**)[96].

---

[87] Cf. Initiative parlementaire fédérale n° 21.495 de MORET Isabelle "Cybersécurité. Mise en place d'une infrastructure numérique souveraine et de standards de sécurité de gouvernance".

[88] *Ibid*.

[89] Voir DFF/UPIC, Rapport Swiss Cloud, p. 43 : Le rapport Swiss Cloud, formulant plusieurs questions, dont celle de savoir dans quelle mesure les autorités suisses doivent suivre les mêmes directives que la CJUE dans l'arrêt *Schrems* qui soumet le transfert des données vers les États-Unis au RGPD ou au contraire s'il va suivre la nLPD. Cette question ne sera pas traitée en détail ici mais il est précisé, même si l'arrêt *Schrems II* ne déploie pas d'effet direct en Suisse et si les autorités suisses conduisent l'analyse à la lumière du droit suisse (LPD), le PFPDT a retenu que le *Swiss-US Privacy Shield* (l'équivalent du *EU-US Privacy Shield*) n'offre pas un niveau de protection suffisant et ne constitue donc plus un instrument permettant le transfert des données vers les États-Unis (communiqué du Préposé du 8 septembre 2020). Ainsi, même si les autorités suisses doivent appliquer le droit suisse, l'approche politique et juridique des autorités européennes (durcissement de la pratique des autorités européennes en matière de transfert vers les US et en attendant un accord remplaçant le *Privacy Shield*) influencent les autorités suisses, comme vu avec le recours au *Cloud* M365.

[90] Pour des réflexions sur cette question, voir *infra* III.4.

[91] La délégation de cette tâche qui constitue traditionnellement une tâche de l'État doit se fonder sur une base légale (art. 178 al. 3 Cst/CH ; art. 34 al. 1 nLPD. Ainsi, plusieurs lois fédérales et cantonales prévoient une base légale expresse autorisant des activités étatiques spécifiques, telles que les lois de protection des données (e.g. art. 12e LPrD/VD et art. 28 LCyb/FR autorisant la communication des données personnelles aux prestataires *cloud*) ou la loi LMETA prévoyant les bases légales pour la transformation numérique de l'administration fédérale) (FF 2022 804, p. 2 : "*La loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (LMETA) crée la base légale requise pour une transformation numérique efficace de l'administration fédérale ainsi que pour la collaboration entre les autorités de différentes collectivités et des tiers dans le domaine de la cyberadministration*").

[92] Voir Arrêt du TF 1C_216/2022 du 28 juillet 2022.

[93] Lors de la première vague de COVID-19, les frontières géographiques se sont à nouveau très fortement matérialisées et un développement similaire ne peut être exclu dans le monde numérique.

[94] Pour de plus amples réflexions sur cette question, voir *infra* III.2.

[95] Ce contrairement à la SUVA estimant le risque comme très improbable *höchst unwahrscheinlich*), ce certainement en raison du durcissement de la pratique des autorités européennes en matière de transfert vers les US et en attendant un accord remplaçant le Privacy Shield. À titre d'exemples, on peut citer les décisions strictes prises dans les affaires *Google Analytics* : la décision de l'autorité autrichienne de protection des données du 22 décembre 2021, la décision de mise en demeure de la CNIL du 10 février 2022 et plus récemment la décision de l'autorité italienne de protection des données du 9 juin 2022. De même, la chambre des marchés publics de Baden-Württemberg (Allemagne) a retenu dans une décision qu'un risque d'accès par les autorités américaines doit être analysé comme une communication effective. En effet, une décision négative quant à l'adéquation de la Suisse aurait des conséquences importantes sur l'économie suisse. Dans le même sens, voir le mémorandum commandé par Ministère de la justice des Pays-Bas, considérant que des entités européennes étaient soumises au *US CLOUD Act* même si elles étaient localisées en dehors des États-Unis. Cf. RAMOS et al. (Étude Greenberg Traurig).

[96] Le Conseil d'État a rappelé au passage qu'il n'était plus envisageable de recourir exclusivement à des services *on premise* sans se retrouver "technologiquement hors-jeu"). Pour le gouvernement zurichois, renoncer à Microsoft 365 signifierait donc se mettre hors-jeu en matière technologique et par rapport aux entreprises privées et aux autres collectivités publiques. Ainsi, ne pas aller dans le *cloud* présente des risques en matière de numérisation et de collaboration, de pérennité et de sécurité, et d'attractivité comme employeur. Voir REGIERUNGSRATES DES KANTONS ZÜRICH, Einsatz von Cloud-Lösungen in der kantonalen Verwaltung (Microsoft 365), Zulassung, 30 mars 2022.

La Chancellerie fédérale a récemment estimé, pour sa part, que les demandes d'accès aux données étaient très rares et que le risque d'accès indu aux données pouvait être fortement diminué par l'utilisation de mesures techniques, en particulier le cryptage des données avec une clé que seul l'utilisateur du *cloud* possède[97]. Privatim, la Conférence des Préposé·e·s suisses à la protection des données, a identifié cinq risques principaux liés à la technologie du *cloud* (conception du contrat, lieux des traitements des données, confidentialité et protection des secrets, données concernant les utilisatrices et utilisateurs des services et contrats de sous-traitance)[98]. Sur cette base, elle requiert que l'organe public responsable exclue ou réduise ces risques à un niveau acceptable par des mesures adéquates, faute de quoi il conviendra de renoncer au service *cloud*.

Une **troisième question** porte sur le respect d'autres règles juridiques, dont la protection des secrets (e.g. secret professionnel, tel que le secret de l'avocat protégé par art. 321 CP et art. 13 LLCA et le secret de fonction protégé par l'art. 320 CP) et les exigences des autorités de surveillance (e.g. FINMA)[99]. Sous l'angle du secret, le prestataire de services *cloud* (*CSP*) est considéré comme un auxiliaire, auquel les données peuvent être confiées sans levée du secret, pour autant que toutes les mesures soient prises pour éviter la violation du secret (contrat prévoyant des mesures techniques et organisationnelles, dont l'interdiction de sous-délégation et de limitation de responsabilité pour la violation du secret)[100]. Sous l'angle des exigences des autorités de surveillance (e.g. FINMA), la pratique tend à admettre le recours à des prestataires *cloud*, même à l'étranger, pour autant que des mesures techniques et organisationnelles permettent de respecter le secret et les autres exigences légales (e.g. accès aux données en tout temps).

Une **quatrième question** est de savoir comment **dissocier les données** personnelles et non personnelles dans le cadre du *cloud*, en particulier en cas d'application cumulative de plusieurs régimes légaux (e.g. protection des données personnelles et protection du droit d'auteur (possibilité de différenciation). Une solution est d'opérer un tri entre les différents objets et d'appliquer les différents fondements légaux et termes contractuels à chaque objet de la licence pris séparément. Si les objets de la licence sont indissociables au point de rendre le tri impossible, une solution est d'appliquer la protection des données personnelles à l'ensemble de l'objet par un phénomène d'absorption de la protection des données, notamment au vu de la nature personnelle et incessible des données personnelles[101].

Un consortium d'entreprises suisses propose une alternative aux prestataires étrangers choisis par la Confédération, afin de contrer la position monopolistique des entreprises choisies qui peuvent casser les prix avant de possiblement les augmenter après la fidélisation du client. Cette alternative indique permettre aussi d'éviter un écosystème fermé et des coûts indirects cachés (e.g. coûts de migration ou de services complémentaires de sécurité qui s'avèrent ensuite indispensables)[102].

---

[97] Cf. CHANCELLERIE FÉDÉRALE, p. 23ss. Sur ce rapport, voir GÖTZINGER.

[98] Cf. PRIVATIM, Aide-mémoire sur les risques et les mesures spécifiques à la technologie du Cloud, 17 décembre 2019.

[99] FINMA, Circulaire 2018/3, Outsourcing : Externalisations dans le secteur des banques, des entreprises d'assurance et de certains établissements financiers au sens de la LEFin, 21 septembre 2017, p. 6 : La FINMA exige par exemple que l'accès aux informations nécessaires à cet effet soit possible à tout moment en Suisse.

[100] En matière de secret professionnel de l'avocat, voir l'ATF 145 II 229 ; En matière de secret de fonction, voir DFF/UPIC, Rapport Swiss Cloud, p. 27ss, estimant que le recours à des services en nuage peut être conforme au secret de fonction pour autant que les relations entre les parties – notamment contractuelles – permettent de tenir compte des exigences légales.

[101] Cette solution de protection des données "par défaut" est préconisée par le Régulateur européen, voir COMMISSION EUROPÉENNE, Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, 2019, § 2.2 ; BENHAMOU Y., RSDA, p. 393ss, 414, comparant cette situation avec l'effet "contaminant" des licences la licence GNU GPL qui soumettent l'ensemble du logiciel à la licence libre lorsqu'un bout de code sous licence libre est inséré dans un logiciel propriétaire.

[102] INFOMANIAK, Cybersécurité et souveraineté numérique : réponses aux questions que nous recevons avec Solange Ghernaouti, *in* InfomaniakNews, 7 mars 2022.

II. Enjeux socio-économiques

La souveraineté numérique est un concept utilisé de multiples façons. Toutes renvoient cependant à une signification centrale : dans quelle mesure une entité politique est-elle en capacité de contrôler la strate matérielle (équipements réseaux, terminaux), la strate logicielle et les données (stocks et flux) qui constituent l'écosystème numérique[103]. Cette question du contrôle des strates se pose du point de vue des différents acteurs, en particulier de sécurité nationale, de développement économique et la capacité des autorités à préserver les droits des individus et leur autonomie d'action individuelle et collective. Ces trois dimensions de la question de la souveraineté numérique (régalienne, économique et citoyenne) dépendent des capacités plus ou moins importantes de superviser et de normer la conception et l'utilisation des technologies et des données[104]. Ces capacités sont elles-mêmes directement fonction des capacités suisses en matière de TIC *(1)*, et de leur dépendance matérielle *(2)* et intellectuelle *(3)*[105].

1. Capacités suisses en matière de TIC

La Suisse se situe systématiquement dans le haut du classement des index évaluant le développement numérique et l'usage des TIC[106]. Cette évaluation repose sur des infrastructures, des services et des compétences développées au niveau national et qui jouent un rôle favorable pour l'innovation. Mais il s'agit **aussi d'une source potentielle de vulnérabilité** sociale, économique et politique. C'est le cas du domaine de la **cybersécurité**, domaine dans lequel la Suisse est considérée comme en retard en raison d'une législation peu développée et d'une préparation insuffisante de la puissance publique aux incidents majeurs[107]. C'est aussi le cas de l'omniprésence de **dispositifs technologiques étrangers**, soit des dispositifs produits, développées et/ou contrôlés à l'extérieur du pays. Il faut noter que cet engagement fort dans le développement des TIC a un impact sur l'emploi. Selon une étude récente, l'investissement dans les technologies numériques est corrélé à une augmentation d'emplois hautement qualifiés avec un effet positif net, en particulier pour les entreprises utilisant des technologies basées sur les machines (e.g. robots, impression 3D ou internet des objets), moins pour les entreprises non basées sur les machines (e.g. systèmes *entreprise resource planning* (ERP), commerce électronique)[108]. Il faut enfin noter que les technologies numériques sont aussi corrélées à un risque de délocalisation, amplifié avec les possibilités de télétravail et le contrôle à distance d'équipements, où la téléprésence permet de dissocier physiquement les services de main-d'œuvre des travailleurs[109].

Ainsi, la notion de souveraineté numérique implique de tenir compte du degré de dépendance d'un pays vis-à-vis du reste du monde en général et de certains pays en particulier en ce qui concerne les TIC. Cette dépendance ne saurait se réduire à une seule métrique et doit être saisie dans ses dimensions

---

[103] Cf. *supra* I.3.c ; CHANDER/SUN, p. 283 ; FLORIDI, p. 369ss ; FALKNER et al., p. 3.
[104] Cf. *supra* I.3.
[105] Pour la notion de "dépendance", cf. n. 8 et 69.
[106] La Suisse était 3ème en 2017, selon l'index de développement des TIC de l'Union internationale des télécommunications (UIT) qui combine 10 indicateurs évaluant les infrastructures d'accès au numérique, l'intensité des usages et les compétences. Elle est classée troisième également en termes d'usage des TIC selon l'indicateur synthétique proposé par le Global Competition Index 2017-2018. Cet indicateur est composé de la part de la population utilisant internet, la part de la population disposant d'un abonnement fixe internet haut débit, d'un abonnement mobile internet haut-débit et de la quantité de la bande passante mobilisée par utilisateur. La Suisse surperforme également par rapport à la moyenne des pays à haut revenu dans l'édition 2021 du du Network Readiness Index compilé par le Portulans Institut et ce dans l'ensemble des dimensions à savoir notamment les infrastructures, les usages privés et public, l'impact économique et la gouvernance des TIC. Voir UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS (UIT), ICT Development Index 2017 (site web) ; WORLD ECONOMIC FORUM (WEF), Global Competitiveness Index 2017-2018 (site web) ; PORTULANS INSTITUTE, Network Readiness Index, Switzerland (site web).
[107] La Suisse est 23ème dans l'édition 2021 du National Cyber Security index de la fondation estonienne e-Governance Academy. Voir EGOVERNANCE ACADEMY, National Cybersecurity Index (site web) ; SECTEUR TRANSFORMATION NUMÉRIQUE ET GOUVERNANCE DE L'INFORMATIQUE (TNI), Stratégie Suisse numérique (site web) : on notera que la Confédération fait actuellement de nombreux efforts pour améliorer la cybersécurité, notamment avec la transformation du NCSC en l'Office fédéral de cybersécurité, la création du Campus cyberdéfense et la mise en place de la Stratégie nationale de protection des infrastructures critiques 2018-2022. On peut également compter passablement de développements législatifs en cours (e.g. révision de la LSI pour créer une obligation de signaler les cyberattaques, OTNI, OPCy, LMETA). Pour le surplus, voir *infra* III.5. ; La *Trust Valley*, émanant d'une alliance entre des acteurs publics, privés et académiques s'est également créée, afin de développer un pôle de compétences lémanique et des technologies de pointe en matière de confiance numérique et de cybersécurité.
[108] BALSMEIER/WOERTER, p. 9.
[109] BALDWIN, p. 179ss.; cf. *infra* III.3.

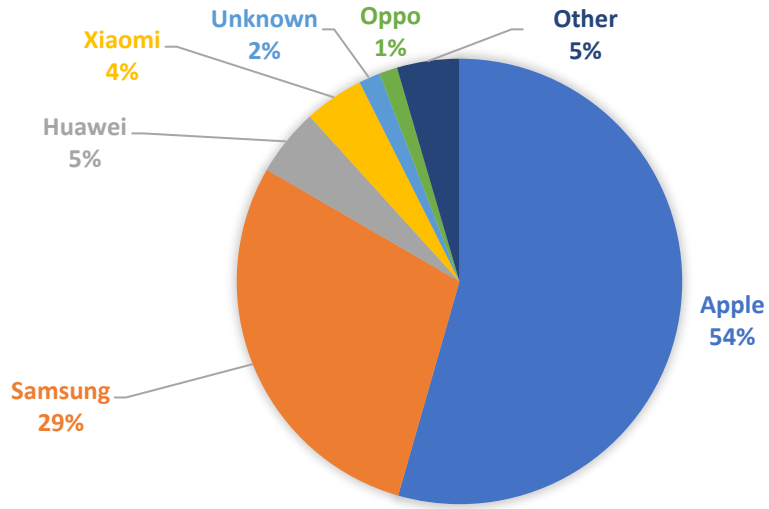
matérielles et intellectuelles[110]. Plutôt que de chercher un état inaccessible et non désirable d'autarcie, il s'agit de pointer les vulnérabilités et les problèmes potentiels qu'elles posent.

2. Dépendance matérielle

Le degré de dépendance matérielle de la Suisse dans le domaine du numérique peut être appréhendé d'une part à travers les **données d'utilisation** tirées des navigations sur Internet et, d'autre part, à travers les **échanges commerciaux**.

S'agissant des **données d'utilisation** (i.e. données issues des appareils, tels qu'ordinateurs, smartphones et tablettes sont utilisés depuis la Suisse), les études font apparaître une **dépendance totale vis-à-vis de l'étranger** en matière d'infrastructure matérielle[111] (Figure 1).

Figure 1. Parts de marché des fabricants de terminaux utilisés en Suisse en juillet 2022 (Source Statcounter)



S'agissant des **échanges commerciaux**, les études font aussi apparaître une **dépendance**. Les échanges de biens sont dominés par les importations qui en représentent 76% en 2021 (Figure 2). Le déséquilibre est particulièrement marqué pour les ordinateurs et périphériques grand public (entre 84 et 86%), tandis que les importations et exportations de composants électroniques sont presque équivalentes (Figure 6). Cela signale la puissance technologique de la base productive suisse dans les segments industriels sophistiqués, tels que les composants micro-électroniques, située en amont du secteur.

Sur le plan géographique, le commerce est dominé par les échanges avec la Chine qui à elle seule est à l'origine de 45% des importations de biens TIC en 2021, suivie de l'Allemagne (13%)[112]. Alors que les échanges avec l'Allemagne sont presque équilibrés, les importations de matériel chinois représentent

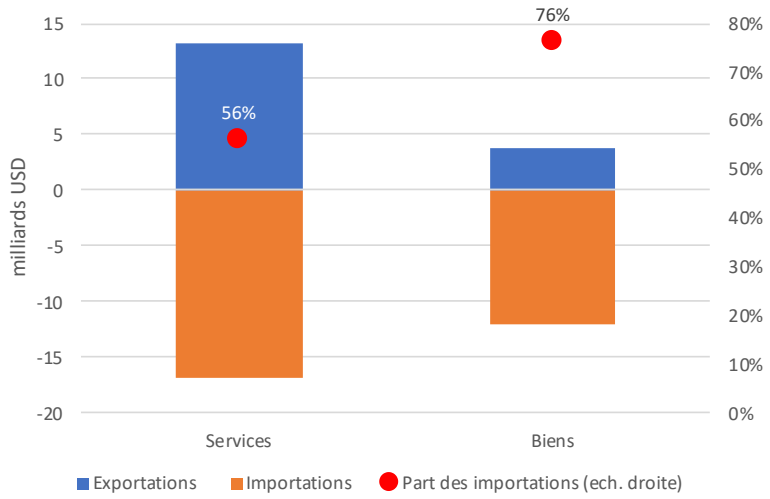
[110] La démarche suivie s'inspire librement de la méthodologie proposée pour construire l'indice de dépendance numérique. Celui-ci mesure le niveau de dépendance à l'égard de différents secteurs technologiques (par exemple, le matériel et les logiciels) de 23 pays. La Suisse n'en fait pas partie. Les principaux indicateurs portent sur le commerce des TIC, les infrastructures de communication et la propriété intellectuelle, c'est-à-dire les brevets. Voir LU/MAYER, p. 5ss.

[111] Apple domine avec une part de 54% des terminaux utilisés, suivi par le coréen Samsung (29 %) puis les chinois Huawei (5%), Xiaomi (4%) et Oppo (1%). Statcounter propose des estimations des parts de marché des navigateurs, moteurs de recherche, système d'exploitation, réseaux sociaux et fabricant de terminaux à l'échelle mondiale et par pays. Cette évaluation se base non pas sur des utilisateurs uniques, mais en proportion du nombre de pages internet consultées à partir de données collectées depuis 1,5 millions de sites. Voir STATCOUNTER GLOBALSTATS, Browser Market Share Worldwide (site web).

[112] Cf. UNCTAD, Handbook of Statistics 2021 (site web).

94% des échanges bilatéraux. Sur le plan matériel, le rapport de la Suisse à la Chine est donc à la fois important et très asymétrique[113].

Figure 2. Échanges commerciaux de biens et services des TIC entre la Suisse et le reste du monde en 2021 (Source UNCTAD)



3. Dépendance intellectuelle

Les enjeux de dépendance et de vulnérabilité ne se cantonnent pas aux aspects matériels, mais renvoient aussi aux aspects intellectuels (ou intangibles) encadrés par la propriété intellectuelle[114]. Il s'agit d'une problématique particulièrement sensible pour les services de l'état, y compris dans ses fonctions régaliennes, lorsqu'ils ont amené à faire appel à des prestataires étrangers pour des suites bureautiques, des logiciels spécialisés ou bien des audits spécifiques, y compris dans le domaine de la sécurité technologique. Pour le pays dans son ensemble, cette dimension du problème peut être aussi appréhendée à travers les **données d'utilisation** et les **échanges commerciaux**.

a) Infrastructure logicielle des usages d'internet dominée par l'étranger

S'agissant des **données d'utilisation**, les études font apparaître une dépendance totale vis-à-vis de l'étranger en matière d'infrastructure logicielle, qu'il s'agisse des outils de navigations ou des plateformes, avec une **domination des entreprises américaines**[115] (Figure 7). Sur le segment des moteurs de recherche, Google est en quasi-monopole avec 91% des usages, tandis que Bing de Microsoft ne pèse que 6% suivi de Duckduckgo et Yahoo avec 1% (Figure 8). Sur le segment des systèmes d'exploitation, Windows de Microsoft est leader (50%), suivi d'IOS et OSX d'Apple (32%) et d'Android de Google (16%) (Figure 9). Sur le segment des réseaux sociaux, l'usage est dominé par Meta avec Facebook (77%) et Instagram (4%) ainsi que Twitter (9%), Pinterest (5%) et Youtube (2%) (Figure 9). Pour être complet, il faut signaler la présence marginale d'autres acteurs comme le navigateur et moteur de recherche Yandex Russe, les moteurs de recherche européens Ecosia et Qwant, le chinois Baidu, le réseau social Vkontakte ainsi que Tumblr et Reddit basés aux États-Unis.

---

[113] La numérisation est une priorité thématique dans le cadre de la coopération sino-helvétique. En matière d'innovation, la Chine est à la fois perçue comme un pôle d'innovation majeur, mais également comme source de risque de dépendances technologiques, puis de menace pour le savoir-faire des entreprises suisses et pour l'exploitation commerciale de celui-ci. Dès lors, cette dualité et cette asymétrie se répercute sur les aspects stratégiques de sécurité, de gouvernance et d'accès au marché numérique ; un dialogue multilatéral avec la Chine via des plateformes et organismes internationaux est privilégié. Voir DFAE, Chine 2021-2024, pp. 28-29.

[114] Pour une introduction à la problématique des intangibles, voir HASKEL/WESTLAKE.

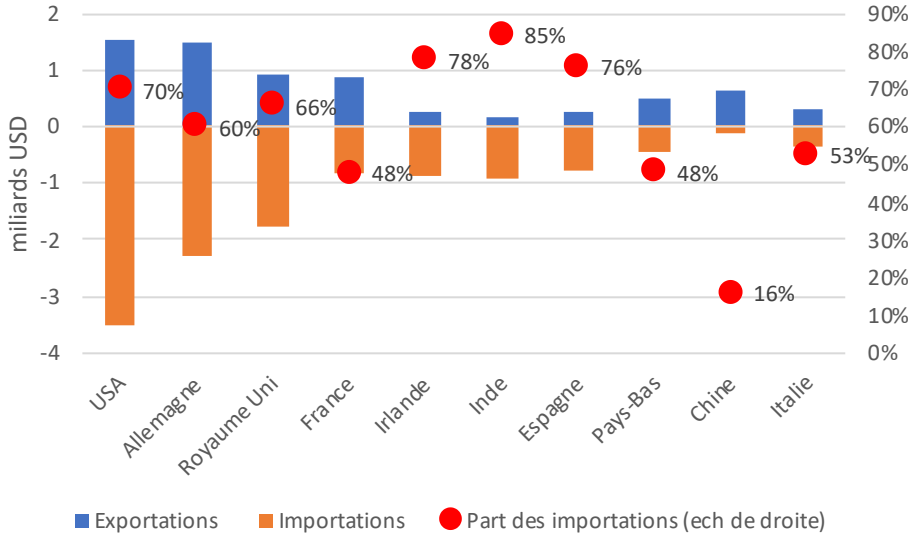
[115] Alphabet domine le marché des navigateur internet avec Chrome (55% des parts de marché), devant Safari d'Apple (21%), Edge de Microsoft (15%), Firefox de la fondation Mozilla (5%) et Samsun internet (3%). Voir données STATCOUNTER GLOBALSTATS, *op. cit.*

b) Échanges de services numériques relativement équilibrés

Les échanges commerciaux de services numériques (e.g. services informatiques, logiciels et télécommunications) permettent de nuancer la domination des usages d'Internet. Ils sont en effet moins déséquilibrés. Au niveau global, les importations de services numériques ne représentent que 56% des échanges de ces produits, contre 76% pour les biens TIC (Figure 2). Ils représentent par ailleurs des montants deux fois plus importants que les échanges de biens (30 milliards contre 15 milliards en 2021).

Ils sont également plus **diversifiés géographiquement** (Figure 3). Les États-Unis sont certes le premier partenaire commercial et celui avec lequel les échanges sont les plus déséquilibrés (après l'Inde), mais ils ne pèsent que moins d'un cinquième des échanges suisses dans ce domaine. Les échanges sont aussi importants et plus équilibrés avec d'autres pays à haut revenu (e.g. Allemagne, France, Royaume-Uni ou Italie). Avec la Chine, les rapports sont cette fois inversés, puisque les exportations de la Suisse représentent 84% des échanges bilatéraux. Comme les montants sont beaucoup moins importants que pour les biens, cela ne suffit cependant pas à rééquilibrer la relation dans son ensemble.

Figure 3. Échanges commerciaux de services TIC entre la Suisse et ses principaux partenaires 2019 (Source OCDE)



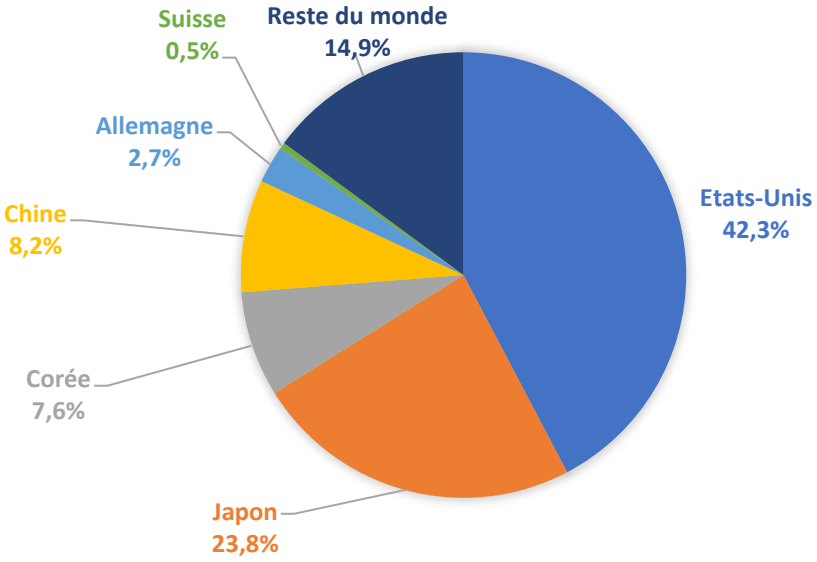
c) Monopolisation de la propriété intellectuelle à l'échelle globale

La dépendance intellectuelle d'un pays suppose de se projeter à l'échelle mondiale en matière de propriété intellectuelle[116]. Du fait d'une certaine harmonisation internationale, c'est à l'échelle mondiale que se définissent les limites que pose la propriété intellectuelle dans le champ du numérique aux acteurs situés en Suisse. Les données de l'OMPI sur l'enregistrement des brevets dans le domaine des TIC permettent d'évaluer la dépendance intellectuelle de la Suisse[117]. Étant donné la taille du pays, il n'est pas surprenant que la proportion des brevets octroyés par les principaux offices de propriété intellectuelle[118] à des entités basées en Suisse soit faible, soit de l'ordre de 0,5%. Mais même en proportion de la population, la **Suisse n'est pas parmi les plus actifs**, avec 117 brevets déposés par million d'habitants contre 411 pour le Japon, 341 pour la Corée, 268 pour les États-Unis mais seulement 69 pour l'Allemagne (Figure 11).

[116] L'économiste Ugo PAGANO définit le monopole intellectuel comme le "*monopole légal sur certains éléments de connaissance, qui s'étend bien au-delà des frontières nationales*" et qui "*limite la liberté de nombreux individus en de multiples endroits*". Voir PAGANO, p. 1413.
[117] Cf. Données sur les brevets par domaine accessibles via le WIPO, IP Statistic Data Center (site web).
[118] Il s'agit de l'office des brevets du Japon, des États-Unis et de l'Europe. On parle alors de brevets triadiques. Un grand nombre de brevets sont également enregistrés en Chine mais en raison de différences d'usages et de qualité, les prendre en compte risquerait de fausser la perspective mondiale adoptée ici.

Le fait essentiel est cependant ailleurs : la concentration de la propriété intellectuelle dans les domaines du numérique à l'échelle mondiale est une source de vulnérabilité pour la Suisse comme pour la plupart des pays. Les États-Unis comptent le plus de brevets déposés dans ce domaine dans le monde (42%), avant le Japon (23%) et la Corée du Sud (8%), ce qui représente trois quarts de la propriété intellectuelle dans ce domaine. La Chine et l'Allemagne représentent respectivement 8% et 3%, ce qui ne laisse que 15% pour le reste du monde (Figure 4).

Figure 4. Répartition des brevets octroyés dans le domaine des TIC par les principaux offices (Etats-Unis, Japon et Office européen) en 2020 (Source WIPO)



Cette dynamique se vérifie pour chacun des sous-domaines des TIC, qu'il s'agisse des aspects plus industriels avec les semi-conducteurs, les technologies audiovisuelles, les télécommunications aussi bien que dans les aspects les plus fondamentaux (e.g. oscillation, modulation, codage/décodage), les activités ayant directement trait à internet, à l'informatique ou aux outils numériques de management (Figure 12). Parmi ces domaines, la Suisse surperforme légèrement dans le champ des applications fondamentales, mais avec 0.9% des brevets déposés elle reste là aussi dépendante de la propriété intellectuelle détenue par des entités étrangères (Figure 13).

d) Montée en puissance de l'intelligence artificielle

Le développement d'algorithmes apprenants et adaptatifs a des implications majeures du point de vue des rapports humains-machines, de la concurrence économique et des capacités de contrôle militaro-policière[119]. En dépit d'une densité de chercheurs dans le domaine de l'intelligence artificielle parmi les plus élevées au monde, cette évolution est préoccupante pour la souveraineté numérique de la Suisse, au même titre qu'elle l'est pour les autres pays européens[120] et de la plupart des autres pays à l'exception de la Chine et des États-Unis qui sont en rivalité exclusive sur ce plan[121].

Pour partie, ce duopole est un produit dérivé du succès des firmes des plateformes grand public de ces deux pays. Inversement, **l'absence de plateforme grand public comparable aux *Big Tech*** en Europe en général et en Suisse[122] a des effets cumulatifs négatifs. Puisque les **données utilisateurs** constituent un des principaux **carburants de l'innovation** dans ce domaine, sans les gigantesques réserves de données d'utilisateurs que génèrent les plateformes grands publics il est très difficile d'être à la frontière

[119] Pour une introduction à ces problèmes voir par exemple O'NEIL ; Voir aussi DURAND/RIKAP, soulignant que la dynamique de monopolisation intellectuelle à l'âge du numérique ne saurait se réduire aux questions de brevet, mais comprend également des logiques spécifiques ayant trait aux rendements d'échelle liées aux données massives et aux modalités de l'innovation.
[120] Voir GROTH/STRAUBE.
[121] Voir LUNDVALL/RIKAP.
[122] Cf. *supra* II.3.a.

de l'évolution de "l'intelligence artificielle"[123]. Les pays concernés comme la Suisse se trouvent exposés aux conséquences des développements extérieurs de ces technologies puissantes, mais sur lesquels ils n'ont presque pas prise.

4. Synthèse des dépendances pour la Suisse

En conséquence, la Suisse dispose de solides atouts dans le domaine du numérique. La qualité des infrastructures et le niveau des compétences se traduisent en partie dans les échanges extérieurs de services numériques dynamiques et peu déséquilibrés.

Le déséquilibre est plus important sur le plan matériel, en particulier concernant les terminaux utilisés, mais ceci s'inscrit dans un contexte plus général de fragmentation internationale des processus productif et n'est **pas préoccupant** en tant que tel, du moins **tant qu'il existe diverses possibilités d'approvisionnement**. L'ampleur de la dépendance et le déséquilibre des échanges de biens avec la Chine est ici un point de vigilance. Cette appréciation générale doit cependant être nuancée et prendre en compte les enjeux de dépendance intellectuelle.

Un 1er point préoccupant concerne l'activité numérique grand public sur Internet qui se trouve en quasi-totalité en main d'entreprises *Big Tech* américaines (Apple, Microsoft, Alphabet, Meta). Il y a là un **triple enjeu** de souveraineté. D'abord, en termes de **contrôle des données personnelles** et de respect de la vie privée. Ensuite, en termes **d'action publique**, les données manipulées par les *Big Techs* permettent non seulement de mieux comprendre et d'anticiper les comportements individuels mais aussi de les influencer. Ceci a des implications dans tous les domaines de la vie sociale tels que la santé, l'éducation, les discriminations ou encore les modes de consommation qui peuvent accompagner ou au contraire contrecarrer les politiques publiques[124]. Enfin, en termes de **développement économique** sur le long terme. L'essor de l'intelligence artificielle découle en grande partie des données récoltées en masse par les plateformes grand public ; il a des implications tant en termes de sécurité pour les personnes, les organisations et les institutions politiques basées en Suisse que de développement économique futur.

Un 2ème point important concerne la propriété intellectuelle dans les domaines du numérique. Celle-ci est concentrée à l'échelle mondiale, en particulier aux États-Unis et en Asie (Japon, Corée, Chine). Cette propriété a pour conséquence de limiter les capacités d'actions des entités basées en Suisse, avec comme dans le cas des données des effets cumulatifs sur l'innovation.

Tableau 1. Évaluation synthétique des enjeux de souveraineté dans le domaine des TIC

	CAPACITÉS GÉNÉRALES	INFRASTRUCTURES MATÉRIELLES	DONNÉES MASSIVES	PROPRIÉTÉ INTELLECTUELLE
VULNÉRABILITÉ	**faible**	**modérée**	**forte**	**forte**
ASPECTS SAILLANTS	• bonne qualité des infrastructures • compétences élevées • cybersécurité à renforcer	• échanges extérieurs déséquilibrés sur les biens de consommation et les équipements • échanges équilibrés sur les composants (compétences industrielles fondamentales)	• usages des données grand public monopolisés par les plateformes étasuniennes • développement de l'intelligence artificielle	• concentration de la propriété intellectuelle • limites aux capacités d'innovation • coût économique

[123] GROTH/STRAUBE, p. 7 : "*Platform companies such as Facebook, Twitter, Google, Tencent and Baidu have had the biggest success in tapping into these pools, collecting and storing data from individuals to continuously improve their algorithms and services. […], the EU lacks actors that could shape the AI age with a European point of view.5The EU's failure to capitalize on the world's third-largest population of data producers (i.e. internet users) means that being more proactive with respect to AI development in the region's industrial sector is critically important*". Ce point est développé de manière plus systématique par RIKAP.

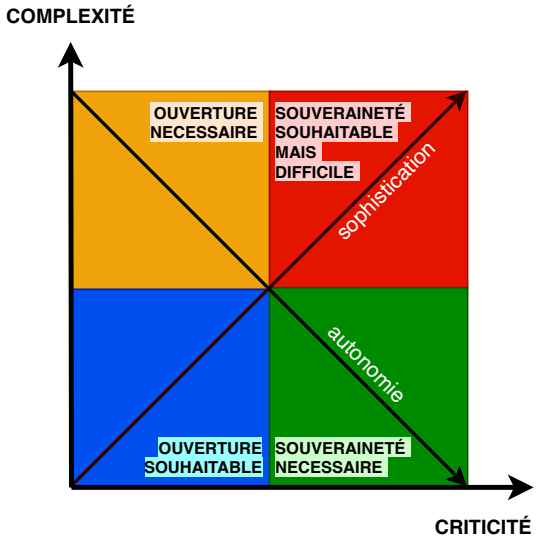
[124] Comme exemple récent, on peut songer à l'impact des plateformes de réseaux sociaux sur la santé des jeunes et des moins jeunes.

En matière de traitement des données, les vulnérabilités exposées sur le plan matériel et intellectuel se traduisent par l'existence d'un **dilemme autonomie-sophistication** (Figure 5). Les autorités doivent avoir conscience qu'être à la pointe des usages numériques peut avoir pour contrepartie une perte d'autonomie susceptible à la fois en matière d'action publique et d'encadrement des usages des données par les individus et l'industrie. En effet, puisque l'État ne peut pas contrôler les TIC dans toutes leurs dimensions vues les dépendances exposées, la vulnérabilité des divers domaines croît proportionnellement à l'intensité des usages des TIC.

Cette difficulté est incontournable, mais elle doit faire l'objet d'une **évaluation du degré de criticité** des différents usages du numérique au sein et hors des administrations, ce afin de guider l'action publique en matière de souveraineté numérique. Celle-ci ne peut pas être faite *a priori* et nécessite une appréciation proprement politique et multicritères de ce qui est critique du point de vue de la continuité de la souveraineté dans les domaines régaliens, économiques et sociaux. A partir d'une telle évaluation par domaine, on peut identifier quatre configurations impliquant des mesures distinctes en fonction de la complexité des dispositifs mobilisés et du degré de criticité[125] :

1. Lorsque les usages sont **peu critiques et simples**, il est **souhaitable de maintenir l'ouverture** (zone bleue). Cela assure la diffusion des solutions les plus performantes auprès des acteurs locaux et permet des effets d'apprentissage.
2. Lorsque les usages sont **critiques et simples** (zone verte), il est **nécessaire de développer des solutions locales** garantissant une souveraineté maximale, d'autant que des solutions relativement peu coûteuses le permettent.
3. Lorsque les usages sont **critiques et complexes** (zone rouge), il est **souhaitable mais difficile de développer des solutions locales** assurant une souveraineté pleine. Dès lors qu'il s'agit d'enjeux essentiels pour la collectivité, il est important de préserver une capacité d'action non entravée par une dépendance d'acteurs hors d'atteinte de l'action publique. Ces solutions peuvent s'avérer très coûteuses. Dans le cas où celles-ci sont complètement hors d'atteinte, faute de pouvoir exercer une véritable souveraineté, l'action publique doit rechercher des moyens pour limiter les risques encourus, soit par des **mesures de protection**, soit dans la **sélection des entités** avec qui elle contracte, soit par la **recherche de coopération** lui permettant d'exercer une souveraineté partagée.
4. Lorsque les usages sont à la fois **peu critiques et complexes** (zone orange), le développement de solutions autonomes est hors d'atteinte ou bien extrêmement coûteux alors que les enjeux ne sont pas essentiels. **L'ouverture est alors nécessaire**.

Figure 5. Le dilemme autonomie-sophistication dans le traitement des données



[125] Cf. LUZEAUX, p. 16, qui parle de 3 niveaux de souveraineté, à savoir (1) faible avec une maîtrise limitée aux infrastructures vitales, (2) partielle avec une maîtrise limitée aux infrastructures critiques et (3) complète avec une maîtrise étendue.

Il sied enfin de souligner **l'importance de la temporalité**. En effet, la question de la criticité évolue dans le temps. Si certaines questions sont cruciales à tout moment (maîtrise des données administratives et fiscales, confidentialité en matière militaire et diplomatique), d'autres applications *a priori* moins sensibles (e.g. dans le domaine de l'éducation, des infrastructures de transport ou de santé) peuvent le devenir soudainement dans un contexte de crise géopolitique. En particulier, il convient de garder à l'esprit que les **garanties juridiques d'accès** aux données à l'étranger ne sont **pas équivalentes** à une **maîtrise politico-matérielle d'accès** aux données sur le territoire national. Seule cette dernière est un véritable gage de souveraineté en cas de crise géopolitique majeure, comme la crise de la Covid-19 et la guerre en Ukraine l'ont rappelé.

La souveraineté n'est ainsi pas seulement spatiale mais a également une dimension temporelle[126], c'est-à-dire en termes de faculté d'anticipation et de temps dont dispose une autorité pour réagir à une situation nouvelle. Dans un domaine où l'innovation est très dynamique, il est difficile pour les autorités publiques d'anticiper en amont les problèmes pertinents par la seule régulation. En effet, les exigences de localisation territoriale ne constituent pas nécessairement une garantie suffisante, au motif qu'une entité résidente en Suisse et contrôlée depuis l'étranger pourrait être soumise à des décisions contraires aux intérêts du pays par la maison-mère. Ceci est d'autant plus vrai que la question même de la nationalité ne va pas de soi lorsque on parle de contrôle économique effectif : s'agit-il de l'adresse du siège, de la majorité de l'actionnariat, de la nationalité du *management* ? Face à cette somme d'incertitudes, la **puissance publique** pourrait être amenée à **prendre des participations actionnariales** dans les entités résidentes dont elle dépend pour des **services critiques**, et ce, de manière à disposer d'un regard interne sur les enjeux qui intéressent directement sa souveraineté[127].

[126] JESSOP, pp. 41-61.
[127] Il s'agirait donc d'aller plus loin que ce que recommande le Rapport Swiss Cloud du DFF/UPIC. Voir note n° 37.

III. Enjeux juridiques

1. Régimes légaux

Les régimes légaux applicables à la souveraineté numérique sont **fragmentés** du fait que celle-ci concerne différentes composantes, strates et une multitude d'acteurs (entités publiques, entreprises, individus)[128]. Parmi les régimes légaux principaux, on songe aux **lois de protection des données personnelles**[129]. On songe aussi aux **lois de propriété intellectuelle**, complétées par les dispositions sur la concurrence déloyale et les secrets d'affaires, ainsi que les droits contractuels[130]. On songe aussi aux **droits fondamentaux**[131], en particulier au droit à la vie privée et familiale[132]. On songe encore aux enjeux de défense, de cybersécurité et au respect du secret (eg. art. 320 CP ; art. 47 LB et 321 CP)[133]

L'intervention étatique permettant d'orienter les politiques publiques se concrétise sous forme de **stratégies politiques et réglementaires**. Celles-ci peuvent porter sur les différentes **composantes**, **strates** et/ou **acteurs** (pour un exemple de réglementations européennes, cf. Annexe 1 (Tableaux) - Figure 14)[134].

L'analyse des enjeux juridiques se concentrera sur les composantes, en particulier la souveraineté des données *(2)*, la souveraineté technologique *(3)*, ainsi que sur la *cyberadministration (4)* et la cybersécurité *(5)* en tant qu'éléments préalables à la souveraineté numérique. Les territoires et les acteurs sont également analysés mais de façon transversale. Les stratégies politiques et réglementaires portant sur ces différents aspects sont synthétisées dans un tableau *(6)*.

---

[128] Pour les composantes, les strates et les acteurs, cf. *supra* I.3.

[129] Ces lois sont aussi complétées par des ordonnances et des dispositions pénales. Le contrôle du respect des lois de protection des données par les entreprises et les organes fédéraux relèvent du PFPDT, tandis que le contrôle du respect des lois cantonales par l'administration cantonale relève de la responsabilité des cantons, ce qui peut conduire à des interprétations divergentes du cadre légal). Au-delà des seules données personnelles, les données en général (e.g. données industrielles et techniques) sont au cœur des technologies, ce qui explique que leur encadrement fait l'objet de nombreux développements législatifs en Suisse et à l'étranger. En droit européen, on songe aux règlementations sectorielles ou horizontales, telles que le Règlement 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) pour les données personnelles, le Règlement sur la protection des données à caractère non personnel pour les données non personnelles, la Directive *Open Data* pour les données publiques ainsi que des propositions législatives en matière de loi et de gouvernance des données (e.g. propositions de "*Data Act*", "*Governance Act*", "*Digital Service Act*"). En droit suisse, il existe plusieurs initiatives qui visent à favoriser l'accès aux données personnelles et non personnelles, voir Institut Fédéral de la Propriété Intellectuelle (IGE), accès aux données non personnelles dans le secteur privé, Rapport du 1er mars 2021, p. 4ss ; JACQUES DE WERRA, p. 365ss et les nombreuses références citées.

[130] Ces lois sont aussi complétées par des ordonnances et des dispositions pénales.

[131] Au niveau international, on songe d'abord aux instruments généraux protégeant les droits humains, au premier rang desquels la CEDH et le Pacte ONU II ainsi que les traités plus spécifiques, par exemple en matière de protection des données, à l'image de la Convention 108. Cette Convention a dans l'intervalle été révisée par le biais d'un protocole d'amendement en 2018, mais celui-ci n'a pas encore été ratifié par la Suisse (même si l'Assemblée fédérale l'a déjà approuvé par le biais d'un arrêté fédéral). Au niveau national, on songe à la Cst/CH, en particulier les art. 7-36 Cst/CH ainsi que les constitutions cantonales (surtout lorsqu'elles ont été récemment révisées) qui contiennent également un catalogue de droits fondamentaux (e.g. à Genève art. 14-43 Cst/GE, et Vaud art. 9-38 Cst/VD).

[132] Le droit à la vie privée est garanti par l'ensemble des niveaux sus-évoqués (art. 8 CEDH ; art. 17 Pacte ONU II ; art. 21 Cst/GE ; art. 15 Cst/VD). Il est rappelé que, si, à l'image des autres droits fondamentaux, le droit au respect de la vie privée est principalement dirigé contre l'État et ses agents avec une obligation négative de ne pas porter atteinte à son contenu, il comporte aussi des obligations positives pour ces derniers de garantir un respect effectif de la vie privée, y compris entre personnes et/ou sociétés privées. Cf. Cour européenne des droits de l'homme (Grande Chambre), Affaire Aksu c. Turquie, requête n° 4149/04, 15 mars 2012, § 59 : "*Par ailleurs, si l'article 8 tend pour l'essentiel à prémunir l'individu contre des ingérences arbitraires des pouvoirs publics, il ne se contente pas de commander à l'État de s'abstenir de pareilles ingérences : à cet engagement négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif de la vie privée, qui peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux*".

[133] DFF/UPIC, p. 27 ; CONSEIL FÉDÉRAL, Stratégie informatique de la Confédération 2020-2023, p. 6.

[134] Pour les composantes, les strates et les acteurs, cf. *supra* I.3.

2. Souveraineté des données

a) Extra-territorialité des lois

Le concept de souveraineté territoriale a été fragilisé depuis une dizaine d'années par l'extraterritorialité de certaines lois qui s'appliquent à des faits produits à l'étranger (e.g. RGPD et *Cloud Act*). Cela répond généralement à des objectifs stratégiques et économiques[135]. Par exemple, le RGPD étend la protection à toutes les personnes concernées qui se trouvent dans l'Union européenne, indépendamment de la localisation effective du traitement[136]. Le *Cloud Act* confère aux autorités un droit d'accès aux données localisées hors territoire américain mais gérées par des sociétés américaines[137]. Le droit suisse prévoit aussi des lois avec effets extra-territoriaux, telles que la LPD applicable à des faits produits à l'étranger, pour autant qu'ils engendrent suffisamment d'effets en Suisse[138].

Ces lois extra-territoriales imposées à un État tiers conduisent à un certain déclin de la souveraineté territoriale, voire à une déterritorialisation du droit, étant précisé qu'elles créent une concurrence de juridictions[139] et qu'elles doivent en tout état respecter le droit international[140].

S'agissant de la concurrence de juridictions, celle-ci doit être réglée selon les règles sur le conflit de lois. En principe, la localisation spatiale des données permet de déterminer la juridiction compétente. Or, les données sont souvent localisées à l'étranger et la localisation varie souvent constamment, de sorte que l'on peut parler d'une localisation éclatée des données[141]. Pour contourner ces difficultés, la jurisprudence tend à abandonner le critère de la localisation des données (stockage sur les serveurs physiques) au profit du critère de l'accès ou maîtrise sur les données[142]. L'abandon du critère de la localisation des données (stricte territorialité) au profit de l'accès ou maîtrise sur les données confirme les nouvelles formes de territoires (glissement d'une strate physique vers une strate des réseaux).

S'agissant du respect du droit international, les lois doivent respecter la souveraineté des autres États (art. 5 Cst/CH). Dans le même temps, la Suisse a conservé un lien étroit entre son territoire et ses prérogatives étatiques, en obligeant la Confédération et les cantons de prendre toutes les mesures nécessaires pour garantir l'indépendance de la Suisse envers d'autres États, l'intégrité et l'inviolabilité de son territoire (art. 1 Cst/CH). Dans le domaine économique, cette obligation peut s'interpréter comme une invitation à privilégier les acteurs suisses aux acteurs étrangers, dès lors que l'indépendance pourrait être menacée. Ainsi, le choix d'équipements et d'infrastructures digitales (e.g. *clouds*, réseaux) doit pouvoir servir l'indépendance de la Suisse[143].

---

[135] Voir THELISSON, p. 524ss, qui ajoute également des concepts de morale internationale, connue dans les domaines de la défense des droits de l'homme, du droit de l'environnement ou du droit pénal international ; Voir aussi BRADFORD, qui parle du "*Brussels effect*" du RGPD pour imposer des standards de protection des données à l'échelle globale consistant pour l'UE de promouvoir ses normes et conduisant à une européanisation du cadre légal européen à l'étranger.

[136] Voir THELISSON, p. 524ss, indiquant que le RGPD répond aussi à des objectifs stratégiques et économiques et influence la souveraineté numérique puisqu'il assujettit les données d'individus européens à la protection européenne indépendamment de leur localisation. Au sujet du Trans-Atlantic Data Privacy Framework voir INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP), Is data localization coming to Europe?, 23 août 2022 ; La Commission européenne a été accusée par un citoyen allemand d'avoir violé le RGPD en attribuant l'hébergement d'un site à Amazon Web Services. Un recours a été déposé devant le tribunal de l'Union européenne. A ce sujet, voir Alice VITARD, La Commission européenne traînée en justice pour avoir utilisé Amazon Web Services, *in* Usine digitale, 19 juillet 2022.

[137] Voir THELISSON, p. 521, indiquant que le *Cloud Act* est considéré comme une réponse américaine au caractère extraterritorial du RGPD et complète et confère une portée extra-territoriale au SCA (pour *Stored Communications Act*). ; CASSART, p. 41 ; DÉPARTEMENT AMÉRICAIN DE LA JUSTICE, USA DoJ, White Paper, Promoting Public Safety, Privacy, and the Rule of Law Around the World : The Purpose and Impact of the CLOUD Act, April 2019.

[138] Cf. Théorie des effets (*Auswirkungsprinzip*). Cf. déjà ATF 91 II 192, consid. 3. Avec la LPD, le TF étendait le champ d'application de l'ancienne LPD en y assujettissant certains traitements de données qui se déroulent à l'étranger (cf. notamment ATF 138 II 346, ATF 138 II 346) avant que le législateur ne codifie cette théorie des effets dans la loi, en prévoyant que "la présente loi s'applique aux états de fait qui déploient des effets en Suisse, même s'ils se sont produits à l'étranger" (art. 3 al. 1 LPD).

[139] Voir THELISSON, p. 525, indiquant que la concurrence de juridictions doit être réglée selon les règles du conflit de lois qui déterminent le droit applicable (sous réserve de solutions régionales de résolution des conflits éventuels via la gouvernance, telle que désignation d'une autorité chef de file) ; PRETELLI, p. 22.

[140] THELISSON, p. 513 et 517 : en droit suisse, la Constitution pose le principe du respect du droit international par la Confédération et les cantons (art. 5) ; MAYER, p. 9ss ; VAN HECKE, p. 309.

[141] Cf. PFDPT, Cloud computing (site web).

[142] Cf. ATF 143 IV 21, consid. 3.4.2 (arrêt Facebook) ; Arrêt du TF 1B_142/2016 du 16 novembre 2016, consid. 3.5-3.6 (arrêt Google).

[143] THELISSON, p. 517 ; MAYER, p. 9ss.

Recommandation : Lors de l'élaboration de lois suisses et de leur interprétation, il est recommandé que les autorités réfléchissent à leur conférer une portée extra-territoriale afin de promouvoir certains objectifs stratégiques et économiques, ce dans le respect du droit international. Lors de l'application de lois étrangères à effet extra-territorial, il est recommandé que les tribunaux analysent soigneusement les règles sur le conflit de lois et la compatibilité de la loi étrangère avec le droit international public, dont la souveraineté suisse avant d'admettre ses effets en Suisse. Il est aussi recommandé de réfléchir à privilégier les acteurs suisses aux acteurs étrangers lorsque l'indépendance peut être menacée (e.g. choix d'équipements et d'infrastructures digitales indigènes pour les données et infrastructures critiques)[144].

b) Transfert des données à l'étranger

Vue l'importance stratégique des données, les États adoptent des règles en matière de transfert des données à l'étranger. Ces règles peuvent être libérales avec une libre circulation des données ou être restrictives avec des exigences de localisation des données, des serveurs et/ou des responsables du traitement. Ces exigences de localisation caractérisent le débat sur la souveraineté numérique. Ainsi, elles poursuivent à la fois un objectif juridique (contrôler le respect de ces règles à l'étranger) et un objectif politique (renforcer la souveraineté des données).

En droit suisse, les règles en matière de transfert des données à l'étranger prévoient une libre circulation des données dans des pays à niveau de protection équivalent et, en l'absence d'un tel niveau de protection, un transfert des données moyennant des garanties supplémentaires (e.g. clauses contractuelles standards ou accord bilatéral)[145]. Ainsi, lorsqu'il existe un risque que les données soient transférées dans un pays, sans niveau de protection équivalent, il convient de procéder à une évaluation des risques et d'aménager les rapports contractuels en conséquence. L'évaluation tiendra compte de la nature des données (e.g. données ordinaires ou sensibles, couvertes par un secret) et l'existence d'un droit d'accès aux données par les autorités étrangères selon les législations étrangères[146].

En droit européen, les règles sont similaires et favorables à une libre circulation des données à l'étranger, même si les autorités et les tribunaux limitent parfois les possibilités de transfert à l'étranger, à travers une interprétation stricte des règles (e.g. l'arrêt Schrems II)[147] et des exigences de localisation de certaines données personnelles et infrastructures (e.g. le DGA et le RGPD prévoyant des exigences de localisation des données respectivement des exigences de certification de cybersécurité pour les services en nuage)[148].

Il convient de préciser que, même lorsque les données sont hébergées en Suisse mais auprès d'un prestataire appartenant à un groupe étranger (e.g. Microsoft suisse), certaines législations ont des effets extra-territoriaux et donnent accès aux autorités indépendamment de la localisation des données (e.g. *US Cloud Act*)[149].

---

[144] Cf. *supra* II.4.

[145] La libre circulation des données est un principe cardinal de la nLDP (cf. 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, FF 2017 6594, soulignant qu'un des principes de la révision est l'*amélioration des échanges de données transfrontières* et 6794 que "le projet de loi vise en outre à faciliter les flux transfrontières en garantissant que les données peuvent transiter d'un pays à l'autre").

[146] E.g. si les données sont hébergées chez un prestataire américain ou suisse sous contrôle d'un groupe américain, le US Stored Communications Act respectivement le *US Cloud Act* pouvant donner un accès aux autorités. Cf. PRIVATIM, Merkblatt Cloud-spezifische Risiken und Massnahmen, p. 4 ; SCHWARZENEGGER et al., p. 83ss ; Cf. FISCHER, *op. cit.*, qui distingue entre un droit d'accès légal ponctuel et généralisé et qui souligne que l'analyse du risque doit encore évaluer la probabilité que l'autorité le fasse valoir et arrive à ses fins.

[147] La jurisprudence par exemple avec l'arrêt Schrems II.

[148] Le régulateur par exemple dans certains secteurs, tels que la santé avec la loi sur la gouvernance des données et la loi sur les données ainsi que des exigences de certification de cybersécurité pour les services en nuage. Cf. Avis conjoint 03/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), adopté le 10 juin 2021.

[149] Le *US Cloud Act* oblige les prestataires IT américains d'aller chercher les données hébergées dans leurs filiales à l'étranger pour les communiquer aux autorités américaines (sous certaines conditions, en particulier si la procédure dans le cadre de laquelle ces données sont requises soit liée à des crimes graves (*serious crimes*, Section 2713 (a) (1). Ainsi, les autorités américaines auraient accès aux données de filiales suisses appartenant à un groupe américain (e.g. Microsoft). Il convient de préciser que le *US Cloud Act* n'est pas la seule réglementaiton étrangère prévoyant un droit d'accès aux autorités étrangères. On songe par exemple au débat actuel concernant l'application TikTok dont la

Sur cette base, en cas d'hébergement et traitement des données en Suisse, le risque d'accès par les autorités étrangères peut être évité uniquement si le responsable du traitement basé en Suisse n'a aucune relation ou contact avec des entreprises étrangères (e.g. avec une filiale américaine) ou, en cas de relation avec des entreprises étrangères, si celles-ci n'ont pas la possession, la garde, le contrôle ou la responsabilité de l'entité européenne. Cette sorte d'immunité du responsable du traitement basé en Suisse suppose, en termes d'organisation, que son siège statutaire et son administration centrale soient établis en Suisse et que son capital social et les droits de vote ne soient pas individuellement ou collectivement détenus au-delà d'un certain seuil (e.g. 24% individuellement, 39 % collectivement) par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement basé à l'étranger[150].

Pour cette raison, le recours par l'administration publique à des prestataires, certes suisses, mais appartenant à un groupe américain fait l'objet de débats actuellement. Le **PFPDT** estime que le recours au *cloud* M365 (services *Outlook* et *Teams*) pour la Caisse suisse d'assurance-accidents (SUVA) est contraire à la LPD même si les données sont hébergées en Europe, au motif qu'il existe un risque résiduel d'accès par les autorités étrangères (approche "restrictive" de zéro-risque)[151]. Le **Conseil d'État zurichois** estimant que le recours au *cloud* M365 pour l'administration cantonale zurichoise est licite pour autant que certaines mesures additionnelles de protection soient prises, afin de limiter le risque d'accès par les autorités étrangères (approche "libérale" fondée sur le risque)[152].

Dans les deux cas, il est question d'une analyse de risque, du fait que la licéité du *cloud* est analysée selon que les mesures additionnelles de protection permettent ou non de limiter le risque d'accès par les autorités étrangères[153]. La réticence du PFDPT est certainement due au durcissement de la pratique des autorités européennes en matière de transfert vers les États-Unis et en attendant un accord remplaçant le *Privacy Shield*[154]. Le risque d'accès des autorités étrangères doit être par ailleurs nuancé puisque la communication depuis la Suisse serait une violation de l'art. 271 CP, qui interdit de procéder à des actes relevant des pouvoirs publics (hors entraide)[155].

Recommandations : Sur cette base, lorsqu'il existe un risque que les données soient transférées dans un pays sans niveau de protection équivalent, il convient de procéder à une évaluation des risques et d'aménager les rapports contractuels en conséquence. Selon la nature des données (s'il s'agit de données sensibles, critiques ou protégées par un secret), il est recommandé de privilégier une solution locale, soit un prestataire suisse (e.g. *cloud souverain*) ou, s'il appartient à un groupe étranger, de renforcer les engagements contractuels, pour s'assurer du respect du secret[156].

---

maison-mère ByteDance basée en Chine pourrait être tenue de donner accès aux autorités chinoises depuis le territoire chinois, indépendamment de la localisation des données, ce sur la base de la législation chinoise.

[150] Voir RAMOS et al., soit l'étude Greenberg Traurig réalisée sur mandat du Ministère néerlandais de la Justice et de la Sécurité.

[151] Voir PFDPT, Guide juin 2021 : contrairement à la SUVA estimant le risque comme très improbable (*höchst unwahrscheinlich*),

[152] Il s'agit donc d'une approche fondée sur les risques pour la licéité du recours aux services *cloud*, considérant qu'il n'est aujourd'hui pas envisageable de recourir exclusivement à des services *on premise* (donc non situés sur un *cloud*) et que, pour ne pas se retrouver "technologiquement hors-jeu" ("*technologisch ins Abseits*"), un recours à des services de type *cloud* (dont des prestataires US) est indispensable.

[153] La Fédération suisse des avocats suit l'approche fondée sur les risques mais recommande la prudence (solutions locales), en tout cas les questions fiscales et des PEB et si la législation étrangère rend délicate le respect des contrats. L'analyse des risques "*nécessite que ce dernier soit contractuellement tenu au secret professionnel et que l'externalisation prévue résiste à l'évaluation des risques. Dans cette analyse, il faut tenir compte de la sensibilité des données, mais aussi du respect attendu des contrats et des lois auxquels est soumis le fournisseur de services cloud à l'étranger, ainsi que de la probabilité concrète d'accès aux données. Cette évaluation des risques peut varier en fonction de l'activité de l'avocat/e. Une prudence élémentaire s'impose, notamment lorsque l'avocat/e conseille des clients étrangers sur des questions fiscales et des clients politiquement exposés*". Cf. SCHWARZENEGGER et al.

[154] Cf. FISCHER, *op. cit.*, citant les décisions strictes prises dans les affaires *Google Analytics* : la décision de l'autorité autrichienne de protection des données du 22 décembre 2021, la décision de mise en demeure de la CNIL du 10 février 2022 et plus récemment la décision de l'autorité italienne de protection des données du 9 juin 2022. De même, la chambre des marchés publics de Baden-Württemberg (Allemagne) a retenu dans une décision qu'un risque d'accès par les autorités américaines doit être analysé comme une communication effective. En effet, une décision négative quant à l'adéquation de la Suisse aurait des conséquences importantes sur l'économie suisse.

[155] Cf. FISCHER, *op. cit.*, indiquant que ce risque ne constitue pas l'unique prisme par lequel un projet d'externalisation doit être analysé. L'impératif de sécurité des données (à savoir la protection contre les accès non autorisés, y compris à l'interne) et la nécessité de garantir la *business continuity* en cas de défaillance du prestataire représentent des enjeux tout aussi importants, voire plus cruciaux en termes de risques effectifs à prendre en compte dans le cadre d'un projet impliquant un traitement de données.

[156] Parmi les engagements contractuels, on songera à l'engagement de mesures techniques et organisationnelles (e.g. cryptage des données), à l'absence d'exclusion de responsabilité en cas de violation de la confidentialité des données, à l'obligation d'informer la localisation précises

A l'échelle globale, les restrictions au transfert des données peuvent apparaître comme des barrières au commerce internationale et au partage de données pour le bien commun[157]. Il est donc recommandé de renforcer la coopération internationale sur ce sujet, ce que la Suisse peut aisément faire auprès des organisations internationales et non gouvernementales basées à Genève (e.g. OMC, UIT).

c) Autodétermination numérique

L'autodétermination numérique est une nouvelle approche pour une politique des données permettant de renforcer la souveraineté des données. Elle peut être définie comme la capacité de décider de son "destin numérique". Elle consiste à renforcer le contrôle des particuliers, des entreprises et la société dans son ensemble sur leurs propres données, afin qu'ils puissent décider eux-mêmes de leurs moyens d'agir dans l'espace numérique, de renforcer leur confiance dans la société numérique et d'accroître leur volonté de partager et d'utiliser les données. Elle suppose d'avoir les capacités de comprendre les technologies, de se faire sa propre opinion et de mettre en œuvre sa décision (composante individuelle). Elle suppose aussi un partage suffisant des données, afin qu'elles soient accessibles au plus grand nombre dans un esprit de bien commun (composante collective).

L'autodétermination numérique est déjà consacrée en droit international et national, en particulier avec les droits fondamentaux et la protection des données, qui visent à construire un écosystème aux conditions appropriées, dans lequel les particuliers et les entreprises peuvent évoluer de manière autodéterminée[158]. Afin de la renforcer, une nouvelle question est de savoir s'il faut reconnaître un nouveau droit à l'intégrité numérique, au motif que les droits existants seraient insuffisants[159] et que la reconnaissance d'un tel droit permettrait d'imposer aux institutions d'interagir avec la population en garantissant la sécurité numérique, l'éducation numérique et de revendiquer l'autodétermination informationnelle[160]. Son ancrage pourrait être une extension de droits fondamentaux existants ou un nouveau droit fondamental *ad hoc* (e.g. norme de "*courroie*")[161].

Recommandations : il est recommandé de renforcer l'autodétermination numérique à travers des actions publiques par les autorités et l'interprétation des lois par les tribunaux, sachant qu'elle est déjà consacrée dans les lois, que cela permettra de mieux en définir les contours et la mettre en œuvre et que cela s'inscrit dans la politique des données de la Confédération.

---

des serveurs ainsi que d'éventuelles réquisitions de données par les autorités étrangères (*lawful access*). Plus spécifiquement, le chiffrement des données permet de rendre caduc le droit d'accès aux autorités étrangères. Bien qu'efficace cette méthode garde trois limites: (i) certains chiffrements peuvent être "cassés", surtout quand ce sont des gouvernements qui interviennent (limite technologique) ; (ii) certaines législations limitent le chiffrement selon les pays (limite juridique), (iii) les coûts liés à la gestion des clés de chiffrements peuvent être élevés (limite économique). Voir LE MAG IT, Quelles différences entre CLOUD Act et PATRIOT Act (et quels impacts sur les entreprises françaises), *in* LE MAG IT, 21 août 2018.

[157] Pour une analyse des restrictions au transfert des données d'un point de vue de droit comparé (UE, US, Chine), voir YAKOVLEVA.

[158] En matière de droits fondamentaux, on songera au droit à la liberté personnelle (art. 10 al. 2 Cst/CH), aux droits à la protection de la sphère privée, à l'autodétermination informationnelle et à la protection contre l'utilisation abusive de données personnelles (art. 13 Cst/CH ; art. 8 CEDH ; art. 17 Pacte ONU II) et à la liberté d'information (art. 16 Cst/CH ; art. 10 CEDH ; art. 19 Pacte ONU II). En protection de la personnalité et des données, on songera à la protection de la sphère privée, de la personnalité et de l'autodétermination informationnelle (i.e. droit de chaque personne de décider à qui confier ses données personnelles, dans quelles circonstances et à quelles fins) – concrétisées dans les art. 27-28 CC et la LPD, complétée par des dispositions pénales en cas d'utilisation abusive des données – sont des composantes importantes de l'autodétermination numérique.

[159] A titre exemplatif, la LPD ne couvrirait pas toutes les atteintes et les droits fondamentaux, tels que la protection de l'art. 13 al. 2 Cst/CH et le droit à l'auto-détermination seraient valable uniquement à l'égard de l'État).

[160] En effet, seul l'État est initialement soumis aux droits fondamentaux, même si ceux-ci doivent se manifester dans l'ensemble de l'ordre juridique et les autorités doivent veiller à ce que les droits fondamentaux, dans la mesure où ils s'y prêtent, prennent également effet entre les particuliers (art. 35 Cst/CH).

[161] E.g. par interprétation jurisprudentielle : droit à la vie et liberté personnelle (art. 10 Cst/CH), dont découle les droits de la personnalité (art. 27ss CC) ; protection de la sphère privée (art. 13 Cst/CH), dont découle l'autodétermination informationnelle comme droit défensif et de maîtrise.

3. Souveraineté technologique

La souveraineté technologique passe par une **politique d'innovation** qui inclut des mesures étatiques (juridiques, économiques et techniques). Les mesures peuvent être offensives et/ou défensives et agir sur les marchés et/ou les acteurs du marché. Des mesures protectionnistes (e.g. contrôle des investissements, rapatriement de chaine de valeur)[162] devraient être toutefois évitées car une indépendance totale de TIC exclusivement indigènes n'est vraisemblablement pas envisageable, vue l'imbrication extrême de l'écosystème numérique suisse dans les infrastructures et les services déployés à l'échelle mondiale[163]. Il conviendra de privilégier une **coopération** européenne et internationale[164].

Une politique d'innovation visant la souveraineté technologique suppose d'évaluer soigneusement quelles sont les **technologies critiques** (KET) et quelles menaces pèsent réellement sur leur fourniture ou leur accès[165]. Pour cela, il faut identifier dans quel contexte les KET s'insèrent et quelles sont les motivations d'intervention étatique (e.g. compétitivité, besoins sociétaux, contribution à des tâches régaliennes), si l'accès à cette technologie pourrait être menacé et ce qui est nécessaire pour y parvenir en tenant compte des ressources et compétences existantes dans le pays (à court ou moyen terme)[166].

Il conviendra aussi d'améliorer les **compétences** décisionnelles et opérationnelles des utilisateurs publics et privés afin de renforcer la liberté de choix et d'éviter une concentration d'offre (e.g. formations de pointe pouvant pallier le manque de personnel dans la production et/ou l'utilisation des KET)[167]. Il conviendra aussi de se **réapproprier la transformation numérique des activités régaliennes** (e.g. identification e-ID et signature électronique)[168].

Le droit de la propriété intellectuelle est un élément-clé de la protection des données et des secrets d'affaires (e.g. algorithmes et techniques d'analyse des données)[169]. La régulation à elle seule est toutefois insuffisante puisque seule une compréhension des technologies et une analyse *ex ante* des effets d'une régulation permet de trouver le bon équilibre, dosage entre protection et libre utilisation[170].

C'est dans cet esprit d'équilibre que l'accès aux données est au cœur du développement de la politique d'innovation, dont l'intelligence artificielle (IA), ce qui explique qu'elle fait l'objet de nombreux développements législatifs en Suisse et à l'étranger.[171]

---

[162] A propos de la chaîne de valeurs, voir ILLGNER, p. 8ss.

[163] SEIFRIED/BERTSCHEK, p. 6ss : il convient de souligner que des mesures autarciques et/ou protectionnistes ne contribuent pas nécessairement la souveraineté des divers acteurs économiques.

[164] La nouvelle stratégie commerciale de l'UE reflète l'intention de cette dernière de défendre davantage ses intérêts économiques. Les experts européens préconisent 3 approches pour le marché européen. La 1ère approche (compétition) consiste à créer des champions européens afin de concurrencer les acteurs dominants en vue d'un marché européen numérique, ce qui suppose d'importants investissements sur le long terme. La 2ème approche (concours) consiste à créer des alliances industrielles avec des acteurs européens existants. La 3ème approche (coopération) consiste à favoriser, voire forcer l'ouverture des données et l'interopérabilité des technologies (e.g. GAIA-X). Cf. CHRÉTIEN/DROUARD, p. 24ss ; COMCO, Rapport annuel 2020 de la Commission de la concurrence (COMCO), DPC 2021/1 p. 23ss, 42.

[165] EDLER et al., p. 19ss, indiquant qu'il ne faut toutefois pas nécessairement faire une veille stratégique / évaluation globale de la position d'un pays en matière de compétitivité technologique et de relations de pouvoir dans les chaînes de valeurs internationales.

[166] EDLER et al., p. 19ss ; WESTPHAL, p. 7 : cartographier les compétences et les (inter-)dépendances en matière de TIC et de données pour mettre en place des modèles de gouvernance et de régulation adaptés.

[167] On distingue généralement les compétences décisionnelles et les compétences opérationnelles, les 1ères étant comprises comme la capacité à comprendre, à évaluer et à vérifier la fiabilité des solutions sur le marché, les 2èmes étant comprises comme l'utilisation efficace des technologies permettant d'augmenter sa propre compétitivité et capacité d'innovation. Voir SEIFRIED/BERTSCHEK, p. 6ss et références ; Chavanne Yannick, Le manque de spécialistes IT en Suisse engendre une perte de création de valeur de 31 milliards, *in* ICTJournal, 12 septembre 2022 ; JAUN René, En 2030, il manquera près de 40'000 informaticiens en Suisse, *in* ICTJournal, 12 septembre 2022.

[168] TÜRK et références.

[169] Voir MARCH/SCHIEFERDECKER.

[170] En cas de protection accrue, PAGANO parle de durcissement des droits de propriété intellectuelle, voire de privatisation des connaissances qui vient s'ajouter au monopole de marché dû à la concentration des compétences dans les machines et le management. Il prend comme exemples les *patents trolls* (entreprises spécialisées dans la détention de brevets).

[171] En droit européen, on songe aux règlementations sectorielles ou horizontales, telles que le Règlement 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) pour les données personnelles, le Règlement sur la protection des données à caractère non personnel pour les données non personnelles, la Directive *Open Data* pour les données publiques ainsi que des propositions législatives en matière de loi et de gouvernance des données (e.g. propositions de "*Data Act*", "*Governance Act*", "*Digital Service Act*"). En droit suisse, il existe plusieurs initiatives qui visent à favoriser l'accès aux données personnelles et non personnelles, voir INSTITUT FEDERAL DE LA PROPRIETE INTELLECTUELLE (IPI), Rapport concernant l'accès aux données non personnelles dans le secteur privé, 1er mars 2021, p. 4ss ; DE WERRA, RSDA, p. 365ss et les nombreuses références citées.

C'est dans cet esprit d'équilibre que la reconnaissance d'une propriété absolue sur les données (*erga omnes*) a fait l'objet de nombreuses études en droit suisse et européen pour conclure systématiquement à son rejet[172] et pour se concentrer plutôt sur l'instauration d'un droit d'accès obligatoire, cas échéant à travers des réglementations horizontales (e.g. exception de *text and data mining* en droit d'auteur) ou sectorielles (e.g. partage des données de l'administration publique)[173]. Lorsque l'accès est volontaire[174], il semble aussi intéressant de se tourner vers les mécanismes contractuels, afin de régir de façon flexible les différents types de données et les interactions entre tous les participant·e·s à l'écosystème[175]. En particulier, il semble intéressant de se tourner vers les modèles de licences libres qui permettent de fluidifier la circulation des données, tout en garantissant le contrôle des titulaires[176]. Les licences libres sont des licences standardisées, applicables à un nombre indéterminé d'utilisations et sont souvent utilisées dans le domaine de l'administration publique (*Open Government Data*), de la recherche (*Open Research Data*), des logiciels ouverts (*Open Source*), des biens issus de collaborations (*Creative commons*)[177] et plus récemment dans le domaine privé[178].

On observe toutefois une **asymétrie** dans le développement des technologies. Les données affluent plus facilement vers les pays développés disposant de capitaux et de ressources qui peuvent influencer la souveraineté numérique et le développement économique des pays plus faibles. La communauté internationale devrait **promouvoir l'égalité** de la souveraineté numérique[179]. L'instauration d'un droit d'accès obligatoire aux données pouvant s'accompagner d'un manque d'incitation à investir dans la collecte et le traitement de données, il semble préférable de recourir à des mesures de soutien complémentaires (e.g. contrats-types, certifications, sensibilisation et formation) plutôt que la mise en place de mesures législatives majeures[180].

Recommandations : il est recommandé de privilégier une **coopération** européenne et internationale (au lieu de mesures protectionnistes). S'agissant des mesures étatiques, il est recommandé d'analyser quelles **technologies critiques** (KET) doivent être accessibles, cas échéant de préférer des mesures de soutien complémentaires (e.g. contrats-types, certifications, sensibilisation et formation) à des mesures législatives majeures. Il est aussi recommandé d'améliorer les **compétences** des utilisateurs publics et privés et de se **réapproprier la transformation numérique des activités régaliennes**.

---

172 Cf. IPI, *op. cit.*, se basant sur l'argument de défaillance de marché et considérant que l'absence actuelle de propriété sur les données ne semble pas avoir d'effet négatif sur l'innovation, tandis que l'introduction d'un tel droit pourrait faire obstacle au développement économique et provoquer une incertitude juridique quant à la portée d'une telle propriété. Les mêmes remarques sont en grande partie applicables à l'introduction d'un droit *sui generis* sur les bases de données.

173 Cf. DE WERRA, RSDA 2021, notes 34-35 ; BENHAMOU Y., RSDA, p, 400 et n. 49ss.

174 L'accès volontaire peut prendre la forme d'un contrat individuel entre deux ou plusieurs acteurs (e.g. contrat de transfert ou d'échange de données, d'abonnement) ou encore d'un contrat standardisé sous la forme de conditions générales ou de politique privée de données ouvertes (*Open Data*) ou de données partagées (*Shared Data*). Cf. IPI, *op. cit.*, p. 7.

175 Cf. BENHAMOU/TRAN, p. 572 ss ; DE WERRA, sic!, p. 194ss et 206.

176 Cette dimension collective est souvent inspirée de la théorie des biens communs, selon laquelle tout bien commun (chose à l'origine librement disponible à la communauté) est menacé par une appropriation (*enclosure*), tandis qu'une gestion communautaire des ressources basée sur une capacité d'auto-organisation est préférable en ce qu'elle conduit à une meilleure production et à un maintien des ressources. Pour des références, cf. BENHAMOU/TRAN, p. 575 et n. 4. Au-delà de la gestion collective des données, on observe aussi un mouvement d'exercice collectif de droits individuels liés aux données, e.g. le droit d'accès qui, lorsqu'il est exercé collectivement, permet de mieux comprendre le fonctionnement de l'algorithme du prestataire, cf. MAHIEU/AUSLOOS, p. 1ss et les nombreuses références citées.

177 Ces licences standardisées sont proposées par différents organismes, p. ex. licence libre GPL (General Public license) par la FREE SOFTWARE FOUNDATION ou licence Creative Commons par CREATIVE COMMONS.

178 Le partage de données ouvertes par les entreprises privées émerge progressivement notamment pour des raisons économiques (la valeur économique des données ouvertes étant estimée à USD 5'000 milliards en 2013) mais reste limité, surtout pour des raisons de protection des droits de propriété intellectuelle et des données personnelles. Les données sont alors généralement partagées par le biais de publications (e.g. rapport annuel), mentionnées sur un site internet et/ou une interface de programmation d'application (API de son acronyme anglais) contenant uniquement certains types de données (e.g. données de base et métadonnées). Cf. IPI, *op. cit.*, p. 26.

179 Voir DURAND.

180 Les mécanismes de certification européenne pour un cloud souverain sont de bons exemples dont la Suisse pourrait s'inspirer directement, notamment vues les considérations similaires ayant conduit l'UE à se tourner vers des mécanismes de certification, cf. n. 61 et 142.

4. Cyberadministration

a) Planification, mise en œuvre et contrôle

La souveraineté numérique suppose que l'Etat puisse décider librement si et comment numériser ses processus internes et ses services à la population (*cyberadministration*) dans de bonnes conditions et de façon autonome[181]. La souveraineté numérique peut en effet aussi signifier ne pas numériser certains services (p.ex. pour des raisons de sécurité et/ou sobriété numérique). Cela nécessite une **politique publique commune** à la Confédération, aux cantons et aux communes[182]. Dans la mise en œuvre de sa politique publique, il est utile de distinguer différentes étapes (qui interviennent chacune aux trois niveaux de l'État, Confédération, canton, communes[183]) : *(i)* une phase de planification, (*ii*) une phase de mise en œuvre et (*iii*) une phase de contrôle.

Dans un premier temps, il convient de mener à bien une phase de planification, qui consiste à examiner les solutions techniques existantes et les risques que celles-ci font peser sur les valeurs et principes de l'Etat de droit suisse, afin d'en dégager des choix stratégiques. Cette phase comporte fréquemment une dimension "législative" découlant de l'identification des vides juridiques à combler avec un cadre juridique plus précis, au niveau international ou national[184]. La phase de planification permet de poursuivre simultanément plusieurs objectifs :

- Dresser un état des lieux de la situation actuelle et des risques encourus : à titre d'exemple, certains rapports soulignent l'augmentation de la collecte des données sans que la société ne sache ce qu'il en advient[185] ou encore la concentration et le contrôle des données aux mains de quelques acteurs (*hyperscalers*)[186]. Dans ce cadre, les risques identifiés en matière de souveraineté des données sont notamment : l'application extraterritoriale de lois étrangères (e.g. l'*US Cloud Act*) et un accès non autorisé aux données, une dépendance à l'égard de prestataires sis à l'étranger, la problématique du secret de fonction (art. 320 CP ; art. 47 LB et 321 CP)[187].

- Déterminer les droits et les valeurs pertinents et les choix qui en découlent : Les autorités placent au cœur de leur réflexion le respect de la protection des droits fondamentaux et des données[188]. A cet égard, les exigences les plus importantes sont l'absence d'obligation de communiquer les données à des tiers et la soumission au droit suisse avec un for en Suisse[189]. L'autodétermination numérique est également suggérée comme nouvelle approche pour une politique des données[190].

- Clarifier la répartition des compétences et créer si besoin des organes de coopération : Les autorités rappellent que ces défis constituent une tâche commune de la Confédération, des cantons, de l'économie et de la société[191]. Cela suppose donc de s'interroger sur le rôle que

---

[181] Le terme "cyberadministration" s'entend ici de façon large pour parler à la fois des processus de transformation de l'administration et des processus numérisés eux-mêmes fournissant des prestations administratives. Cf. MONTAVON, p. 25ss ; PLATTNER ; ROBERTS et al.

[182] ROBERTS et al, pp. 5-6 ; MONTAVON, p. 25ss ; Voir également DFF, Administration numérique (site web).

[183] Et ce même si une volonté d'harmonisation est présente. Cf. CONSEIL FÉDÉRAL, *op cit*., p. 1767 : "*Le Conseil fédéral compte donc promouvoir l'interopérabilité des applications de la cyberadministration tant à l'intérieur des services des trois niveaux de l'État qu'entre eux, ce qui garantit une utilisation multiple des solutions et des données*".

[184] CONSEIL FÉDÉRAL, Message du 4 mars 2022 concernant la loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités, FF 2022 804.

[185] DFAE, Politique extérieure numérique 2021–2024, p. 14 ("*la communauté et la société ne profitant quasiment pas des enseignements ni de la création de valeur économique que l'on pourrait tirer de ces données et des recoupements entre elles*").

[186] DETEC/DFAE, Rapport sur la création d'espaces de données fiables, p. 3 ; Voir également DFF/UPIC, Rapport Swiss Cloud, p. 7, qui en souligne l'impact technologique, économique et potentiellement aussi (géo)politique.

[187] DFF/UPIC, p. 27 ; CONSEIL FÉDÉRAL, Stratégie informatique de la Confédération 2020-2023, p. 6.

[188] CONSEIL FÉDÉRAL, Stratégie informatique de la Confédération 2020-2023, p. 6. ; Cette réflexion permet aussi de rappeler certains principes cardinaux d'un État fondé sur le droit : "*[L]es droits de l'homme doivent être tout autant respectés dans le monde numérique que dans le monde physique, peu importe les frontières géographiques*". Cf. DFAE, Politique extérieure numérique 2021–2024, p. 14.

[189] Dans le domaine du Cloud, les recommandations du PFPDT semblent se contenter d'un for européen, voir *supra* I.4.c. et n. 81 ; DFF/UPIC, Rapport Swiss Cloud, p. 5 et 16 : dans le domaine informatique, la sécurité comprend trois aspects : confidentialité, intégrité et disponibilité.

[190] Voir DETEC/DFAE, Rapport sur la création d'espaces de données fiables, p. 13 : Cette autodétermination numérique se compose d'un volet individuel – qui protège la personne via les droits humains, l'autodétermination informationnelle et les libertés contractuelle, économique et de la science – et d'un volet collectif.

[191] CONSEIL FÉDÉRAL, Stratégie Suisse numérique 2020, p. 12.

doivent jouer les pouvoirs publics : fournisseurs de prestations ou émetteurs d'un cadre juridique approprié (voire même laisser placer, en tout cas dans un premier temps, à de l'autorégulation)[192], ainsi que sur la mise en place d'infrastructures dédiées ou d'organes de coopération[193]. Par ailleurs, au sein de chaque collectivité publique, il convient de désigner, le cas échéant, la ou les autorité(s) chargée(s) d'accompagner ou de favoriser la transformation numérique. Ainsi, au niveau fédéral, le Conseil fédéral a décidé en 2020 de créer un centre de compétences pour les questions de numérisation au sein de la Chancellerie fédérale (appelé "secteur TNI"). Le secteur TNI peut donner des instructions, lancer ses propres projets et soutenir les projets des départements et des offices[194]. De même, l'Office fédéral de la statistique (OFS) agit dans le domaine de l'IA comme organe de mise en réseau de compétences[195]. Au niveau cantonal et communal, il existe des délégués au numérique qui se réunissent au sein de l'assemblée des délégués de l'Administration numérique suisse.

- Suggérer des moyens et des niveaux d'action : Sur la base des éléments qui précèdent, la réflexion stratégique est l'occasion de proposer des pistes d'action, qui peuvent être de nature formelle ou matérielle. Par exemple, s'engager dans les instances internationales et européennes compétentes, dans le but d'élaborer des normes communes allant dans le sens de l'autodétermination numérique[196]. Pour les cantons, l'action recommandée se situe fréquemment au niveau intercantonal ou fédéral[197]. Il arrive également que la décision de mettre sur pied un projet national public entraîne l'exclusion d'autres solutions techniques, par exemple issues du secteur privé, élément qui est illustré par le projet d'infrastructure nationale de données de mobilité (NaDIM selon l'acronyme germanophone)[198].

Dans un deuxième temps, à l'issue de la phase de planification, la phase de mise en œuvre débute. Celle-ci peut emprunter différentes voies, parmi lesquelles l'adaptation de nouvelles bases légales, la modification de bases légales existantes[199], la création de nouveaux organes[200] ou la sélection des entreprises (devant assurer les prestations souhaitées) et qui peut intervenir aux différents échelons (fédéral, cantonal, communal)[201].

Dans un troisième temps, une phase de contrôle des normes adoptées et de leur application intervient. Ce contrôle est opéré par des instances judiciaires nationales ou internationales, mais également par des autorités de surveillance de certains secteurs d'activités. Le cas échéant, ce contrôle peut conduire à des modifications de la législation adoptée destinées à se conformer aux exigences fixées.

---

[192] DETEC/DFAE, Rapport sur la création d'espaces de données fiables, p. 40.

[193] En matière de transformation numérique des administrations, on peut songer à l'Administration numérique suisse (ANS). En matière de cyberadministration, on peut songer à la "Cyberadministration suisse", pilotée par des représentantes et représentants politiques des trois niveaux de l'État, créée en 2007 via la convention-cadre de droit public concernant la collaboration en matière de cyberadministration, les autorités étant libres de décider des conditions d'accès, de stockage et de réutilisation des données dont elles ont la responsabilité (tant qu'aucune politique publique des données n'aura été clairement définie). CONSEIL FÉDÉRAL, Stratégie suisse de cyberadministration 2020-2023, p. 5. Cf. Délégué à la cybersécurité, Direction P041 – Analyse des besoins de protection (sur la base de l'art. 11 al. 1 let. e de OPCy. Processus GRAES.

[194] CHANCELLERIE FÉDÉRALE, Transformation numérique et gouvernance de l'informatique, Secteur TNI (site web).

[195] OFS, Nouvelles informations statistiques, Réseau de compétences Intelligence artificielle, 25 août 2021 (site web).

[196] DETEC/DFAE, Rapport sur la création d'espaces de données fiables, p. 4.

[197] DÉPARTEMENT GENEVOIS DES INFRASTRUCTURES (DI), Rapport - Une politique numérique pour Genève, p. 40.

[198] Cf. ALLIANCE SWISS PASS, NaDIM, La plateforme nationale emplie de données de mobilité, 26 janvier 2021 (site web) : "*Par le biais du projet d'infrastructure nationale de données de mobilité (abrégé NaDIM de l'allemand), la Confédération lance une réunion de toutes les données de mobilité de la Suisse. La plateforme vise à relier entre elles les bases de données de tous les prestataires afin de proposer des prestations de mobilité multimodale en un seul et même endroit. L'Alliance SwissPass accompagne le projet de près. Les entreprises de transport et les communautés sont quant à elles tenues d'interrompre leurs propres projets d'infrastructures de données*".

[199] Voir par exemple le projet précité de loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (LMETA) du 4 mars 2022.

[200] Réunissant notamment des représentant·e·s des différents échelons de l'État fédéral – Voir l'exemple précité de l'entité "Cyberadministration suisse".

[201] Au niveau communal, le Conseil municipal de la Ville de Genève a voté le 28 juin 2022, sur proposition du Conseil administratif, un crédit de CHF 2'000'000.- destiné à l'implémentation de la suite bureautique Office 365 de Microsoft en Ville de Genève.

b) Répartition des compétences

Au niveau national, les principales contraintes découlent de la nature fédérale de l'État (fédéralisme). Les cantons sont en effet souverains tant que leur souveraineté n'est pas limitée par la Constitution fédérale et que leurs droits ne sont pas délégués à la Confédération (art. 3 Cst/CH). Ainsi, si l'on considère la transformation numérique (au sens large, c'est-à-dire incluant l'administration et la société) comme une **nouvelle tâche** de l'État, il s'agit aujourd'hui d'une **tâche cantonale** (en dehors des compétences propres de la Confédération pour l'administration fédérale)[202]. Dans ce contexte, de nombreuses voix prônent la mise en place de normes et standards communs à l'ensemble des échelons de l'État[203], tandis que d'autres voient, dans la diversité des solutions techniques retenues dans les différentes collectivités qui composent l'État fédéral, un atout en matière de sécurité en cas de cyberattaque[204]. On notera que ces choix résultant de la répartition des compétences et présentés comme purement techniques ont souvent des conséquences contraignantes pour les cantons, notamment puisque leurs spécificités risquent de ne pas être prises en compte suffisamment (e.g. importante population transfrontalière). Pour tenir compte de ces contraintes, des modes de collaboration plus souples peuvent être utilisés (e.g. Convention-cadre concernant la collaboration en matière de cyberadministration en Suisse)[205].

En revanche, **lorsqu'une compétence a été confiée à la Confédération** par le biais d'une modification constitutionnelle fédérale et que celle-ci a fait usage de sa compétence, les **cantons ne sont plus compétents** pour faire certains choix (e.g. en matière de transformation et de souveraineté numériques) (art. 49 Cst/CH ; primauté du droit fédéral). Ce cas de figure est illustré par le débat sur le déploiement de la technologie 5G. En 2020, à l'instar d'autres cantons romands ayant adopté un moratoire sur les technologies 4G+ et 5G (Vaud, Jura et Neuchâtel), le Grand Conseil genevois avait modifié la loi genevoise sur les constructions et sur les installations diverses (LCI/GE) pour soumettre à autorisation toute élévation, adaptation ou modification, en tout ou en partie, sur le plan physique ou logiciel, des stations émettrices. Faisant application du principe de la primauté du droit fédéral (art. 49 al. 1 Cst/CH) la Chambre constitutionnelle de la Cour de justice genevoise a annulé la disposition litigieuse, estimant que tant les télécommunications (art. 92 Cst/CH) que la protection de l'être humain et de son environnement naturel contre les atteintes nuisibles (art. 74 Cst/CH) étaient des compétences fédérales qui avaient été dûment concrétisées (en particulier dans la LTC, la LPE et plus précisément l'ORNI s'agissant des antennes de téléphonie mobile)[206].

Recommandation : au vu de ce qui précède, l'**action cantonale** dans ce domaine n'est pas inutile mais est souvent limitée. Sa portée est ainsi souvent **symbolique ou politique**. Il est recommandé de clarifier quelle "souveraineté (ou autonomie) cantonale" subsiste. Dans le doute (e.g. domaines de la

---

[202] Ce aussi longtemps du moins que la Constitution fédérale n'est pas modifiée MONTAVON, p. 53ss ; Voir le Communiqué de presse du Parlement, du mardi 18 octobre 2022, L'élimination des divergences relatives à la LMETA : la commission maintient la version du Conseil des États : les discussions récentes sur l'extension du champ d'application de la LMETA et l'opposition exprimée par les cantons.

[203] MONTAVON, p. 53ss ; Voir également l'un des objectifs identifiés dans le cadre de la mise en place de l'Administration numérique Suisse dans DFF/UPIC, Rapport Swiss Cloud, p. 34 : "*Harmonisation des compétences juridiques et techniques au niveau cantonal ou fédéral et, lorsque cela est judicieux, les rassembler*".

[204] Un tel procédé est illustré par le chantier du dossier électronique du patient (DEP), pour lequel il a été décidé d'introduire le DEP de manière décentralisée par le biais de "communautés" régionales certifiées officiellement. Cf. CONFÉDÉRATION SUISSE ET CONFÉRENCE DES DIRECTRICES ET DIRECTEURS CANTONAUX DE LA SANTÉ, Dossier électronique du patient : La phase d'introduction est en cours, 16 août 2022. Le DEP est prévu et encadré par la LDEP, adoptée en 2015 et entrée en vigueur en 2017.

[205] La Convention-cadre actuelle, adoptée par le Conseil fédéral le 24 septembre 2021 et par la Conférence des gouvernements cantonaux à l'assemblée plénière du 17 décembre 2021, a été publiée à la FF 2021 3030. Dans cette convention, la Confédération et les cantons créent notamment une organisation appelée "Administration numérique suisse" (ANS), dont la fonction est de "piloter la transformation numérique au sein du système fédéral" (art. 2 al. 1). Elle est toutefois compétente uniquement pour émettre des recommandations et non des réglementations contraignantes (art. 2 al. 3). FISCHER, notant que la collaboration ou l'harmonisation ne va pas de soi pour autant, comme le montrent les longs travaux relatifs à la mise en place d'un service national des adresses pour les tâches administratives (FISCHER Peter, Il faut trouver un équilibre entre les avantages et les inconvénients du fédéralisme, *in* ICT Journal, 23 septembre 2011 : "*L'harmonisation des registres, par exemple, a été imposée par la Confédération et a entraîné de lourdes charges pour les cantons. Au final, la plupart d'entre eux sont toutefois très satisfaits d'en voir les fruits, y compris pour d'autres projets. Mais les choses sont parfois plus difficiles, comme dans le domaine des arrivées et départs et des changements d'adresse auprès du contrôle des habitants. Nous avons ici affaire à 2750 communes et aucune d'entre elles n'a a priori intérêt à mettre en place un projet pour toute la Suisse. Dans cette initiative, l'argent de la Confédération a permis au projet de faire un grand pas et il faudra sans doute un soutien supplémentaire pour atteindre les objectifs du projet*").

[206] ACST/11/2012 du 15 avril 2021, consid. 6 et 7.

souveraineté numérique), on pourrait considérer qu'il existe une "*souveraineté (ou autonomie) cantonale*" au nom du principe de la primauté du droit fédéral et de subsidiarité[207].

c) Principe de la légalité

Dans un État de droit, la transformation numérique doit respecter le principe de la légalité (art. 5 al. 1 Cst/CH), qui exige que toute action étatique se fonde sur une base légale (exigence de la base légale) et que cette dernière soit suffisamment précise et détaillée (exigence de densité normative)[208]. La transformation numérique doit, selon nous, impérativement s'appuyer sur des **bases légales formelles** (exigence de base légale)[209]. A l'heure actuelle, une grande partie des débats et discussions qui entourent la transformation numérique concerne l'exigence d'une base légale, à l'instar de la LMETA[210] et de l'adjudication de marchés *cloud* à des prestataires privés [211]. Pourtant l'exigence de **densité normative** doit être tout autant analysée et bien utilisée. En effet, la grande complexité technique du domaine ainsi que sa constante évolution se prêtent difficilement à une réglementation exhaustive directement dans la loi. Dans une certaine mesure, il paraît donc légitime d'admettre des clauses de délégation de compétences en faveur du pouvoir exécutif[212], ainsi que des renvois à des normes techniques[213].

On peut enfin songer au recours à des **législations expérimentales**, c'est-à-dire des législations limitées, dans le temps et à des secteurs déterminés qui peuvent être ensuite évaluées et, cas échéant, pérennisées et étendues à d'autres secteurs[214]. Cette solution permettrait de se donner le temps d'apprendre et de dégager les éléments nécessaires à l'adoption d'une réglementation ultérieure définitive[215]. A Genève, ceci pourrait se fonder sur la loi concernant la législation expérimentale (LLExp/GE)[216]. Il faut encore ajouter qu'il est possible que des innovations soient proposées au niveau cantonal, s'inscrivant dans ce qu'il est convenu d'appeler le "laboratoire du fédéralisme". Ainsi, à Genève, le Grand Conseil a adopté le 22 septembre 2022 le projet de loi constitutionnel 12945-B qui propose d'introduire un art. 21A dans la Constitution cantonale consacrant un nouveau droit fondamental, le "droit à l'intégrité numérique"[217]. Cette modification doit à présent être soumise au corps électoral (art. 65 et 91 Cst/GE).

<u>Recommandation</u> : sur cette base, il est recommandé de **réfléchir** soigneusement à la **planification** de la transformation numérique, notamment du point de vue de ses **étapes** ; et adopter et/ou **modifier les bases légales** nécessaires pour que la transformation numérique respecte le principe de la légalité.

---

[207] D'autant que la subsidiarité (ou autonomie) cantonale a des avantages, notamment le fait que les cantons sont proches des administrés et qu'une décentralisation des processus peut améliorer la cybersécurité.

[208] Voir MALINVERNI et al., p. 683ss, indiquant que l'exigence de la base légale trouve sa principale justification dans le principe de l'État de droit et le principe démocratique puisqu'elle permet de ramener l'activité étatique à une loi votée par les représentantes et les représentants du peuple et soumise au référendum. ; OFK-BIAGGINI, BV 36 N 13 et BV 164 N 3-4, rappelant que le degré d'exigence dépend de la norme en cause (cf. art. 36 al. 1 et 164 al. 1 Cst/CH exigeant que les restrictions graves des droits fondamentaux respectivement les dispositions importantes soient prévues dans une loi fédérale adoptée par le parlement).

[209] Ce, vue la place qu'elle occupe qui dépasse de mesures d'organisation de l'administration. Cf. MONTAVON, p. 350ss.

[210] Message du CONSEIL FÉDÉRAL concernant la loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités du 4 mars 2022, FF 2022 804, p. 2 : "*La loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (LMETA) crée la base légale requise pour une transformation numérique efficace de l'administration fédérale ainsi que pour la collaboration entre les autorités de différentes collectivités et des tiers dans le domaine de la cyberadministration*".

[211] Voir TF, Arrêt 1C_216/2022 du 28 juillet 2022.

[212] MONTAVON, pp. 323-324 : L'auteur identifie au surplus un phénomène d'"inversion législative", qui renverse le modèle traditionnel d'élaboration et de hiérarchie des normes. Sur ce phénomène, voir FLÜCKIGER, Légistique, p. 244.

[213] Voir ZUFFEREY, p. 61ss.

[214] La transformation numérique de l'administration et de la société civile étant actuellement en pleine "phase d'apprentissage", qui se caractérise par de nombreuses incertitudes sur le plan juridique, le recours à la législation expérimentale. Cf. MONTAVON, p. 431ss ; Sur la législation expérimentale et les précautions qui doivent accompagner son usage dans un État de droit, voir FLÜCKIGER, Légistique, p. 660ss ; Voir également, dans le contexte de la pandémie de COVID-19, FLÜCKIGER, Droit expérimental, p. 142-158. *Pour une vision critique du recours à la législation expérimentale, voir* COTTIER, Cyberespace, p. 247ss.

[215] Voir OFJ, Guide de législation, p. 269, exposant les principes devant être respectés lors de la création et de l'application d'actes législatifs à caractère expérimental.

[216] Voir la LLEx/GE, dont l'article unique prévoit : "*Une loi peut être établie à titre expérimental à condition : a) qu'elle soit limitée au temps strictement nécessaire à l'expérimentation ; b) qu'elle fixe le but de l'expérimentation et les hypothèses qu'elle cherche à vérifier; c) que ses effets soient évalués dans un rapport remis sur le bureau du Grand Conseil au plus tard 3 mois avant la date prévue pour son expiration.*" *La loi expérimentale doit par ailleurs "déterminer le type de données à récolter, la démarche méthodologique, les critères d'appréciation de l'expérimentation et les organes responsables pour l'effectuer*".

[217] Voir le Projet de loi constitutionnelle modifiant la constitution de la République et canton de Genève (Cst-GE) (Pour une protection forte de l'individu dans l'espace numérique) (PL 12945), publié le 30 septembre 2022.

d) Droit des marchés publics

La transformation numérique de l'administration doit également tenir compte du droit des marchés publics, puisque les TIC sont en principe soumises au droit des marchés publics et que les contraintes de ce domaine juridique s'appliquent à l'acquisition de biens ou services par des entités administratives auprès de sociétés privées[218].

L'application du droit des marchés publics rend absolument crucial le libellé des appels d'offres et les exigences fixées par les entités adjudicatrices. A titre d'exemple, lorsque l'administration fédérale a lancé en décembre 2020 l'appel d'offres "*Public Clouds Confédération*" portant sur la fourniture de services *cloud* pendant une durée de cinq ans, elle a expressément exigé que "*[l]e soumissionnaire possède des centres de données sur au moins 3 continents (y compris au sein de l'Espace économique européen*"[219]. Ce faisant, les entreprises suisses se sont trouvées écartées de la procédure et, en juin 2021, la décision d'adjudication a sélectionné quatre entreprises provenant des États-Unis (Amazon, IBM, Microsoft et Oracle) et une de Chine (Alibaba).

Cela étant, le droit des marchés publics ménage une certaine marge de manœuvre permettant de recourir à des procédures de gré à gré, notamment en cas de solution *in-house* ou de la présence d'une entreprise unique en mesure de fournir le bien ou le service requis. On notera par ailleurs que les États européens s'intéressent aux procédés américains d'attribution des marchés publics ayant permis le développement de géants technologiques, en particulier en mettant en place des instruments qui ont permis à des petites et moyennes entreprises (PME) de s'appuyer sur la commande publique pour se développer[220].

Recommandation : sur cette base, il est recommandé d'analyser le champ d'application du droit des marchés publics (e.g. quels services informatiques sont soumis à l'AMP 2012 avec leur code de classification) et d'analyser les instruments envisageables permettant à des petites et moyennes entreprises de s'appuyer sur la commande publique pour se développer, ce en conformité avec les obligations suisses et internationales et sur la base de solutions étrangères (e.g. *Small Business Act*).

[218] Le droit des marchés publics inclut les accords ratifiés par la Suisse en matière de marchés publics, soit l'Accord de l'OMC sur les marchés publics révisé en 2012 ("AMP 2012", RS/CH 0.632.231.422) et l'Accord entre la Confédération suisse et la Communauté européenne sur certains aspects relatifs aux marchés publics conclu en 1999 (RS/CH 0.172.052.68).

[219] Voir simap.ch, projet no. 204859 (appel d'offres du 7 décembre 2020).

[220] E.g. le *Small Business Act* a orienté une part de la commande publique vers des petites entreprises, ce qui a permis à des entreprises innovantes de s'appuyer sur des clients solvables pour améliorer leurs produits et services. Pour des experts français, ce type d'instrument pourrait être déployé au niveau français pour les achats publics innovants sans contrevenir au droit européen. Voir BENHAMOU B., Souveraineté numérique.

5. Cybersécurité

La cybersécurité[221] est un élément clé dans une société numérique, en particulier vus les risques d'accès indu aux données, les risques de manipulation de l'information ou d'autres formes de cybercriminalité[222].

La cybersécurité suppose de recourir à des TIC résilientes, soit des moyens technologiques permettant d'assurer la sécurité, la confidentialité et la disponibilité des données. Le *cloud* souverain ou plus généralement le stockage des données sur un seul territoire (*résidence des données*) est souvent évoqué à cet effet[223]. Or, cette approche peut être contre-productive, du fait que plus les données sont distribuées, moins elles sont concentrées et vulnérables[224]. Il faudra plutôt passer par une **diversification des fournisseurs** de solutions matérielles et logicielles en vue de réduire les dépendances[225], en tenant compte du fait que les technologies importées – qui sont dominées par certaines entreprises – peuvent contenir des portes dérobées (*backdoors*)[226].

La cybersécurité passe aussi par une préparation adéquate en cas de cyberincident[227], laquelle suppose de développer des **compétences** (de production, décisionnelles et/ou opérationnelles), la mise en place de **contrats** permettant de garder le contrôle des données (juridique et de fait)[228] et de processus de contrôle et de conformité (*compliance*) vues les potentielles violations des réglementations en vigueur[229].

La cybersécurité passe aussi par un cadre légal clair, cas échéant par le renforcement des **instruments juridiques** en matière de cybercriminalité et de cybersécurité (e.g. infractions pénales, obligations de signaler les cyberattaques)[230]. Cela passe par des **recommandations du NCSC** et par des mesures incitatives ou contraignantes en assurant le respect[231].

---

221 CONSEIL FÉDÉRAL, Rapport sur la sécurité, p. 7 : Le domaine de la cybersécurité est entendu comme un ensemble des mesures visant à prévenir et à gérer les incidents et à améliorer la résilience face aux cyberrisques ainsi qu'à développer la coopération internationale à cet effet. De manière générale, la définition de la cybersécurité fait l'objet de controverses, qui ne seront pas approfondies dans le cadre de ce rapport.

222 Cf. DURAND, p. 91 : Ces risques sont amplifiés dans une société numérique vue la dépendance aux technologies, ce qui renforce les vulnérabilités aux cyberattaques et vue la démultiplication des acteurs, ce qui rend difficile d'allouer les responsabilités en cas de cyberattaques (e.g. avec l'internet des objets et l'IA, entre fabricants, opérateurs, programmeurs, entraineur, clients-finaux) ; DANET explique que la maîtrise des données est au cœur des opérations d'influence (e.g. manipulation de l'opinion publique), des opérations militaires, voire de la "guerre cognitive". Cf. *supra* III.2

223 TIPPER/KRISHNAMURTHY, p. 2ss, distinguent 4 approches de résilience des TIC : La 1ère approche (isolationniste) consiste à utiliser des composants nationaux et de la main d'œuvre locale pour la construction et le maintien de l'infrastructure numérique d'un État (e.g. création de Mir par la Russie pour remplacer Visa et Mastercard). La 2ème approche (coopérative) vise la conclusion de traités, d'accords et de standards internationaux pour réglementer la construction et l'exploitation des infrastructures numériques (e.g. GAIA-X au sein de l'UE). La 3ème approche (compétitive) cherche à établir des partenariats stratégiques entre l'industrie et le gouvernement, afin de promouvoir la technologie d'infrastructure numérique provenant de fournisseurs nationaux ou de confiance (e.g. *Digital Silk Road Initiative* de la Chine). La 4ème approche (militaire) vise à mobiliser des ressources militaires pour protéger l'infrastructure numérique physique et cybernétique et servir de menace de représailles aux adversaires.

224 BAUER/ERIXON, p. 11, 26ss.

225 CONSEIL FÉDÉRAL, Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense, p. 7 : Par cyberdéfense est entendu "l'ensemble des mesures prises par les services de renseignement et l'armée dans le but de protéger les systèmes critiques dont dépend la défense nationale, de se défendre contre les cyberattaques, de garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et de développer ses capacités et compétences afin qu'elle puisse apporter un appui subsidiaire aux autorités civiles ; ce domaine inclut également des mesures visant à identifier les menaces et les attaquants ainsi qu'à entraver et à bloquer les attaques". ; BAUER/ERIXON, p. 26 : Le cyberespionnage reste toutefois indétectable dans la majorité des cas de figure.

226 Et le risque de fuite de données critiques ou de cyberattaques sur des systèmes critiques. Voir BERCHTOLD Carina, Avez-vous pensé à toutes les portes dérobées?, *in* ICTJournal, 22 août 2022 ; Le marché est principalement dominé par des entreprises américaines, chinoises et quelques acteurs isolés de Corée (Samsung), de Russie (Kaspersky) et d'Allemagne (SAP). Voir SATW, Cybersecurity Map, Souveraineté (site web).

227 Une préparation adéquate en matière de cybersécurité passe traditionnellement par les 5 phases suivantes : identifier, protéger, détecter, réagir, récupérer (*NIST Core Framework*), la 1ère phase d'identification incluant notamment l'élaboration de stratégies de gestion des risques et la détermination du cadre légal. Voir aussi DEFR/OFAE, Résilience informatique, p. 14ss.

228 Parmi les engagements contractuels, on songera à l'engagement de mesures techniques et organisationnelles (e.g. cryptage des données), à l'absence d'exclusion de responsabilité en cas de violation de la confidentialité des données, à l'obligation d'informer la localisation précises des serveurs ainsi que d'éventuelles réquisitions de données par les autorités étrangères (*lawful access*).

229 TAN et al., p. 3 ; TIPPER/KRISHNAMURTHY.

230 Ces obligations sont prévues dans diverses lois et renforcent l'identification des menaces, en particulier dans la nLPD (art. 24 nLPD) et dans la LSI (art. 74a ss P-LSI). Cf. CONSEIL FÉDÉRAL, Message du 2 décembre 2022 concernant l'obligation de signaler les cyberattaques contre les infrastructures critiques, FF 2023 84.

231 Voir CHAVANNE Yannick / ZÜLLIG Yannick, Cybersécurité: la Confédération lance une campagne de prévention, *in* ICTJournal, 5 septembre 2022 ; KOLLER Rodolphe, Mobiliser les collaborateurs pour signaler les e-mails de phishing: ça marche, selon une étude suisse, *in* ICTJournal, 14 janvier 2022 ; CHAVANNE Yannick, Pourquoi les employés enfreignent les protocoles de cybersécurité, *in* ICTJournal, 7 février 2022.

A **l'international**, il serait intéressant de rechercher des solutions internationales pour protéger les civils en cas de cyberattaques étatiques[232], pour sanctionner les cyberattaques gouvernementales[233] et soumettre les entreprises technologiques aux règles de droit humanitaire[234]. Il serait aussi intéressant de développer des mesures politiques-juridiques, telles que les ambassades virtuelles (*Data-Embassies*) (i.e. stockage des données bénéficiant du statut d'immunité / inviolabilité à l'instar des missions diplomatiques)[235].

Recommandation : sur cette base, il est recommandé de s'assurer que les acteurs de la souveraineté recourent à des TIC résilientes, à des contrats incluant des TOMs, des processus de contrôle de conformité (*compliance*) et qu'ils aient les compétences nécessaires. Il est aussi recommandé de s'assurer d'un cadre légal clair, ce qui plaide pour le suivi des recommandations du NCSC et des mesures incitatives ou contraignantes en assurant le respect. A l'international, il serait intéressant de rechercher des solutions internationales pour protéger les civils en cas de cyberattaques étatiques, de soumettre les entreprises technologiques aux règles de droit humanitaire et de développer des solutions de types ambassades virtuelles (*Data-Embassies*).

---

232 Comme la Convention de Genève du numérique a été envisagée pour protéger le cyberespace. Cf. DIGITAL GENEVA TASK FORCE, A white paper to make Switzerland the core of digital governance in a secure digital world, p. 9.

233 A ce titre, on peut également se demander si l'art. 266 CP, pénalisant une atteinte à l'indépendance de la Confédération, trouvera une acception incluant la souveraineté numérique, cf. BREITENFELDT/JORDAN, p. 959ss : "*Définir l'indépendance de la Confédération est une tâche difficile, dès lors qu'il s'agit d'une notion juridique indéterminée et que, par essence, celle-ci ne se prête pas à une définition "à l'emporte-pièce". Elle est cependant étroitement liée à celle de la souveraineté nationale. Un État n'est indépendant que s'il a la faculté de s'organiser de façon souveraine ; réciproquement, il n'est souverain que s'il dispose de la faculté de régler ses affaires indépendamment des autres. Ces notions sont éminemment liées entre elles si bien que nous les considérerons, dans le cadre de cette analyse, comme identiques. La souveraineté est également un concept difficile à traiter. Elle peut être politique, et traite alors de son organisation en tant qu'État, mais elle peut être également économique, sociale, judiciaire, voire numérique*".

234 Par exemple, sur le modèle du Document de Montreux. Voir DÉPARTEMENT FÉDÉRAL DES AFFAIRES ÉTRANGÈRES (DFAE), Document de Montreux (site web) et COMITÉ INTERNATIONAL DE LA CROIX-ROUGE (CICR), Le document de de Montreux (site web).

235 L'État estonien stocke un duplicata des données critiques "dans un pays ami", afin d'assurer la continuité du système en cas d'attaque cybercriminelle grave visant les infrastructures étatiques nationales. Voir MONTAVON/SCHWAB, p. 16 ; ROBINSON et al, p. 391ss ; WGS/OCDE, p. 42ss.

6. Synthèse des réglementations suisses agissant sur la souveraineté numérique

La réglementation suisse (ou plus largement les stratégies politiques et règlementaires) agit sur les différentes composantes de la souveraineté numérique (souveraineté des données, souveraineté technologique, cyberadministration, cybersécurité) ainsi que sur les strates et les acteurs[236]. Cela peut être synthétisé dans le tableau ci-dessous[237].

Tableau 2. Evaluation synthétique des enjeux juridiques de la souveraineté numérique

	Souveraineté des données	**Souveraineté technologique**	**Cyberadministration**	**Cybersécurité**
Acteurs publics et parapublics	• Protection des données • Secrets de fonction • Lois avec effet extra-territorial (e.g. RGPD, US Cloud Act)	• Droit des marchés publics • Lois sur les télécommunications	• LMETA • OTNI	• Droit pénal • LSI • OPCy
Industrie	• Protection des données • Propriété intellectuelle • Droit de la concurrence • Droits contractuels • Lois sectorielles • Lois avec effet extra-territorial	• Propriété intellectuelle • Droit de la concurrence	• Droit des marchés publics	• Protection des données • Droit pénal • LSI • Lois sectorielles
Société civile	• Protection des données • Droits fondamentaux • Droits à l'autodétermination et à l'intégrité numérique	• Responsabilité civile • Droits fondamentaux	• Protection des données • Droits fondamentaux • Lois spécifiques (e.g. LDEP, LSIE)	• Protection des données • Droit pénal

[236] Les strates et les acteurs sont analysés de façon transversale dans cette partie III et de façon spécifique dans la partie II.

[237] Il est précisé que ce tableau contient les éléments principaux de l'analyse. Il est donc non exhaustif et susceptible d'évoluer selon l'évolution des enjeux juridiques et des compléments d'analyse. Les frontières sont par ailleurs poreuses, de sorte que certains éléments – arbitrairement attribués à l'une ou l'autre case – peuvent concerner plusieurs cases simultanément. Il est enfin précisé que ce tableau s'inspire d'un tableau synthétisant les réglementations européennes, cf. *infra* Annexe 1 (Tableaux) – Figure 14.

IV. Recommandations

Sur la base des éléments figurant ci-dessus, il est possible de formuler certaines recommandations à destination des autorités publiques afin d'accroître la souveraineté numérique de la Suisse, certaines étant tournées vers l'interne (e,g. 1-4), voire la cyberadministration (e.g. 1), d'autres étant tournées vers l'externe et les efforts à l'international (e.g. 5).

Quelques remarques générales préalables. Ces recommandations doivent être adaptées selon le degré de criticité des usages et des outils concernés[238]. Une approche purement protectionniste du problème n'est par ailleurs pas réaliste vue l'imbrication de l'écosystème numérique helvétique dans les infrastructures et les services déployés à l'échelle mondiale[239]. Il est en effet impossible de viser une maîtrise totale des TIC dans toutes leurs dimensions[240]. La souveraineté numérique signifie donc être capable de maîtriser le degré de dépendance vis-à-vis de chacun des fournisseurs et des partenaires afin de préserver les capacités économiques et politiques d'autodétermination des divers acteurs du pays[241]. L'action publique devra être enfin menée par les autorités des différents échelons (Confédération, cantons, communes) qui devront déterminer si la mise en œuvre a lieu de manière autonome ou en concertation avec d'autres institutions publiques ou privées[242].

1. Planifier et évaluer en continu la transformation numérique (cyberadministration)

- Identifier les compétences fédérales et cantonales, cas échéant proposer un principe de subsidiarité numérique, selon lequel la tâche de la confédération doit se limiter au "strict minimum" afin de laisser un maximum de souveraineté aux cantons[243] ;
- Identifier le degré de numérisation voulu (e.g. certains processus et informations classifiés pourraient ne pas être numérisés afin de limiter les risques) ;
- Avant d'investir massivement dans de nouveaux dispositifs technologiques, articuler de manière cohérente les objectifs et les ressources disponibles, d'une part, et les processus et les effets escomptés des technologies envisagées, d'autre part ;
- Préserver la capacité d'archivage et de traitement non-numérique pour les éléments les plus vitaux, afin de garantir une action publique minimale en cas d'incident majeur sur les infrastructures numériques. Dans le temps long, c'est un facteur important de stabilité.

2. Assurer l'autonomie de l'action publique

- En fonction de la criticité des données, stocker les données dans le pays et maîtriser les infrastructures essentielles aux services numériques (possiblement mais pas nécessairement à travers le développement de solutions indigènes) ;
- Diversifier les solutions technologiques et la "nationalité" des fournisseurs afin d'éviter la dépendance à une solution technologique unique et à des fournisseurs basés dans un seul pays ;
- Pour les fonctions critiques, prendre des participations dans des entreprises résidentes dont les autorités publiques dépendent ;

---

238 Cf. *supra* II.4.

239 WERTHNER, recommandant de trouver le bon équilibre entre des mesures permettant une coopération à l'international et des mesures visant à protéger l'écosystème suisse d'influence extérieures.

240 Dans le même sens que AWK, considérant qu'une souveraineté haute serait irréaliste : "*en raison des coûts élevés, du rythme plus lent de l'innovation et de la complexité des chaînes d'approvisionnement mondiales existantes dans de nombreux domaines*" et pose plusieurs niveaux de souveraineté (niveau 1 avec des exigences de base, telles que des garanties du système ; niveau 2 avec des exigences avancées, telles que le contrôle du cycle de vie de la donnée et du réseau ; niveau 3 avec exigences élevées dans les dimensions choisies, pouvant aller jusqu'au contrôle et à l'autonomie complets sur les différents aspects du cycle de vie et/ou du cadre du système.

241 SEIFRIED/BERTSCHEK, p. 11 ; POHLE, p. 15, indiquant que, sur la durée, il s'agit d'une condition à la soutenabilité de l'économie nationale.

242 Référence peut être faite ici au rapport du DETEC du 15 octobre 2019 concernant les recommandations du groupe d'experts qui indique à propos de la recommandation 25 sur les exploitants d'infrastructures critiques "*[la] Confédération et les cantons élaborent, en étroite collaboration avec les associations professionnelles, des normes de sécurité informatiques*" et à la prise de position du Conseil fédéral qui indique que d'ici fin 2020 "*le nouveau Centre de compétence en matière de cybersécurité examinera des normes de sécurité contraignantes et identifieront les solutions possibles, en collaboration avec d'autres offices et les cantons*". Voir DETEC, Avenir du traitement et de la sécurité des données, p. 10ss.

243 Cf. *supra* III.4.b.

- Poser des clauses exigeantes dans la commande publique (achats de matériels et de logiciels) ;

3. Analyser systématiquement le cadre juridique applicable

- Déterminer systématiquement et préalablement, au sein de l'État fédéral, la collectivité compétente pour légiférer sur les questions relatives à la "souveraineté numérique" ;
- Identifier précisément les contraintes et les possibilités découlant du droit international et du droit supérieur (par exemple dans le domaine du droit des marchés publics) ;
- Adopter et/ou modifier les bases légales nécessaires pour que la transformation numérique respecte le principe de la légalité ;
- Analyser les instruments envisageables permettant à des petites et moyennes entreprises de s'appuyer sur la commande publique pour se développer, ce en conformité avec les obligations suisses et internationales et sur la base de solutions étrangères (e.g. *Small Business Act*) ;
- Envisager des mesures de soutien complémentaires aux actions législatives (e.g. contrats-types, certifications, sensibilisation et formation).

4. Promouvoir le développement des technologies, des compétences et des industries dans une démarche de responsabilité selon les valeurs à promouvoir[244]

- Mettre la recherche et l'industrie au cœur des stratégies de souveraineté numérique aux différents échelons de l'État. A cette fin, prévoir des investissements financiers et humains suffisants pour développer un écosystème local fort (infrastructures et logiciels) et renforcer la collaboration avec les multinationales pour accroître les moyens financiers et la compétitivité technologique dans un cadre réglementé protecteur des intérêts suisses ;
- S'efforcer de garder la propriété intellectuelle des technologies produites en Suisse, la maîtrise de la production des technologies numériques et une capacité de contrôle de la chaine de production[245] ;
- Favoriser un usage plus parcimonieux des données personnelles par rapport aux *Big Tech*. De telles alternatives existent déjà en Suisse et pourraient s'étendre pour les navigateurs (Firefox, 5%), les moteurs de recherche (DuckDuckGo, 1%) et les systèmes d'exploitation (Linux 1%) (Figure 8, Figure 9, Figure 10), pour autant que cela n'entraîne pas de perte importante de la productivité. De telles alternatives n'existent en revanche ni pour les réseaux sociaux ni pour les terminaux (Figure 1, Figure 10) ;
- Développer ou soutenir des initiatives qui font émerger les plateformes renforçant les droits et les capacités d'actions des individus (e.g. *civic tech*), à l'instar du modèle Decidim déployé à Barcelone et à Genève ;
- Renforcer la formation et l'éducation à tous les niveaux en vue d'une littératie numérique (*Digital Litteracy*), soit une compréhension des enjeux du numérique de façon interdisciplinaire, holistique, critique et responsable[246] ;
- Impliquer et promouvoir des initiatives visant à garantir un niveau adéquat d'information de transparence et de responsabilisation des acteurs, notamment par la mise à disposition d'informations sous forme d'*Open data*, à l'instar du modèle Publish What You Pay ;
- Renforcer le droit à l'autodétermination numérique, cas échéant aussi l'intégrité numérique ;
- Poursuivre une politique cohérente d'*Open Source*, en gardant un esprit critique sur les enjeux économiques et juridiques de l'innovation ouverte (e.g. possible récupération des données ouvertes par des géants numériques et possible responsabilité des participants à l'innovation

[244] A titre exemplatif, au-delà des valeurs et droits fondamentaux auxquels on peut songer (e.g. respect de la vie privée, démocratie), l'État peut vouloir promouvoir d'autres valeurs, telles que la sobriété numérique. Notons que l'UE endosse un rôle de pionnière dans ces domaines, notamment en matière de *digital grid management*, voir WESTPHAL, p. 7 ; Les recommandations suivantes sont tirées des éléments de la présente étude ainsi que des études européennes récentes, telles que BOUNIE, AUFRECHTER/KLOSSA et IDATE DIGIWORLD, Souveraineté numérique en Europe (livre blanc), 2020.
[245] Cf. *supra* II.4.
[246] De telles formations existent naturellement dans la plupart des hautes écoles, dont l'UNIGE avec ses cours transversaux sur le numérique qui visent à monter en compétences numériques toute la communauté estudiantine. Il s'agira de renforcer de telles offres.

ouverte). Cet esprit critique passera par une prise en compte de l'Open Source lors de chaque grand projet numérique et de révisions des lois.

5. Poursuivre une action diplomatique déterminée en matière de souveraineté numérique

- Établir des objectifs de politique extérieure cohérents au niveau international, en renforçant le rôle de la "Genève internationale" afin qu'elle joue pleinement son rôle de *hub* pour les questions du numérique (*Geneva Hub*), dont les questions de souveraineté numérique[247] ;
- Poursuivre l'approche multipartite intégrant toutes les parties prenantes, en plaçant la question de souveraineté numérique au cœur des débats, dont le modèle de gouvernance basé sur l'autorégulation (souveraineté faible) ou sur la régulation nationale (souveraineté forte) ;
- Cartographier et coordonner les entités impliquées dans les relations internationales en matière de numérique, en prenant en compte – de manière transversale – non seulement les autorités fédérales, mais également les autorités cantonales ;
- Prendre en compte les territoires du numérique et les réalités technologiques, économiques, et sociétales, afin d'adopter une approche réaliste, en particulier de tenir compte des normes internationales et des effets extraterritoriaux des lois nationales touchant au numérique, afin de définir la portée des pouvoirs des autorités fédérales et cantonales sur le numérique ;
- Envisager et faire des propositions novatrices, telles que traiter les géants du numérique comme des entités politiques[248], développer des solutions globales pour protéger les civils en cas de cyberattaques étatiques et des ambassades de données (*Data-Embassies*).

* * *

[247] Cf. DFAE, Politique extérieure numérique 2021-2024, pp. 8-9, rappelant que la Suisse, et plus particulièrement la Genève internationale est un lieu d'accueil privilégié pour la gouvernance du numérique, accueillant de nombreuses organisations internationales comme le secrétariat du FGI, l'OMPI et l'UIT. Elle joue un rôle de plateforme opérationnelle avec une approche multipartite intégrant toutes les parties prenantes (gouvernements, entreprises, communauté scientifique et société civile) sur différents sujets appelant une réponse globale, dont l'Agenda 2030 et les 17 objectifs mondiaux de développement durable ; Cf. aussi COMITE D'ETUDES DE DEFENSE NATIONALE, proposant la création d'un bureau européen de la résilience pour répondre à l'extra-territorialité du droit au détriment de la souveraineté nationale.

[248] Vue leur puissance normative de fait, il paraît légitime de chercher à encadrer leur influence en vue de préserver les droits individuels et collectifs des individus, ou au moins de les soumettre aux règles de droit humanitaire.

Annexe 1 (Tableaux)

Figure 6. Échanges commerciaux de différents types de biens des TIC entre la Suisse et le reste du monde en 2021 (Source UNCTAD)

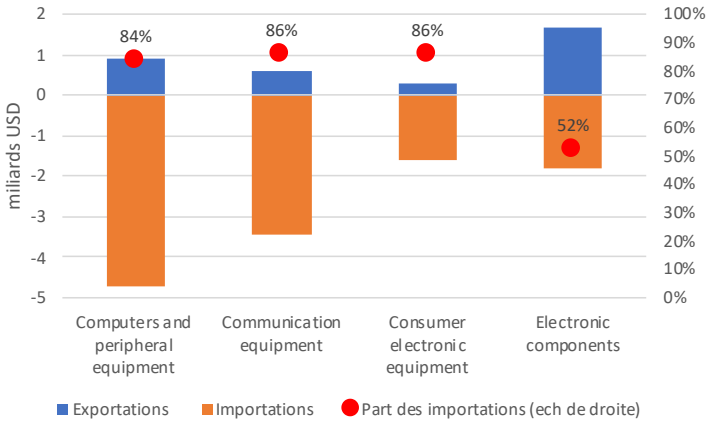


Figure 7. Parts de marché des navigateurs utilisés en Suisse en juillet 2022 (Source Statcounter)

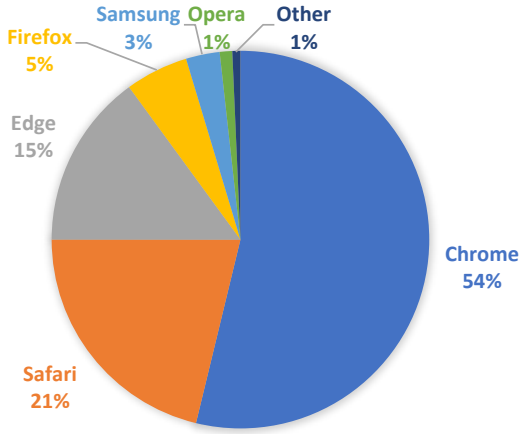


Figure 8. Parts de marché des moteurs de recherche utilisés en Suisse en juillet 2022 (Source Statcounter)

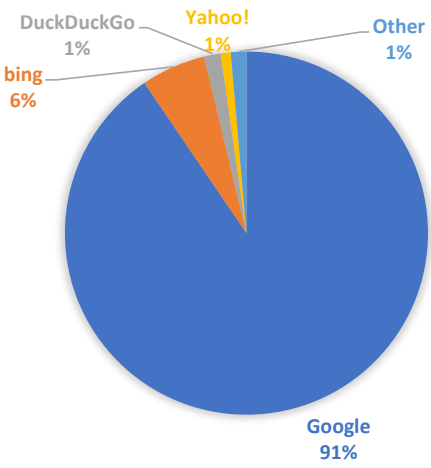


Figure 9. Parts de marché des systèmes d'exploitation utilisés en Suisse en juillet 2022 (Source Statcounter)

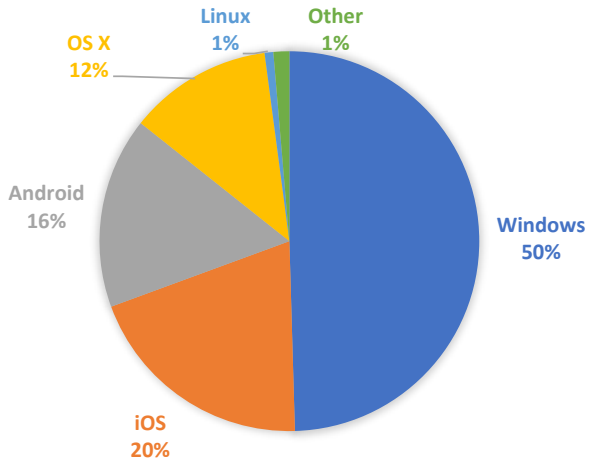


Figure 10. Parts de marché des réseaux sociaux utilisés en Suisse en juillet 2022 (Source Statcounter)

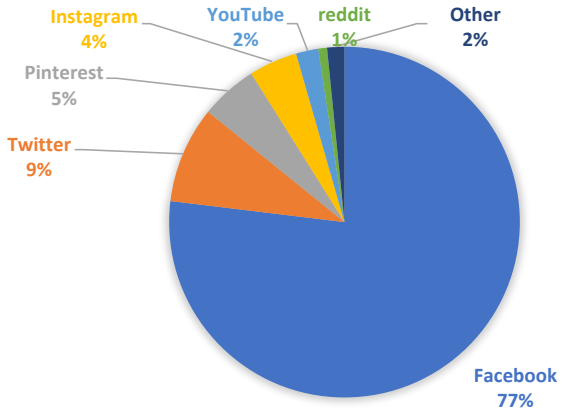


Figure 11. Nombre de brevets octroyés dans le domaine des TIC dans les principaux offices (États-Unis, Japon et Office européen) par million d'habitants en 2020 (Source WIPO)

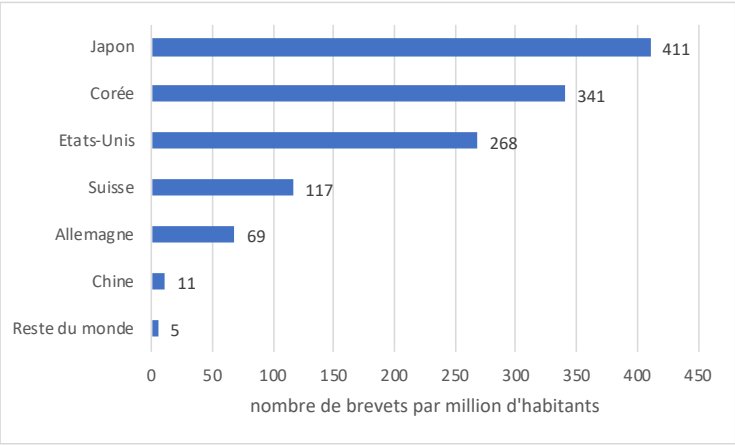


Figure 12. Répartition des brevets octroyés dans les différents sous-domaines des TIC déposés dans les principaux offices (États-Unis, Japon et Office européen) en 2020 (Source WIPO)

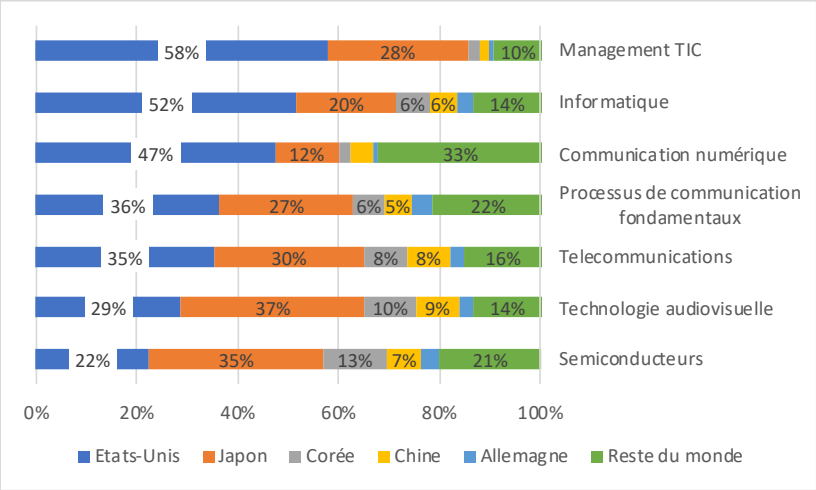


Figure 13. Parts de la Suisse dans le total des brevets octroyés par sous-domaine dans les principaux offices (États-Unis, Japon et Office européen) en 2020 (Source WIPO)

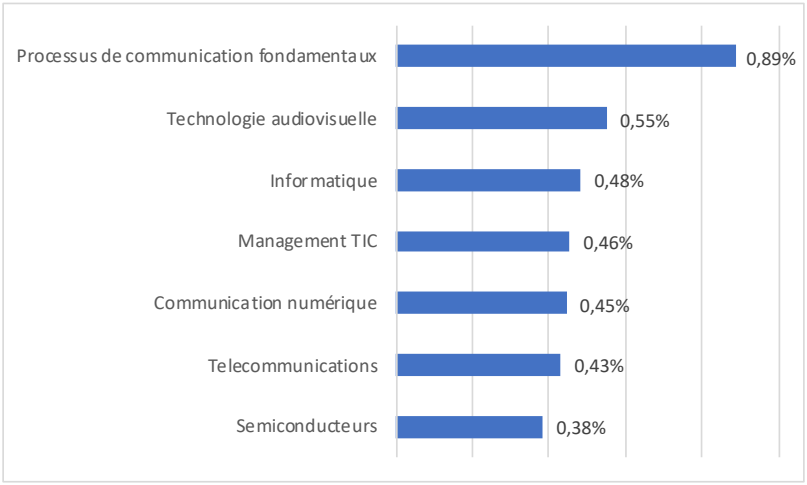
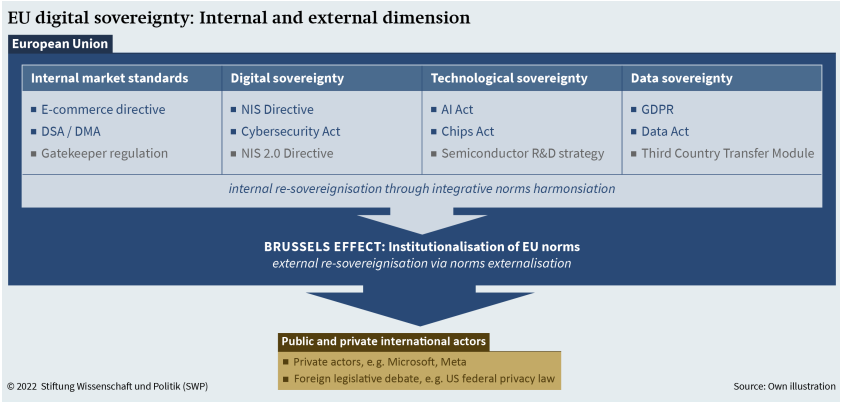


Figure 14. Exemples de réglementations européennes agissant sur différentes composantes de la souveraineté numérique (Source SWP)



Annexe 2 (Table des définitions principales de la souveraineté numérique)

Acteurs	→ Leviers d'action sur lesquels peuvent porter les politiques publiques en vue d'une → souveraineté numérique, à savoir les entités étatiques publiques et parapubliques, l'industrie et la société civile.
Autonomie	Dans le contexte du numérique, l'autonomie désigne la capacité à utiliser et contrôler les biens (matériels et immatériels) et les services numériques de manière indépendante et/ou autodéterminée.
Cloud souverain	Un environnement de *cloud computing* contrôlé, déployé et/ou géré localement au sein d'une seule juridiction.
Composantes	Dans le cadre de l'analyse de la → souveraineté numérique, les composantes principales identifiées sont la → souveraineté technologique et la → souveraineté des données.
Cyberadministration	Ce terme désigne, au sens large, les processus de transformation de l'administration et des processus numérisés eux-mêmes fournissant des prestations administratives.[249]
Cyberdéfense	Ensemble des mesures prises par les services de renseignement et l'armée dans le but de protéger les systèmes critiques dont dépend la défense nationale, de se défendre contre les cyberattaques, de garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et de développer ses capacités et compétences afin qu'elle puisse apporter un appui subsidiaire aux autorités civiles ; ce domaine inclut également des mesures visant à identifier les menaces et les attaquants ainsi qu'à entraver et à bloquer les attaques.[250]
Cyberespace	En sciences sociales, le cyberespace est considéré comme un "espace sociotechnique", car des relations sociales et politiques se tissent au sein de son infrastructure.[251]
Cybersécurité	Dans ce rapport, la cybersécurité est entendue comme un ensemble des mesures visant à prévenir et à gérer les incidents et à améliorer la résilience face aux cyberrisques ainsi qu'à développer la coopération internationale à cet effet.[252]

[249] MONTAVON, p. 25ss.
[250] CONSEIL FÉDÉRAL, Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense, p. 7.
[251] Cf. CONNOLLY et ROSSI et al. et références.
[252] CONSEIL FÉDÉRAL, Rapport sur la sécurité, p. 7.

Dépendance	Dans le contexte du numérique, la notion de dépendance vise à saisir "*la mesure dans laquelle les acteurs d'un pays donné doivent s'appuyer sur des technologies numériques contrôlées par des entités étrangères pour exercer des activités numériques*"[253]. Il s'agit de données structurelles qui affectent en amont les capacités de la puissance publique d'un pays donné à réguler le domaine numérique et plus largement à exercer ses prérogatives dans les domaines régaliens, économiques et concernant la protection des droits individuels et collectifs des citoyen·ne·s.
Dimensions	Dans ce rapport, les dimensions de la → souveraineté numérique sont régalienne, économique et citoyenne.
Leviers d'action	En écho aux → dimensions de la souveraineté numérique, → acteurs sur lesquels peuvent porter les politiques publiques en vue d'une → souveraineté numérique.
Souveraineté	D'un point de vue juridique, la souveraineté se réfère au → territoire d'un État, soit à l'acteur souverain qu'est la nation (i.e. souveraineté externe) et qui a le monopole sur les règles de droit et la force publique (e.g. police ou justice) (i.e. souveraineté interne).
Souveraineté des données	La capacité d'utilisation et de contrôle des entités politiques sur les données.
Souveraineté numérique	Le développement d'une autonomie stratégique en matière de numérique. Il s'agit du droit et de la capacité des entités politiques à pouvoir utiliser et contrôler de manière autonome (i.e. de manière indépendante et/ou autodéterminée) les biens matériels et immatériels et les services numériques qui impactent significativement la démocratie, l'économie et la société.
Souveraineté technologique	La capacité d'utilisation et de contrôle des entités politiques sur les *hardwares*, les *softwares*, les infrastructures et les services numériques ("sous-composantes").
Souveraineté sur les réseaux	Exercice de la souveraineté sur le réseau mondial de communications interconnectées.
Strates	Terme utilisé pour conceptualiser la → souveraineté sur les réseaux. Dans ce rapport, ces réseaux (nouvelles formes de territoires) sont composés de 3 strates sur lesquelles l'État peut exercer son autorité : (1) → strate physique (2) → strate logique et (3) → strate des données.

[253] LU/MAYER, p. 5.

Strate des données	Strate territoriale sur laquelle se situent les données circulant sur les réseaux. La strate des données étant dénuée de territoire physique défini, l'État peut y exercer une autorité limitée, sous réserve d'une nationalisation du → cyberespace.
Strate logique	Strate territoriale sur laquelle se situent les codes et les normes régissant les composants TIC (e.g. attribution des adresses IP et des noms de domaine, administration des serveurs racine du DNS) et rendant possibles l'échange d'informations entre eux. La strate logique n'étant pas rattachée à un territoire physique défini, l'État peut y exercer une autorité limitée, sous réserve d'une nationalisation du → cyberespace.
Strate physique	Strate territoriale sur laquelle se situent les composants TIC, sur lesquels l'État peut exercer une autorité territoriale exclusive.
Territoire	Dans une perspective socio-économique, les territoires du numérique sont conceptualisés en → strates.
Transformation numérique	De manière générale, la transformation numérique est le processus d'encodage d'éléments de données dans des formats numériques, transformant des données analogiques en format lisible par ordinateur, en vue de leur transmission, de leur réutilisation et du traitement de l'information.[254]

[254] TAN et al., p. 1.

Annexe 3 (Questionnaire)

Questions générales

- Quelle est votre définition/vision de la souveraineté numérique ?
- Dans votre domaine d'expertise, quels sont – selon vous – les enjeux autour de la souveraineté numérique ?
- Selon vous, quelles mesures concrètes – tout domaine confondu – sont propres à renforcer la souveraineté numérique suisse, aux niveaux fédéral, cantonal, et/ou communal ?
- Selon vous, la mise en place d'un "cloud souverain" est-elle nécessaire dans le cadre des politiques publiques suisses, cantonales et/ou communales ?
  Si oui/non, pourquoi ?
- Avez-vous d'autres remarques, suggestions ou questionnements au sujet de la « souveraineté numérique » ?

Computer science et systèmes d'information

- Selon vous, est-ce qu'un "cloud souverain" garantirait mieux la protection des données de l'administration publique et de la population ?
- Identifiez-vous des "infrastructures technologiques" – hardware et software – qui seraient plutôt bénéfiques ou néfastes pour la "souveraineté numérique" suisse, cantonale et/ou communale ?
- Considérez-vous que la Suisse et/ou l'administration publique soit "dépendante" des technologies étrangères ? (Mots-clés : *cloud*, USA, Chine)
- Quels sont, dans votre domaine d'expertise, les plus grands *challenges* de la Suisse dans sa gouvernance du numérique ? (Mots-clés : transformation numérique, stratégie du numérique)
- Est-ce que la stratégie numérique de la Suisse est suffisante, afin de garantir sa "souveraineté numérique" ?
- Quels sont les risques liés à l'*open source* ?
- Considérez-vous que le marché suisse soit prêt à répondre aux besoins de "souveraineté numérique" de l'administration publique et de la population suisse à un niveau fédéral, cantonal et/ou communal ?

Sociologie

- Quelles entités sont concernées – directement ou indirectement – par la "souveraineté numérique" et comment ?
- La question de la "souveraineté numérique" appelle-t-elle à une redéfinition des "territoires" ?
- Quel est le rôle de l'État dans le cadre des questions de "souveraineté numérique" ?

Économie

- Considérez-vous que les politiques publiques en matière de "souveraineté numérique" constituent généralement un frein à l'innovation ?
- Considérez-vous que la Suisse soit « dépendante » des technologies étrangères ? (Mots-clés : *cloud*, USA, Chine)
- Pensez-vous que les GAFAM ont une influence négative sur la "souveraineté numérique" suisse, cantonale et/ou communale ?
- Considérez-vous que le marché suisse soit prêt à répondre aux besoins de "souveraineté numérique" de l'administration publique et de la population suisse à un niveau fédéral, cantonal et/ou communal ?

Droit

- Quels domaines juridiques sont particulièrement touchés par la question de la « souveraineté numérique » ?
- Est-ce qu'un "cloud souverain" garantirait mieux la protection des données de l'administration publique et de la population ?
- Le cadre légal actuel – et à venir – est-il suffisant, afin de garantir la "souveraineté numérique" des administrations publiques et de la population suisse ?
- Une réglementation des marchés publics visant à favoriser les "technologies locales" serait-elle possible ? Au contraire, les appels d'offre en matière de technologies discriminent-ils les entreprises suisses ?
- Identifiez-vous des *challenges* liés au fédéralisme, dans le cadre de l'élaboration de politiques publiques en matière de "souveraineté numérique" ?
- Quelles sont les implications du secret de fonction dans le cadre de l'utilisation de services *cloud* ?

Table des abréviations

4G+	Norme de réseau de téléphonie mobile correspondant au LTE-Advanced (4ème génération)
5G	Norme de réseau de téléphonie mobile succédant à la 4G (5ème génération)
6G	Norme de réseau de téléphonie mobile en développement, qui pourrait succéder à la 5G (6ème génération)
Al.	Alinéa(s)
AP	Avant-projet
AP-LPD	Avant-projet de révision totale de la loi fédérale sur la protection des données mis en consultation le 21 décembre 2016
AP-LSI	Avant-projet de modification de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (Loi sur la sécurité de l'information, LSI) mis en consultation le 12 janvier 2022
Art.	Article(s)
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
BaK	*Basler Kommentar*
Big Tech	Nom donné aux entreprises les plus dominantes de l'industrie des technologies de l'information
BHATX	Acronyme des géants du web chinois, à savoir Baidu, Huawei, Alibaba, Tencent et Xiaomi.
CC	Code civil suisse du 10 décembre 1907 (RS/CH 210)
CEDH	Convention européenne des droits de l'homme du 4 novembre 1950, ratifiée par la Suisse en 1974 (RS/CH 0.101)
Cf.	*Confer*
Ch.	Chiffre
CJUE	Cour de justice de l'Union européenne (anciennement CJCE : Cour de justice des communautés européennes)
Cloud Act	*Clarifying Lawful Overseas Use of Data Act* (États-Unis)
Charte ONU	Charte des Nations Unies du 26 juin 1945 (RS/CH 0.120)
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/CH 220)
COMCO	Commission de la concurrence
Consid.	Considérant
Convention 108	Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, ratifiée par la Suisse en 1997 (RS/CH 0.235.1)
CP	Code pénal suisse (RS/CH 311.0)

CPC	Code de procédure civile du 19 décembre 2008 (RS/CH 272)
CR	Commentaire romand
Cst/CH	Constitution fédérale de la Confédération suisse du 18 avril 1999 (RS/CH 101)
Cst/GE	Constitution de la République et canton de Genève du 14 octobre 2012 (RS/GE A 2 00)
Cst/VD	Constitution du canton de Vaud du 14 avril 2003 (RS/VD 101.01)
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
DGA	*European Data Governance Act*
DNS	*Domain Name System*
e.g.	*Exempli gratia*
e-ID	Moyen d'identification électronique
édit.	Editeur·ice·s
EDPB	*European Data Protection Board (en français : Comité Européen de la Protection des Données)*
ENISA	Agence de l'Union européenne pour la cybersécurité
Et al.	*Et alii*
etc.	*Et caetera*
FF	Feuille fédérale
FGI	Forum de l'ONU sur la gouvernance de l'Internet
FINMA	Autorité fédérale de surveillance des marchés financiers
FSA	*U.S. Federal Security Agency*
GAFAM	Acronyme des géants du web étasuniens, à savoir Google (Alphabet), Apple, Facebook (Meta), Amazon et Microsoft
GPL	*General public license*
i.e.	*Id est*
Ibid.	*Ibidem*
ICANN	*Internet Corporation for Assigned Names and Numbers*
IDN	*Internationalized domain name*
IP	*Internet protocol*
IPI	Institut fédéral de la propriété intellectuelle
IPv6	*Internet Protocol version 6*
JdT	Journal des tribunaux

JOUE	Journal officiel de l'Union européenne
KET	*Key enabling technology*
LB	Loi fédérale du 8 novembre 1934 sur les banques et les caisses d'épargne (Loi sur les banques, LB) (RS/CH 952.0)
LCD	Loi fédérale du 19 décembre 1986 contre la concurrence déloyale (RS/CH 241)
LCI/GE	Loi genevoise du 14 avril 1988 sur les constructions et les installations diverses (RS/GE L 5 05)
LCyb/FR	Loi fribourgeoise du 18 décembre 2020 sur la cyberadministration (RS/FR 184.1)
LDEP	Loi fédérale du 19 juin 2015 sur le dossier électronique du patient (RS/CH 816.1)
LDIP	Loi fédérale du 18 décembre 1987 sur le droit international privé (RS/CH 291)
LEFin	Loi fédérale du 15 juin 2018 sur les établissements financiers (RS/CH 954.1)
Lit.	*Litera*
LLEx/GE	Loi genevoise du 14 décembre 1995 concernant la législation expérimentale (RS/GE A 2 35)
LMETA	Loi fédérale du 4 mars 2022 sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (FF 2022 805)
LPD	Loi fédérale du 19 juin 1992 sur la protection des données (RS/CH 235.1)
LPE	Loi fédérale du 7 octobre 1983 sur la protection de l'environnement (RS/CH/ 814.01)
LPrD/VD	Loi vaudoise du 11 septembre 2007 sur la protection des données personnelles (RS/VD 172.65)
LSI	Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (RS/CH 128)
LTC	Loi fédérale du 30 avril 1997 sur les télécommunications (RS/CH 784.10)
N	Note marginale
n.	Note de bas de page
NaDIM	Infrastructure nationale de mise en réseau des données sur la mobilité
NCSC	Centre national pour la cybersécurité
nLPD	Loi fédérale du 25 septembre 2020 sur la protection des données (RS 235.1), qui entrera en vigueur le 1er septembre 2023 (RO 2022 491)
No.	Numéro
not.	notamment
OCDE	Organisation de coopération et de développement économiques
OFAE	Office fédéral de l'approvisionnement économique du pays
OFJ	Office fédéral de la justice
OFS	Office fédéral de la statistique
OIAF	Ordonnance du 9 décembre 2011 sur l'informatique et la télécommunication dans l'administration fédérale (RS/CH 172.010.58)

OMC/WTO	Organisation mondiale du commerce
OMPI/WIPO	Organisation mondiale de la propriété intellectuelle
ONU	Organisation des Nations Unies
op. cit.	*Opere citato*
OPCy	Ordonnance du 27 mai 2020 sur les cyberrisques (RS/CH 123.73)
ORNI	Ordonnance du 23 décembre 1999 sur la protection contre le rayonnement non ionisant (RS/CH 814.710)
OSI	*Open Systems Interconnection*
OTNI	Ordonnance du 25 novembre 2020 sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale, RS/CH 172.010.58.
P-LSI	Projet de loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (Loi sur la sécurité de l'information, LSI), FF 2020 9665
Pacte ONU II	Pacte des Nations Unies sur les droits civils et politiques du 16 décembre 1966, ratifié par la Suisse en 1991 (RS/CH 0.103.2)
Par.	Paragraphe
PFPDT	Préposé fédéral à la protection des données et à la transparence
PME	Petites et moyennes entreprises
Privacy Shield	*Swiss-US Privacy Shield* (bouclier de protection des données personnelles) du 12 avril 2017.
Privatim	Conférence des préposé·e·s suisses à la protection des données
RGPD	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4 mai 2016, p. 1-88
RO	Recueil officiel
RS	Recueil systématique
Schrems I	Décision C-362/14 de la CJUE invalidant le *EU-U.S. Safe Harbor*, publiée le 6 octobre 2015.
Schrems II	Décision C-311/18 de la CJUE invalidant le *EU-U.S. Privacy Shield*, publiée le 16 juillet 2020.
SECO	Secrétariat d'État à l'économie
ss.	Suivant·e·s
SUVA	Caisse nationale suisse d'assurance en cas d'accidents
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
TFUE	Version consolidée du Traité sur le fonctionnement de l'Union européenne du 30 mars 2010, JOUE C 83/47

TIC	Technologies de l'information et de la communication
TOM	*Technical and organisational measures*
UE	Union européenne
UIT	Union internationale des télécommunications
UNCTAD	Conférence des Nations Unies sur le commerce et le développement
UPIC	Unité de pilotage informatique de la Confédération
Vol.	Volume
WIPO/OMPI	World Intellectual Property Organization
y.c.	Y compris

Bibliographie

Publications d'offices et départements fédéraux

CHANCELLERIE FÉDÉRALE, Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung : Bericht in Umsetzung vom Meilenstein 5 der Cloud-Strategie des Bundesrates, 31 août 2022.

DÉPARTEMENT FÉDÉRAL DE L'ÉCONOMIE, DE LA FORMATION ET DE LA RECHERCHE (DEFR) / OFFICE FÉDÉRAL DE L'APPROVISIONNEMENT ÉCONOMIQUE DU PAYS (OFAE), Norme minimale pour améliorer la résilience informatique, 2018 (cité : DEFR/OFAE, Résilience informatique).

DÉPARTEMENT FÉDÉRAL DE L'ENVIRONNEMENT, DES TRANSPORTS, DE L'ÉNERGIE ET DE LA COMMUNICATION (DETEC), Rapport sur les recommandations du groupe d'experts sur l'avenir du traitement et de la sécurité des données, Prise de connaissance et suite de la procédure, 15 octobre 2019 [https://www.newsd.admin.ch/newsd/message/attachments/58797.pdf] (12.10.22) (cité : DETEC, Avenir du traitement et de la sécurité des données).

DÉPARTEMENT FÉDÉRAL DE L'ENVIRONNEMENT, DES TRANSPORTS, DE L'ÉNERGIE ET DE LA COMMUNICATION (DETEC) / DÉPARTEMENT FÉDÉRAL DES AFFAIRES ÉTRANGÈRES (DFAE), Rapport sur la création d'espaces de données fiables, sur la base de l'autodétermination numérique, Berne, 2022 [https://www.newsd.admin.ch/newsd/message/attachments/70837.pdf] (12.10.22) (cité : DETEC/DFAE, Rapport sur la création d'espaces de données fiables).

DÉPARTEMENT FÉDÉRAL DES AFFAIRES ÉTRANGÈRES (DFAE), Stratégie Chine 2021-2024, Berne, 2021, [https://www.eda.admin.ch/eda/fr/dfae/dfae/publikationen.html/content/publikationen/fr/eda/schweizer-aussenpolitik/China_Strategie_2021-2024.html] (12.10.22) (cité : DFAE, Chine 2021-2024).

DÉPARTEMENT FÉDÉRAL DES AFFAIRES ÉTRANGÈRES (DFAE), Stratégie de politique extérieure numérique 2021–2024, Berne, 2020 [https://www.eda.admin.ch/content/dam/eda/fr/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_FR.pdf] (12.10.22) (cité : DFAE, Politique extérieure numérique 2021-2024).

DÉPARTEMENT FÉDÉRAL DES FINANCES (DFF) / CENTRE NATIONAL POUR LA CYBERSÉCURITÉ (NCSC), Rapport explicatif relatif à l'ouverture de la procédure de consultation concernant l'inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques, Modification de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information, LSI) [https://www.newsd.admin.ch/newsd/message/attachments/69898.pdf] (12.10.22) (cité : DFF/NCSC, Modification LSI).

DÉPARTEMENT FÉDÉRAL DES FINANCES (DFF) / UNITÉ DE PILOTAGE INFORMATIQUE DE LA CONFÉDÉRATION (UPIC), Rapport sur l'évaluation des besoins d'un nuage informatique suisse ("Swiss Cloud"), Berne, décembre 2020 (cité : DFF/UPIC, Rapport Swiss Cloud).

OFFICE FÉDÉRAL DE LA JUSTICE (OFJ), Le Guide de législation, Guide pour l'élaboration de la législation fédérale, 4ème éd. 2019 [https://www.bj.admin.ch/dam/data/bj/staat/legistik/hauptinstrumente/gleitf-f.pdf] (12.10.22) (cité : OFJ, Guide de législation).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), Explications concernant l'informatique en nuage (*cloud* computing), [https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/cloud-computing/explications-concernant-l-informatique-en-nuage--cloud-computing.html] (06.03.2021) (cité : PFPDT, Cloud computing).

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 (cité : PFPDT, Guide juin 2021).

ROBERTS Tony / HERNANDEZ Kevin / FAITH Becky / PRIETO MARTIN Pedro, Key Issues in Digitalisation and Governance, Berne (Direction du développement et de la coopération), mars 2022 (cité : ROBERTS et al.).

Sources scientifiques

ALCAUD David, Souveraineté, *in* Encyclopædia Universalis [https://www.universalis-edu.com/encyclopedie/souverainete/] (12.10.22).

AUFRECHTER Fabien / KLOSSA Guillaume, Pour une souveraineté numérique européenne, Concilier indépendance et attractivité, Paris (EuropaNova) 2022.

BAISCHEW Dajan / KROON Peter / LUCIDI Stefano / Märkel CHRISTIAN / SÖRRIES Bernd, Digital Sovereignty in Europe – a first benchmark, Bad Honnef (WIK Consult) 2020 (cité : BAISCHEW et al.).

BALDWIN Richard E., The great convergence: information technology and the new globalization, Cambridge / Massachusetts (The Belknap Press of Harvard University Press), 2016.

BALSMEIER Benjamin / WOERTER Martin, Is this time different? How digitalization influences job creation and destruction, *in* The Digital Transformation of Innovation and Entrepreneurship, 2019, vol. 48, no 8.

BARRINHA André / CHRISTOU George, Speaking sovereignty: the EU in the cyber domain, *in* European Security, 2022, vol. 31, no 3, p. 356ss.

BAUER Matthias / ERIXON Fredrik, Europe's quest for technology sovereignty: Opportunities and pitfalls, *in* European Centre for International Political Economy (ECIPE) Occasional Paper, No. 02/2020.

BAUR Andreas, European Dreams of the Cloud Imagining Innovation and Political Control, *in* Geopolitics, 2023.

BELLI Luca, Structural Power as a Critical Element of Digital Platforms Private Sovereignty (non-final draft), *in* EDOARDO Celeste / HELDT Amélie / IGLESIAS KELLER Clara (édit.), Constitutionalising Social Media, 2022.

BENDIEK Annegret / STÜRZER Isabella, Advancing European internal and external digital sovereignty: The Brussels effect and the EU-US Trade and Technology Council, *in* Stiftung Wissenschaft und Politik (SWP) Comment, 2022, no. 20.

BENHAMOU Bernard, Souveraineté numérique : quelles stratégies pour la France et l'Europe ? [https://www.vie-publique.fr/parole-dexpert/276126-souverainete-numerique-quelles-strategies-pour-la-france-et-leurope] (12.10.22) (cité : BENHAMOU B., Souveraineté numérique).

BENHAMOU Yaniv, Big Data and the Law: a holistic analysis based on a three-step approach – Mapping property-like rights, their exceptions and licensing practices, *in* Revue suisse de droit des affaires et du marché financier (RSDA), 2020, no. 4, p. 393ss (cité : BENHAMOU Y., RSDA).

BENHAMOU Yaniv / TRAN Laurent, Circulation des biens numériques: de la commercialisation à la portabilité, *in* sic! 2016, no 11, p. 571ss.

BERTANI Sebastiano / CACCIA Andrea / MASSIMO Fabio / ALLARD Jean-Luc / TUMIETTO Daniele, White Paper on Digital Sovereignty, Bruxelles (European Digital SME) 2021 (cité : BERTANI et al.).

BIAGGINI Giovanni, BV Kommentar, 2ème éd., Zurich (Orell Füssli) 2017 (cité : OFK-AUTEUR).

BLANDIN-OBERNESSER Annie, Les entreprises souveraines de l'Internet : un défi pour le droit en Europe, *in* BLANDIN-OBERNESSER Annie (édit.), Droits et souveraineté numérique en Europe, Bruxelles (Bruylant), 2016, p. 95ss

BOIZARD Maryline, La tentation de nouveaux droits fondamentaux faee à Internet : vers une souveraineté individuelle ? Illustration à travers le droit à l'oubli numérique, *in* BLANDIN-OBERNESSER Annie (édit.), Droits et souveraineté numérique en Europe, Bruxelles (Bruylant), 2016, pp. 31-56.

BOUNIE David, Digital Strategic Autonomy: Industry Views and EU Policy Implications, *in* POGOREL Gérard / NESTORAS Antonios / CAPPELLETTI Francesco (édit.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles (European Liberal Forum) 2022, pp. 3-6.

BRADFORD Anu, The Brussels effect: how the European Union rules the world, New York (Oxford University Press) 2020.

BREITENFELDT Friedo / JORDAN Sylvain, Atteinte à l'indépendance de la Confédération, *in* AJP/PJA 2022, vol. 9, p. 959ss.

BRUNESSEN Bertrand (édit.), La politique européenne du numérique, Bruxelles (Bruylant) 2023.

BÜCHEL Jan / ENGELS Barbara, The Importance of the Data Economy for Europe's Digital Strategic Autonomy, *in* POGOREL Gérard / NESTORAS Antonios / CAPPELLETTI Francesco (édit.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles (European Liberal Forum) 2022, pp. 13-18.

BURGFRIED Andreas / RECKERT-LODDE Andreas, Die Deutsche Verwaltungscloud-Strategie, Auf dem Weg zur Digitalen Souveränität, *in* Datenschutz und Datensichercheit (DuD), 2022, vol. 46, no. 10, p. 611ss.

BURWELL Frances G. / PROPP Kenneth, Issue brief - The European Union and the Search for Digital Sovereignty - Building "Fortress Europe" or Preparing for a New World?, *in* Atlantic Council, 22 juin 2020.

CASSART Alexandre, Premières réflexions sur le Cloud Act : contexte, mécanismes et articulations avec le RGPD, *in* Revue du droit des technologies de l'information, 2018, vol. 73, p. 41ss.

CELESTE Edoardo, Digital Sovereignty in the EU: Challenges and Future Perspectives, *in* FABBRINI Federico / CELESTE Edoardo / QUINN John (édit.), Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty, Oxford (Hart Publishing) 2021, pp. 211-228.

CHANDER Anupam / SUN Haochen, Sovereignty 2.0, *in* Vanderbilt Journal of Transnational Law, 2022, vol. 55, no 2, p. 283ss.

CHAPDELAINE Pascale / MCLEOD ROGERS Jaqueline, Contested Sovereignties: States, Media Platforms, Peoples, and the Regulation of Media Content and Big Data in the Networked Society, *in* Laws, 2021, vol. 10, no 66.

CHRÉTIEN Jennyfer / DROUARD Étienne, European technological sovereignty, Paris (Renaissance Numérique) 2022 [https://www.renaissancenumerique.org/wp-content/uploads/2022/01/renaissancenumerique_note_souverainetetechnologique.pdf] (10.10.22).

COMITE D'ETUDES DE DEFENSE NATIONALE, Extraterritorialité et coercition économique : Quelles solutions pour la France et l'Europe face à des pratiques internationales d'extraterritorialité du droit ?, *in* REVUE DEFENSE NATIONALE, 2022, vol. 4, no. 849, p. 66ss.

CONNOLLY Randy, Why computing belongs within the social sciences, *in* Communications of the ACM, 2020, vol. 63, no. 8, p. 54ss.

CORY Nigel / DASCOLI Luke, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, *in* Information Technology & Innovation Foundation (ITIF), 19 juillet 2021 [https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost [https://perma.cc/D4LN-H5T8] (18.01.23).

COTTIER Bertil, La privatisation de la fonction législative ou la face sombre de la révolution numérique, *in* LeGes, 2019, vol. 30, no 3 (cité : COTTIER, Privatisation).

COTTIER Bertil, Le droit "suisse" du cyberespace ou le retour en force de l'insécurité juridique et de l'illégitimité, *in* ZSR/RDS 2015, vol. 134, no. 2, p. 205ss (cité : COTTIER, Cyberespace).

COUTURE Stéphane / TOUPIN Sophie, What Does the Concept of "Sovereignty" Mean in Digital, Network and Technological Sovereignty?, *in* New Media & Society, 2019, vol. 21, no. 10, p. 2305ss.

CREEMERS Rogier, China's conception of cyber sovereignty: rhetoric and realization, *in* BROEDERS Dennis / VAN DEN BERG Bibi (édit.), Digital Technologies and Global Politics, Lanham (Rowman & Littlefield) 2020, pp. 107-142.

CRESPI Francesco / CARAVELLA Serenella / MENGHINI Mirko / SALVATORI Chiara, European Technological Sovereignty: An Emerging Framework for Policy Strategy, *in* Inter Economics, 2021, vol. 56, no 6, p. 348ss (cité : CRESPI et al.).

DANET Didier, L'enjeu des données pour la cyberdéfense, *in* Annales des Mines - Réalités industrielles, 2022, vol. 3, p. 88ss.

DANET Didier / DESFORGES Alix, Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques, *in* Hérodote, 2020, vol. 177-178, no 2-3 (2020), p. 179ss.

DE WERRA Jacques, Entreprises et Big Data : peut-on forcer les entreprises à partager leurs données non personnelles (par des licences obligatoires ou des licences "FRAND")?, *in* Revue suisse de droit des affaires et du marché financier (RSDA), 2020, vol. 92, no 4, p. 365ss (cité : DE WERRA, RSDA).

DE WERRA Jacques, Perspective "Inside-Out", Défis du droit d'auteur dans un monde connecté, *in* sic! 2014, p. 194ss (cité : DE WERRA, sic!).

DUCHEINE Paul A. L., Military Cyber Operations, *in* DIETER Fleck / GILL Terry D. (édit.), The Handbook of the International Law of Military Operations, 2ème edition, Oxford (Oxford University Press), 2015, pp. 458-475.

DURAND Cédric, Technoféodalisme, Critique de l'économie numérique, Paris (Zones) 2020.

DURAND Cédric / RIKAP Cecilia, Intellectual monopoly capitalism - challenge of our times, 5 octobre 2021 [https://socialeurope.eu/intellectual-monopoly-capitalism-challenge-of-our-times] (22.10.22).

EDLER Jakob / BLIND Knut / KROLL Henning / SCHUBERT Torben, Technology Sovereignty as an Emerging Frame for Innovation Policy – Defining Rationales, Ends and Means, Fraunhofer ISI Discussion Papers Innovation Systems and Policy Analysis No. 70, juillet 2021 (cité : EDLER et al.).

ERGAS Henry / BRANIGAN Joe, Digital Strategic Autonomy: An Australian Perspective, *in* POGOREL Gérard / NESTORAS Antonios / CAPPELLETTI Francesco (édit.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles (European Liberal Forum) 2022, pp. 75-84.

FABIANO Nicola, Digital Sovereignty Between "Accountability" and the Value of Personal Data, *in* Advances in Science, Technology and Engineering Systems Journal, 2020, vol. 5, no 3, p. 270ss.

FALKNER Gerda / HEIDEBRECHT Sebastian / OBENDIEK Anke / SEIDL Timo, Digital Sovereignty-Rhetoric and Reality, Framework Paper, 2022 (cité : FALKNER et al.).

FLORIDI Luciano, The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, *in* Philosophy & Technology, septembre 2020, vol. 33, no 3, p. 369ss.

FLÜCKIGER Alexandre, Le droit expérimental : Potentiel et limites en situation épidémiologique extraordinaire, *in* Sécurité et droit, 2020, vol. 3, p. 142ss (cité : FLÜCKIGER, Droit expérimental).

FLÜCKIGER Alexandre, (Re)faire la loi : Traité de légistique à l'ère du droit souple, Berne (Stämpfli) 2019, p. 244 (cité : FLÜCKIGER, Légistique).

GANNE Emmanuelle, Can Blockchain revolutionize international trade ?, Genève (OMC) 2018.

GOLDMAN James E., Network Concepts, *in* WHITAKER Jerry C. (édit.), Systems Maintenance Handbook, 2ème edition, Boca Raton / London / New York / Washington D.C. (CRC Press) 2002.

GOLLIEZ André, Souveraineté des données, *in* SCHÄRER Claudia (édit), Technology Outlook 2021, Zurich / Lausanne (Schweizerische Akademie der Technischen Wissenschaften) avril 2021.

GÖTZINGER Lena, Public-Cloud-Bericht der Bundesverwaltung, 15 octobre 2022 [https://datenrecht.ch/public-cloud-bericht-der-bundesverwaltung/] (12.10.22).

GROTH Olaf / STRAUBE Tobias, Analysis of current global AI developments with a focus on Europe, Berlin (Konrad-Adenauer-Stiftung) 2020.

GUEHAM Farid, Vers la souveraineté numérique, Paris (Fondation pour l'innovation politique) 2017.

HASKEL Jonathan / WESTLAKE Stian, Capitalism without capital: the rise of the intangible economy, Princeton / Oxford (Princeton University Press) 2018.

HONG Yu / GOODNIGHT Thomas G., How to think about cyber sovereignty: the case of China, *in* Chinese Journal of Communication, 2020, vol. 13, no. 1, p. 8ss.

ILLGNER Klaus (édit.), Technological Sovereignty: Methodology and Recommandations, Frankfurt am Main (Verband der Elektrotechnik) 2020.

JÄGER Wilfried / NENTWICH Michael / EMBACHER-KÖHLE Gerhard / KRIEGER-LAMINA Jaro, Digitale Souveränität und politische Prozesse, *in* BOGNER Alexander / DECKER Michael / NENTWICH Michael / SCHERZ Constanze (édit.), Digitalisierung und die Zukunft der Demokratie Beiträge aus der Technikfolgenabschätzung, Baden-Baden (Nomos) 2022, pp. 189-204 (cité : JÄGER et al.).

JESSOP Bob, Redesigning the state, reorienting state power and rethinking the state, *in* JENKINS Craig / LEICHT Kevin (édit.), Handbook of politics, New York (Springer) 2010, pp. 41-61.

KAGERMAN Henning / STREIBICH Karl-Heinz / SUDER Katrin, Souveraineté numérique, Statu quo et champs d'action, Munich (Acatech IMPULS) 2021 (cité : KAGERMAN et al.).

KALOUDIS Martin, Digital Sovereignty–European Union's Action Plan Needs a Common Understanding to Succeed, *in* History Compass, 2021, vol. 19, no. 12 (cité : KALOUDIS, Action plan).

KALOUDIS Martin, Sovereignty in the Digital Age – How Can We Measure Digital Sovereignty and Support the EU's Action Plan?, *in* New Global Studies, 25 octobre 2021 (cité : KALOUDIS, Index).

LAMBACH Daniel / OPPERMANN Kai, Narratives of digital sovereignty in German political discourse, *in* Governance Journal (early view), 2022, p. 1ss.

LEWIS James A., Sovereignty and the Evolution of Internet Ideology, *in* Center for Strategic and International Studies, octobre 2020.

LU Yen-Chi / MAYER Maximilian, Illusions of Autonomy? Global Digital Dependence Structures, Bonn (Center for Advanced Security) 2022.

LUNDVALL Bengt-Åke / RIKAP Cecilia, China's catching-up in artificial intelligence seen as a co-evolution of corporate and national innovation systems, *in* Research Policy, 2022, vol. 51, no 1.

LUZEAUX Dominique, *Cloud* souverain : souveraineté et résilience, ou confiance ?, *in* Revue Défense Nationale, 2022, vol. 855, no. 10, p. 14ss.

MAHIEU René / AUSLOOS Jef, Harnessing the collective potential of GDPR access rights: towards an ecology of transparency, *in* Internet Policy Review, 6 juillet 2020.

MALINVERNI Giorgio / HOTTELIER Michel / HERTIG RANDALL Maya / FLÜCKIGER Alexandre, Droit constitutionnel suisse, vol. I : L'Etat, 4ème éd., Berne (Stämpfli) 2021 (cité : MALINVERNI et al.).

MARCH Christoph / SCHIEFERDECKER Ina, Technological Sovereigntyas Ability, Not Autarky, Center for Economic Studies and IfoInstitute (CESifo) Working Paper, 2021, No. 9139.

MAURER Tim / SKIERKA Isabel / MORGUS Robert / HOHMANN Mirko, Technological Sovereignty: Missing the Point?, *in* 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, p. 53ss (cité : MAURER et al.).

MAYER Pierre, Le phénomène de la coordination des ordres juridiques étatiques en droit privé : cours général de droit international privé, *in* RCADI, 2007, vol. 327, p. 9ss.

MOEREL Lokke / TIMMERS Paul, Reflections on Digital Sovereignty, EU Cyber Direct, 2021 [https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/khGGovSY/rif_timmersmoerel-final-for-publication.pdf] (10.10.22).

MOGHIOR Cosmina, European Digital Sovereignty: An Analysis of Authority Delegation, *in* Romanian Journal of European Affairs, 2022, vol. 22, no. 1, p. 104ss.

MONTAVON Michael, Cyberadministration et protection des données, Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyen-ne-s et des autorités de contrôle, Zurich (Schulthess) 2021.

MONTAVON Michael / SCHWAB Stéphane, eGovernment : quelques comparaisons et réflexions à partir de l'exemple estonien (1/2), Revue fribourgeoise de jurisprudence (RFJ), 2019.

NANNI Riccardo, Digital sovereignty and Internet standards: normative implications of public-private relations among Chinese stakeholders in the Internet Engineering Task Force, *in* Information, Communication & Society, 2022, vol. 25, no 16, p. 2342ss.

O'NEIL Cathy, Algorithmes, la bombe à retardement, Paris (Les Arènes) 2018.

PAGANO Ugo, The crisis of intellectual monopoly capitalism, *in* Cambridge Journal of Economics, 2014, vol. 38, no 6, p. 1409ss.

PISTOR Katharina, Rule by data: The end of markets?, *in* Law & Contemporary Problems, 2020, vol. 83, no. 2, p. 101ss.

PLATTNER Roger, Digitales Verwaltungshandeln, Rechtliche Aspekte der Digitalisierung in der öffentlichen Verwaltung, Zurich (sui generis) 2019.

POHLE Julia, Digital Sovereignty, A New Key Concept of Digital Policy in Germany and Europe, Berlin (Konrad-Adenauer-Stiftung) 2020.

POHLE Julia / THIEL Thorsten, Digital Sovereignty, *in* HERLO Bianca / IRRGANG Daniel / JOOST Gesche / UNTEIDIG Andreas (édit.), Practicing Sovereignty, Digital Involvement in Times of Crises, Bielefeld (Transcript) 2021, pp. 47-67.

PRETELLI Ilaria, Conflict of Laws in the Maze of Digital Platforms/Le droit international privé dans le labyrinthe des plate-formes digitales, Zurich (Schulthess) 2019.

PUGLIERIN Jana / ZERKA Pawel (édit.), European Sovereignty index, ECFR/451, June 2022 [https://ecfr.eu/wp-content/uploads/2022/06/European-Sovereignty-Index.pdf] (12.10.22).

RAMOS Gretchen / MACIEJEWSKI Andrea / JONGEN Herald (Greenberg Traurig LLP), Application of the *CLOUD Act* to EU Entities, Memorandum to the Dutch Ministry of Justice and Security, 26 juillet 2022 [https://www.ncsc.nl/documenten/publicaties/2022/augustus/16/cloud-act-memo] (12.10.22) (cité : RAMOS et al.).

RIKAP Cecilia, Capitalism, Power and Innovation: intellectual monopoly capitalism uncovered, Londres (Routledge) 2022.

ROBINSON Nick / KASK Laura / KRIMMER Robert, The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis, *in* ICEGOV2019, Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, 2019, p. 391ss (cité : ROBINSON et al.).

ROGUSKI Przemysław, Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment, *in* 11th International Conference on Cyber Conflict (CyCon), 2019, p. 1ss.

ROSSI Julien / MUSIANI Francesca / CASTEX Lucien, La gouvernance d'Internet, entre infrastructures et espaces socio-politiques : apports de la recherche, *in* Terminal [Online], 2022, p. 132s (cité : ROSSI et al.).

ROUVROY Antoinette / BERNS Thomas, Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ?, *in* Réseaux, 2013, vol. 177, no. 1, p. 163ss.

SAVIN Andrej, Digital Sovereignty and Its Impact on EU Policymaking, *in* Copenhagen Business School Law (CBS LAW) Research Paper, 2022, Series No. 22-02.

SCHMITZ Luuk / SEIDL Timo, As Open as Possible, as Autonomous as Necessary: Understanding the Rise of Open Strategic Autonomy in EU Trade Policy, *in* Journal of Common Market Studies (JCMS), 2022, p. 1ss.

SCHWARZENEGGER Christian / THOUVENIN Florent / STILLER Burkhard, Avis de droit concernant l'utilisation des services de cloud par les avocates et avocats, 2019 [https://digital.sav-

fsa.ch/documents/1060627/1169162/gutachten_sav-franzoesisch.pdf/81740267-8cf0-36b1-6918-c3ddb9c71ee4?t=1618228137307] (17.01.23) (cité : SCHWARZENEGGER et al.).

SEIFRIED Mareike / BERTSCHEK Irene, Schwerpunktstudie Digitale Souveränität, Berlin (Bundesministerium für Wirtschaft und Energie) 2021.

SHEIKH Haroon, European Digital Sovereignty: A Layered Approach, *in* Digital Society (DISO), 2022, vol. 1, no. 25.

SHI-KUPFER Kristin / OHLBERG Mareike, China's Digital Rise, Challenges for Europe, *in* Mercator Institute for China Studies (Merics) Papers on China, No 7, April 2019.

TAN Kheng-Leong / CHI Chi-Hung / LAM Kwok-Yan, Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization, 2022 (cité : TAN et al.).

THELISSON Eva, La portée du caractère extraterritorial du Règlement général sur la protection des données, *in* Revue internationale de droit économique 2019/4, p. 501ss.

TIPPER David / Krishnamurthy Prashant, Digital Sovereignty and Resilience, 1er août 2022.

TÜRK Pauline, Définition et enjeux de la souveraineté numérique, 14 septembre 2020 [https://www.vie-publique.fr/parole-dexpert/276125-definition-et-enjeux-de-la-souverainete-numerique] (10.10.22).

VAN HECKE George A., Le droit anti-trust : aspects comparatifs et internationaux, *in* Recueil des cours de l'Académie de droit international de La Haye, 1962, vol. 106, p. 309ss.

VATANPARAST Roxana, Data Governance and the Elasticity of Sovereignty, *in* Brooklyn Journal of International Law (Brook. J. Int'l L), 2020, vol. 46, no. 1, p. 1ss.

WEBER Herbert, Digitale Souveränität, *in* Informatik Spektrum, 2022, vol. 45, p. 152ss (cité : WEBER H.)

WEBER Rolf H., Elements of a Legal Framework for Cyberspace, *in* Swiss Review of International and European Law, 2016, vol. 26, no. 2 p. 195ss (cité : WEBER R.)

WERTHNER Hannes, Geopolitics, Digital Sovereignty…What's in a Word?, *in* WERTHNER Hannes / PREM Erich / LEE Edward A. / GHEZZI Carlo (édit.), Perspectives on Digital Humanism, Cham (Springer) 2021, pp. 241-248.

WESTPHAL Kirsten, Strategic sovereignty in energy affairs: reflections on Germany and the EU's ability to act, SWP Comment 7/2021, Berlin (Stiftung Wissenschaft und Politik) 2021.

WOOD Sam / HOFFMANN Stacie / MCFADDEN Mark / KAUR Akhiljeet / WONGSAROJ Sarongrat / SCHOENTGEN Aude / FORSYTH Grant / WILKINSON Laura, Digital Sovereignty: the overlap and conflict between states, enterprises and citizens, Londres (Plum Consulting) 2020, p. 11 (cité : WOOD et al.)

WORLD GOVERNMENT SUMMIT (WGS) / ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), Case Study : The world's first data embassy – Estonia, *in* Embrassing Innovation in Government - Global Trends 2018, p. 42ss [http://www.oecd.org/gov/innovative-government/embracing-innovation-in-government-2018.pdf] (10.10.22).

YAKOVLEVA Svetlana, EU's trade policy on cross-border data flows in the global landscape: navigating the thin line between liberalizing digital trade, "digital sovereignty" and multilateralism, *in* FAHEY Elaine / MANCINI Isabella (édit.), Understanding the EU as a Good Global Actor, Ambitions, values and metrics, Glos / Massachusetts (Edward Elgar) 2022, pp. 192-208.

YEN Huai-Shing, Digital Autonomy and Taiwan–EU Partnership, *in* POGOREL Gérard / NESTORAS Antonios / CAPPELLETTI Francesco (édit.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles (European Liberal Forum) 2022, pp. 105-110.

YUGUCHI Kiyotaka, Japan: Digital Sovereignty as an Element of the Economic Security, *in* POGOREL Gérard / NESTORAS Antonios / CAPPELLETTI Francesco (édit.), Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners, Bruxelles (European Liberal Forum) 2022, pp. 75-84.

ZUBOFF Shoshana, The age of surveillance capitalism: the fight for the future at the new frontier of power, Londres (Profile Books) 2019.

ZUFFEREY Jean-Baptiste, Le traitement de l'énergie en droit de la construction : Une belle illustration des problèmes du renvoi aux normes techniques, *in* HOTTELIER M. / FOËX B. (édit.), La propriété immobilière face aux défis énergétiques : Du statut juridique de l'énergie au contrôle des loyers, Genève (Schulthess) 2016.