Emma MIQUEL.

> *Nota bene* : les citations de ce texte non issues de sources françaises, sont des traductions réalisées par l'auteure à partir des sources originales généralement en anglais ou en chinois.

Le concept d'État de droit repose sur l'idée fondamentale que la puissance publique doit être soumise au droit, pour garantir la prééminence des normes juridiques sur les actions discrétionnaires des

gouvernants[1]. Dans ce cadre, la souveraineté[2], comprise comme l'autorité suprême exercée par l'État sur son territoire et sa population, se heurte aux phénomènes contemporains de la mondialisation[3] et de la numérisation. La souveraineté numérique en particulier, qui se définit comme l'autorité d'un État sur le cyberespace national[4], remet en question les mécanismes traditionnels de contrôle étatique en raison de la nature transfrontalière des technologies numériques et de la domination d'acteurs privés régionaux et même internationaux dans cet espace.

La doctrine souligne alors que l'État de droit, pour s'adapter à ces mutations, doit renforcer les principes de légalité, de transparence et d'imputabilité dans la gouvernance numérique[5]. Cependant, la souveraineté numérique soulève également des tensions entre autonomie étatique et interdépendance globale[6]. Cette tension est parfaitement illustrée par l'initiative chinoise de la *Digital Silk Road* (DSR[7] qui privilégie un contrôle étatique renforcé, perçu comme un prolongement de la souveraineté territoriale[8].

Après sa législation sur la cybersécurité de 2016[9], la Chine a déployé en 2021 une nouvelle législation sur la protection des données personnelles[10], marquant un tournant dans sa gouvernance numérique. Parmi ses dispositions, l'obligation pour les entreprises étrangères de stocker les données des utilisateurs chinois sur le sol chinois a suscité des préoccupations[11]. Cet exemple illustre l'application de la souveraineté numérique, à travers des politiques strictes sur le contrôle des données et des infrastructures numériques. Au cœur de cette stratégie se trouve l'objectif de maintenir plus largement la souveraineté nationale et de garantir la sécurité des données tout en imposant un contrôle étatique sur les flux d'informations.

Or, cette approche soulève une question fondamentale : dans quelle mesure un tel modèle est-il compatible avec les principes de l'État de droit, qui, selon la tradition juridique internationale, suppose la limitation des pouvoirs étatiques au regard des droits fondamentaux et de la liberté individuelle ?

Cette question se pose avec d'autant plus de force que le pouvoir chinois lui-même emploie parfois le terme d'État de Droit. En effet, le 10 janvier 2021 le Comité Central du Parti Communiste Chinois (PCC) avait publié un Plan de construction de l'État de droit (2020–2025)[12]. Ce document d'orientation matérialise des ambitions du Président Xi annoncées lors de la conférence centrale sur les travaux liés à la gouvernance globale fondée sur le droit de2020.[13] Il a, à cette occasion, rappelé que l'« État de droit »[14] – ce à quoi le pays tend comme l'explique par ailleurs Jean-Pierre Cabestan[15] – est un symbole notable du « progrès de la civilisation humaine ». La République Populaire de Chine n'entend pas ici établir un État de droit tel qu'il est défini par l'Organisation des Nations Unies[16] mais présente sa propre conception. Il s'agit d'instaurer « un État de droit socialiste aux caractéristiques chinoises »[17]. Cette distinction est loin d'être purement sémantique, car elle reflète une divergence fondamentale entre deux visions de l'État de droit, chacune se réclamant pourtant du même principe[18].

La Chine, tout en affirmant sa souveraineté numérique, s'éloigne de l'idéal d'un État de droit « classique » où la transparence, la protection des libertés et l'indépendance judiciaire priment généralement. En

conséquence, le concept d'État de droit « socialiste » renvoie à des exigences parfois contradictoires comme protéger les droits fondamentaux tout en consolidant une souveraineté numérique compatible avec les impératifs de sécurité et d'innovation.

Cet article se propose d'analyser la manière dont la Chine construit son modèle de souveraineté numérique à travers ses réformes législatives internes, et comment ce modèle se projette au-delà de ses frontières à travers des initiatives telles que la *Digital Silk Road*. Ce projet de réseau numérique a été annoncé en mars 2015 par le ministère chinois des Affaires étrangères et le Ministère du Commerce (NDRC) à travers la publication d'un livre blanc[19], accompagnant l'ambition d'une expansion de la 5G dans le cadre d'une nouvelle stratégie Internet[20]. Ce réseau stratégique, intégré dans le cadre de la *Belt and Road Initiative* (BRI) vise à développer des infrastructures numériques et à promouvoir des normes technologiques alignées avec les objectifs géopolitiques de la Chine.

Cet article explore ainsi les tensions entre la souveraineté numérique chinoise et les principes de l'État de droit, tant sur le plan national qu'international. Dans un premier temps, il examinera comment la Chine utilise l'État de droit comme un outil pour renforcer son contrôle numérique au niveau interne (I). Dans un second temps, il analysera les implications de l'exportation de ce modèle, notamment à travers la *Digital Silk Road*, et les défis qu'elle pose aux normes internationales et aux droits fondamentaux (II).

I. Le cadre juridico-institutionnel autoritaire propice au développement de la souveraineté numérique chinoise

Selon Hans Kelsen, l'État de droit repose sur l'idée que le pouvoir politique doit être exercé dans les limites du droit, garantissant ainsi que les actes des autorités publiques sont soumis à des règles juridiques prédéterminées, qui assurent la liberté et les droits des individus. Dans sa célèbre définition, Kelsen soutient que l'État de droit repose sur l'idée que tout pouvoir, même celui de l'État, doit être fondé sur le droit. Ainsi ce droit doit être appliqué de manière prévisible, égale et systématique[21].

Cependant, l'État de droit tel qu'il est compris dans les démocraties libérales se distingue de sa conception en Chine, où il sert plutôt à renforcer l'autorité étatique qu'à limiter son pouvoir. En Chine, le Parti communiste chinois (PCC), à travers sa légitimité politique, a redéfini cette notion pour qu'elle serve les objectifs du régime, notamment la sécurité nationale[22] et le contrôle social. Ainsi, l'État de droit n'est pas perçu comme une contrainte au pouvoir, mais comme un outil de régulation permettant au Parti de maintenir l'ordre tout en conservant une légitimité juridique.

En ce sens, le cadre légal chinois montre que la notion d'État de droit est conçue différemment de son

acception occidentale. L'une des principales sources juridiques est la Constitution de la République populaire de Chine[23], qui, tout en affirmant le principe de l'État de droit, subordonne cette notion à la prééminence du PCC. L'article 5 de la Constitution dispose que :

« La République populaire de Chine doit pratiquer une gouvernance fondée sur le droit et construire un État socialiste régi par l'État de droit.

L'État garantit l'unité et le caractère sacré du système juridique socialiste »[24].

Cette disposition, bien que proclamant l'État de droit, en réduit la portée en établissant que le droit doit être subordonné aux objectifs politiques du Parti. Dans ce contexte, des lois telles que la Loi sur la cybersécurité et la Loi sur la protection des données personnelles sont des instruments permettant au gouvernement chinois de renforcer son contrôle tout en prétendant respecter les normes juridiques (A). Ces textes offrent un cadre pour la gestion de la cybersécurité et de la protection des données personnelles, mais les critères de conformité à ces lois sont souvent laissés à l'appréciation des autorités, ce qui peut entraîner une instrumentalisation du droit afin de favoriser le nationalisme prégnant en Chine (B).

A. Une législation nationale au service d'une souveraineté numérique renforcée

Comme il a été évoqué précédemment, la souveraineté numérique chinoise repose sur un cadre législatif conçu pour renforcer le contrôle étatique sur les données et les infrastructures numériques. Depuis le début des années 2010, la Chine a progressivement mis en place une série de lois et de régulations visant à assurer une gouvernance numérique sous la direction du PCC. Ce cadre législatif, loin de se limiter à des questions techniques ou de sécurité, incarne une vision politique de la souveraineté numérique, où la régulation du cyberespace devient un outil stratégique pour maintenir l'ordre social et politique[25]. Autrement dit, contrairement à d'autres grandes puissances numériques, qui privilégient souvent des régulations orientées vers la protection des données personnelles ou la libre circulation des informations[26], la Chine s'appuie sur un contrôle direct et centralisé de son cyberespace (1). Elle utilise le droit non seulement comme un moyen de garantir la cybersécurité, mais aussi comme un outil de régulation politique.

C'est en 2022 que la Chine a commencé à mettre en avant sa « solution chinoise » à la cybergouvernance mondiale dans un rapport sur le développement de l'économie numérique. [27] Cette ambition amplifie la dimension normative du DSR. En plus d'exporter des infrastructures numériques, la Chine a cherché à souligner, voire à réitérer, la « cybersouveraineté »[28] de ses partenaires DSR. À cet égard, elle précise qu'elle « respecte le droit de chaque pays à choisir indépendamment sa voie de développement du cyberespace, son modèle de gestion des réseaux et sa politique publique sur les questions liées à l'Internet, ainsi que son droit à une participation égale à la gouvernance internationale du

cyberespace »[29].

Ce plan stratégique s'incarne également dans des lois telles que la Loi sur la cybersécurité de la République populaire de Chine[30]. Ce modèle de régulation numérique permet au gouvernement de maintenir une surveillance omniprésente sur les comportements des citoyens et de garantir un *censorship* numérique efficace, reposant sur un mécanisme de collecte des données personnelles (2).

1. L'instauration législative d'un « digital border » pour un contrôle souverain des données

La Loi sur la cybersécurité et la PIPL introduisent des cadres législatifs visant à renforcer la souveraineté numérique chinoise, mais elles soulèvent des interrogations quant à leur compatibilité avec une conception classique de l'État de droit.

En effet, l'origine de la théorie de l'État de droit se situe dans une volonté de garantir la subordination des pouvoirs publics au droit, une idée qui émerge au XIX^{e} siècle dans le cadre de l'État libéral. Cette théorie, inspirée par les conceptions allemandes du Rechtsstaat[31] et consolidée par la pensée de juristes comme Maurice Hauriou et Léon Duguit,[32] repose sur trois piliers principaux : la primauté du droit, la séparation des pouvoirs et la protection des droits fondamentaux. Elle établit ainsi que l'autorité publique ne peut agir qu'en vertu d'une norme juridique préexistante, ce qui limite l'arbitraire et favorise la sécurité juridique. Parallèlement, à cette tradition continentale initialement fondée sur la primauté de la loi, la conception anglo-saxonne de *rule of law* repose sur un contrôle juridictionnel fort, incarné notamment par le *judicial review* aux États-Unis.[33] Ce mécanisme garantit notamment que toute action du pouvoir respecte le droit. Cette approche a contribué à l'évolution des conceptions européennes, où l'État de droit intègre aujourd'hui pleinement les trois piliers susmentionnés. Le juriste Luc Heuschling, dans son analyse comparative, souligne ainsi la convergence progressive entre ces modèles juridiques sous l'influence du droit international et des juridictions supranationales[34].

Or, la politique chinoise de souveraineté numérique marque une rupture avec la tradition libérale de l'État de droit et du *rule of law*, en privilégiant un modèle où la primauté de l'État sur le droit et la sécurité nationale justifient une régulation centralisée des données et du cyberespace. Ainsi, ces lois chinoises consolident le contrôle étatique sur les données et les infrastructures numériques en imposant, par exemple, des obligations strictes de localisation des données,[35] des audits de sécurité pour les entreprises opérant dans des secteurs stratégiques,[36] ainsi qu'un accès étendu aux données par les autorités publiques.[37] Si elles répondent aux impératifs de protection nationale et de gestion des risques numériques, elles remettent en question certains principes fondamentaux associés à l'État de droit, tels que la transparence, l'indépendance judiciaire ou encore la protection des droits individuels face à l'arbitraire de l'État.

C'est ainsi que pour assurer le contrôle des activités en ligne des citoyens et de leurs données, l'article 66 de la Loi sur la cybersécurité[38] impose aux opérateurs des principales infrastructures d'information de conserver les données personnelles et autres données importantes sur le territoire chinois. Les opérateurs sont également tenus de soutenir les organisations de sécurité publique et nationale, en leur permettant une inspection et un accès complet aux données[39].

Par la suite, la réglementation chinoise a étendu cette obligation, puisque l'article 40 de la PIPL exige que les données personnelles collectées et générées par « les opérateurs d'infrastructures d'informations critiques (CII) et les processeurs d'informations personnelles qui traitent des informations personnelles atteignant un montant désigné par l'Administration du cyberespace de Chine »[40] soient stockés en Chine. Cette exigence de localisation des données oblige les entreprises étrangères à envisager de déployer une infrastructure informatique dans le pays, spécifiquement pour leurs activités en Chine. Le trafic Internet chinois ne peut être acheminé que via des infrastructures chinoises locales, excluant ainsi la possibilité d'une opération de surveillance ou de collecte de renseignements par une agence étrangère.

En d'autres termes, la législation chinoise interdit la collecte par des organisations étrangères de données personnelles de citoyens chinois sans que ces organisations ne travaillent avec une entreprise chinoise ni qu'elles installent leur infrastructure sur le territoire chinois. Si l'entreprise traite les données de résidents chinois mais n'a aucune présence commerciale dans le pays, il est nécessaire de créer une agence spéciale ou de désigner des représentants en Chine.[41] Cela a eu plusieurs conséquences pour les entreprises étrangères comme *Amazon*. Afin de se conformer à la loi chinoise, *Amazon Web Services (AWS)* a vendu, en 2017, certains actifs d'infrastructures physiques (notamment l'unité de *cloud computing* public) à *Beijing Sinnet Technology Co Ltd* (le partenaire chinois de l'entreprise américaine)[42].

En exigeant des pays partenaires qu'ils partagent des données, la Chine assure un flux continu d'informations stratégiques et économiques. Par ailleurs, la Chine impose des restrictions strictes aux entreprises étrangères opérant sur son territoire afin de protéger son marché intérieur et ses données sensibles. Les entreprises étrangères doivent se conformer aux exigences relatives aux collaborations avec des partenaires locaux, au transfert de technologie et à l'hébergement de données en Chine. Autrement dit, alors que la Chine exige de ses partenaires qu'ils partagent leurs données et ouvrent leur territoire à la Chine, elle souhaite à l'inverse conserver le contrôle des entreprises étrangères s'implantant dans le pays, traduisant une stratégie de gestion asymétrique des flux d'information et d'influence économique.

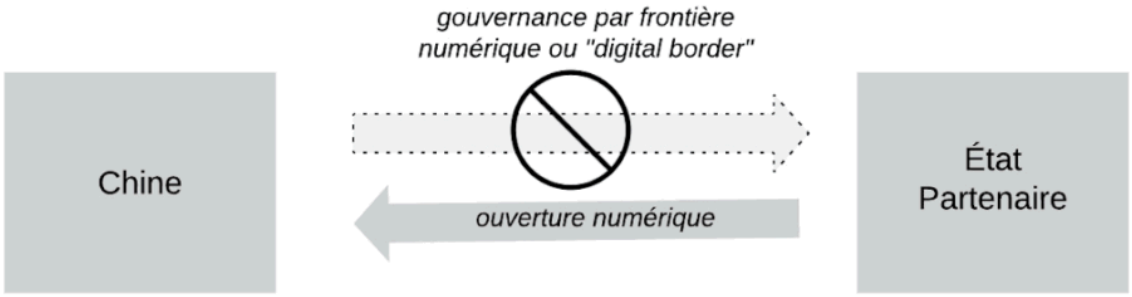

Figure 1 : Frontière numérique de la Chine

Ce constat met en évidence une asymétrie stratégique dans la gestion des flux d'informations et des influences économiques par la Chine, qui s'éloigne des principes classiques de l'État de droit et de la souveraineté qui en découle. L'un des fondements de cette souveraineté repose sur la capacité de l'État à établir des règles applicables de manière uniforme sur son territoire, sans distinction entre acteurs nationaux et étrangers.

Or, la stratégie chinoise, qui impose aux entreprises étrangères des contraintes strictes, introduit une dissymétrie normative. Cette approche interroge le principe d'universalité du droit étatique, en créant un cadre différencié selon l'origine des acteurs économiques et en instaurant un contrôle politique sur l'économie numérique.

Alors que le modèle westphalien repose sur une souveraineté égale entre les États et une application uniforme du droit sur un territoire donné, l'essor du numérique et des flux transnationaux de données a conduit certains États, comme la Chine, à redéfinir leur souveraineté de manière fonctionnelle et stratégique, plutôt que purement territoriale. Le concept de souveraineté numérique vient ainsi complexifier la théorie de l'État, puisqu'il intègre des logiques de pouvoir asymétriques qui ne se limitent plus à un strict contrôle territorial, mais s'étendent aux dépendances technologiques.

En parallèle, les défis posés par les technologies numériques, tels que la surveillance de masse, l'intelligence artificielle ou la protection des données personnelles, interrogent la capacité de l'État de droit à protéger efficacement les libertés individuelles face à des acteurs globaux et à des logiques algorithmiques opaques. En somme, si la théorie originelle de l'État de droit demeure un idéal normatif, son application dans la pratique révèle des écarts significatifs, notamment sous l'effet de dynamiques géopolitiques, économiques et technologiques.

Même si des inquiétudes subsistent quant à l'utilisation des données par les entreprises chinoises, l'exportation de technologies dans le cadre du DSR a un impact sur les pratiques de gouvernance des pays partenaires. Ces entreprises fournissent non seulement l'infrastructure, mais également le savoir-

faire et l'assistance technique nécessaires à son exploitation. Leur présence sur le terrain conduit également à l'intégration des approches chinoises de gouvernance dans les réglementations locales. Comme le Professeur Rogier Creemers l'a souligné, la diffusion des normes technologiques chinoises s'accompagne souvent de la promotion de leur modèle de gouvernance, caractérisé par de vastes mécanismes de surveillance et de censure de l'État[43].

2. La réglementation sur la récolte des données : outil clé pour la croissance numérique

La Chine profite de ses alliances au sein de la DSR pour collecter les données nécessaires au bon fonctionnement de ses systèmes d'Intelligence Artificielle. Grâce à ses grandes entreprises technologiques, la Chine récupère de grandes quantités de données et les partage avec le gouvernement et ses agences[44]. En retour, le gouvernement soutient ces entreprises en leur garantissant une position monopolistique sur le marché intérieur, limitant ainsi la concurrence étrangère par des barrières réglementaires strictes et un contrôle accru des services numériques étrangers. *WeChat*, le réseau social de *Tencent Company*, en est un bon exemple. Avec ses fonctionnalités intégrées de paiement mobile, de services administratifs et de communication professionnelle, *WeChat* est devenu un outil incontournable du quotidien en Chine. Il s'agit de l'application de chat la plus utilisée au monde, avec 1 200 milliards d'utilisateurs[45].

Cependant, cette application a fait l'objet de nombreuses controverses. Premièrement, parce que ses politiques de confidentialité sont opaques, les utilisateurs n'étant pas correctement informés de la manière dont leurs données sont collectées, stockées et utilisées. Les finalités du partage de ces données restent floues, et l'application ne garantit pas une transparence suffisante quant aux entités pouvant y accéder, qu'il s'agisse d'entreprises partenaires ou des autorités chinoises.[46] Un autre point de préoccupation majeure réside dans l'absence de preuve d'un lien direct entre le traitement des données des utilisateurs et les finalités déclarées pour lesquelles ces derniers utilisent *WeChat*. Alors que l'application se présente avant tout comme une plateforme de communication et de services, la quantité et la nature des données collectées vont bien au-delà des besoins fonctionnels de ses utilisateurs[47]. *WeChat* intègre en effet des outils de reconnaissance faciale, des systèmes de suivi des transactions financières et des mécanismes de censure, ce qui alimente les inquiétudes quant à un possible usage détourné de ces informations, notamment à des fins de surveillance ou de contrôle social.

Dans cette optique, plusieurs gouvernements ont pris des mesures pour limiter l'influence de *WeChat* et d'autres technologies chinoises sur leur territoire. En 2023, le gouvernement d'Ottawa a ainsi décidé d'interdire l'application sur les téléphones gouvernementaux, invoquant des risques liés à la cybersécurité et à la protection des données sensibles[48]. De même, aux États-Unis, l'administration Biden a pris des mesures radicales pour restreindre l'accès aux infrastructures numériques chinoises. En novembre 2022, l'importation et la vente de nouveaux équipements de télécommunications fournis par

plusieurs grandes entreprises chinoises – dont *Zhongxing Telecom Ltd (ZTE)*, *Huawei*, *Dahua, Hikvision* et *Hytera* – ont été interdites[49].

Le tribunal Internet de Pékin[50] a lui-même jugé que le partage d'informations personnelles entre *WeChat* et d'autres applications sœurs ne répondait pas aux attentes raisonnables des utilisateurs, notamment s'ils ne sont pas informés du traitement avec suffisamment de transparence, même si ces applications sont développées par la même société (c'est-à-dire *Tencent*)[51]. *WeChat* et ses affiliés partagent les données des utilisateurs pour en savoir plus sur les clients potentiels. Par exemple, *Weimin Insurance Agent Ltd*, qui vend des produits d'assurance via *Wesure*, un service proposé sur *WeChat*, partage l'historique de navigation des utilisateurs avec *WeChat* et *Tenpay*[52].

Le DSR a été largement piloté par des entreprises technologiques chinoises telles que *Alibaba Group Holding Limited*, *Huawei Technologies Company Limited*, *ZTE Corporation* et *Tencent*. Compte tenu des politiques de traitement des données de ces entreprises et de leurs liens plus ou moins étroits avec le gouvernement chinois, des doutes sont apparus quant aux risques sur les données des États partenaires. Et ces derniers sont nombreux à être concernés. À titre d'exemple, *Huawei* est responsable de près de 70 % du réseau de télécommunications africain, et cible des villes africaines mondiales comme Johannesburg, Le Caire et Casablanca en raison de leur emplacement stratégique, de leur développement urbain intensif et de leur nature internationale[53].

Ainsi,« la possibilité d'utiliser ces données pour atteindre l'objectif global d'intégration des économies et des sociétés des pays de la BRI avec celles de la Chine reste élevée »[54].

D'ailleurs, en 2018, *Telecom Egypt* avait reçu un prêt de 160 millions de dollars de la Banque d'Exim de Chine pour un projet confié à *Huawei* afin d'étendre l'accès au numérique[55], ce qui témoigne de la coopération économique croissante entre la Chine et les pays africains, où la Chine finance des projets d'infrastructure et de développement des TIC. Cela s'inscrit dans la politique gouvernementale chinoise visant à encourager les entreprises nationales à se développer à l'étranger et à accéder à ces marchés délocalisés.

Ces mesures de régulation permettent à la Chine de maintenir un modèle autoritaire de gouvernance numérique, dans lequel les entreprises technologiques et les citoyens sont intégrés dans une logique de surveillance étatique continue[56]. Au-delà de cet accès aux données, la Chine construit un réseau d'échanges et d'intérêts entre elle et des États cibles. Elle constitue ainsi un écosystème ouvert sur l'extérieur, avec pour objectif de maintenir son propre équilibre interne et de renforcer sa position de puissance régionale et mondiale. Cette stratégie lui permet de tisser un réseau de dépendances économiques et géopolitiques par la diffusion technologique, qui peut s'avérer difficile à démanteler pour les pays concernés. De l'autre, la Chine met en place une frontière numérique autour de son territoire et à travers sa législation pour maintenir un protectionnisme numérique national[57].

Il s'agit d'une stratégie ambitieuse qui permet au pays de renforcer sa souveraineté numérique et de protéger son marché intérieur de la concurrence étrangère. Cette approche reflète une conception singulière de la gouvernance du numérique, éloignée des modèles institutionnels et des équilibres de pouvoir en vigueur en Occident.

B. L'architecture institutionnelle chinoise de la souveraineté numérique

Le protectionnisme numérique en Chine s'inscrit dans un modèle alternatif de légalité (1), où la primauté est donnée à l'autorité centrale et à la restriction des libertés individuelles (2). À travers ses lois, le pays a centralisé la gestion des données et des flux d'information. Ce protectionnisme numérique favorise l'autosuffisance technologique en stimulant les entreprises nationales tout en limitant les échanges avec les autres acteurs privés internationaux, créant ainsi un marché numérique fermé au niveau interne. Toutefois, cette stratégie s'accompagne d'une dérive vers un contrôle social plus rigide, où les citoyens sont soumis à une surveillance numérique constante et à des restrictions sévères concernant l'accès à certains contenus et plateformes étrangères. Cette centralisation de la légalité vise à garantir la stabilité du régime en renforçant la capacité de l'État à superviser les activités en ligne, tout en restreignant les capacités d'auto-organisation des citoyens et de la société civile.

Ainsi, en faveur d'une sécurité nationale et d'une gestion centralisée de l'espace numérique, la Chine développe un modèle où le contrôle de l'information et l'intrusion dans la vie privée des individus sont justifiés par des impératifs de préservation de l'ordre public et du pouvoir central.

1. Un modèle alternatif à l'État de droit occidental privilégiant le pouvoir centralisé

Le modèle juridique chinois en matière de cybersécurité et de régulation des données repose sur ce que certains auteurs appellent une *légalité autoritaire*.[58] La légalité autoritaire désigne un système dans lequel les lois ne sont pas pensées pour limiter les pouvoirs étatiques, mais pour légitimer leur contrôle sur la société.[59] Cette notion est particulièrement pertinente dans le contexte de la *Digital Silk Road*, où la Chine exporte des modèles de régulation qui permettent aux régimes partenaires de renforcer leur pouvoir centralisé sous couvert de sécurisation numérique. La souveraineté numérique s'inscrit ainsi dans une logique où les gouvernements ne cherchent pas à garantir des libertés individuelles, mais à sécuriser et centraliser le contrôle sur les informations et les infrastructures numériques.

Cette théorie de la légalité autoritaire permet de mieux comprendre comment la Chine, par l'intermédiaire de lois telles que la Loi sur la cybersécurité et la PIPL, impose un modèle où la protection des données et la sécurité nationale deviennent des prétextes pour renforcer la surveillance étatique et le

contrôle des flux d'informations[60]. Bien que relativement marginale dans la doctrine juridique occidentale, cette théorie trouve ses racines dans une conception alternative de légalité et du rôle de l'État dans sa mise en œuvre. Contrairement à l'idéal libéral où la légalité est souvent perçue comme un traitement identique sous la loi, cette théorie repose sur l'idée que la légalité peut nécessiter une intervention proactive et centralisée de l'État, souvent au prix de restrictions sur certaines libertés individuelles. La légalité autoritaire s'inscrit ainsi dans une vision paternaliste, où l'État, agissant comme garant du bien commun, impose des normes uniformes pour réduire les disparités sociales et économiques.

Ce concept trouve un ancrage dans des régimes où l'uniformisation des conditions de vie et des opportunités passe par une forte centralisation du pouvoir et des mécanismes de contrôle étatique. Dans ce cadre, la légalité devient une finalité supérieure justifiant une concentration des pouvoirs. Comme l'a observé le juriste allemand Ernst Fraenkel dans sa typologie des régimes[61], les États adoptant une telle approche tendent à opposer le bien collectif aux libertés individuelles, créant une tension structurelle entre la légalité matérielle et les droits fondamentaux. Cette théorie repose sur l'idée que la légalité substantielle, et non simplement formelle, exige une planification et une coercition étatiques pour surmonter les déséquilibres socio-économiques structurels.

En ce sens, la théorie de légalité autoritaire entre en tension directe avec les fondements classiques de l'État de droit, notamment lorsqu'elle subordonne la primauté du droit à des impératifs politiques ou économiques. L'État de droit, tel que conceptualisé par des penseurs comme Albert Venn Dicey[62] et, plus récemment, Mireille Delmas-Marty[63], repose sur une limitation des pouvoirs. En revanche, la légalité autoritaire tend à privilégier une interprétation instrumentale du droit, où les règles juridiques sont avant tout des outils au service de l'ingénierie sociale, et non des bornes imposées à l'autorité publique.

Cette divergence est particulièrement marquée dans les régimes où la légalité autoritaire est appliquée de manière coercitive. Les libertés fondamentales, telles que la liberté d'expression, d'association ou même de propriété, peuvent être restreintes pour atteindre des objectifs collectifs jugés prioritaires par l'État. Cette approche peut conduire à un affaiblissement des mécanismes de contrôle du pouvoir, notamment en réduisant l'indépendance du pouvoir judiciaire ou en marginalisant les contre-pouvoirs institutionnels. Ainsi, des régimes comme celui de la Chine contemporaine, qui revendiquent une conception harmonieuse[64] de la société reposant sur une légalité autoritaire, illustrent bien cette dynamique. La Chine fait primer de cette façon, l'ordre social et le développement économique, sur les libertés individuelles, ce qui conduit à des interprétations flexibles des principes fondamentaux de l'État de droit.[65] L'article 1 de la Constitution de la République populaire de Chine prévoit par exemple que le Parti communiste chinois est la force dirigeante de l'État, et le pays doit adhérer à la voie du socialisme « à la chinoise »[66]. La légalité et l'État de droit en Chine sont donc intimement liés à l'autorité du Parti.

Par ailleurs, le contrôle de constitutionnalité n'existe pas au sens libéral du terme, [67] tel qu'il est conçu en France. Le droit constitutionnel chinois repose sur un principe d'interprétation législative qui se

distingue fondamentalement d'un contrôle juridictionnel indépendant.[68] Ce système a été formalisé par une résolution du Comité permanent de l'Assemblée populaire nationale (APN) de 1981, qui établit quatre règles principales en matière d'interprétation des lois[69]. Tout d'abord, le Comité permanent de l'APN détient la compétence exclusive pour interpréter la Constitution et les lois adoptées par l'APN ou par lui-même, ainsi que pour abroger toute norme inférieure contraire[70]. Cette règle confère à un organe politique, et non à une instance judiciaire, le pouvoir d'interpréter et de contrôler la conformité des lois, ce qui élimine toute indépendance dans le contrôle de constitutionnalité.

Ensuite, le Conseil des affaires de l'État, qui correspond au gouvernement chinois, est compétent pour interpréter les lois dans le cadre de ses fonctions administratives[71]. Ce mécanisme permet à l'exécutif d'ajuster l'application des lois sans passer par une instance juridictionnelle. De leur côté, les comités permanents des assemblées populaires locales sont chargés d'interpréter les normes locales. Comme l'expliquent Xu Yi-chong et Patrick Weller, ce rôle ne doit pas être minimisé puisque cela instaure une certaine décentralisation[72]. Les comités permanents assurent la coordination et la résolution des conflits, au-delà du contrôle hiérarchique que la pensée populaire attribue souvent au PCC. Enfin, la Cour suprême détient un pouvoir d'interprétation des lois, mais seulement dans le cadre de leur application en procédure juridictionnelle, sans possibilité de censurer une loi contraire à la Constitution[73].

Ce système rompt radicalement avec la logique libérale de l'État de droit qui repose sur la séparation des pouvoirs et l'existence d'un contrôle juridictionnel indépendant. Contrairement au modèle français, où le Conseil constitutionnel, et indirectement le Conseil d'État et la Cour de cassation grâce à la question prioritaire de constitutionnalité, peuvent censurer une loi contraire à la Constitution, la Chine n'offre aucun recours indépendant contre les abus du législateur[74]. Dans un État de droit libéral, le contrôle de constitutionnalité est confié à une juridiction indépendante, la Constitution est une norme supérieure qui limite le législateur, et les citoyens ainsi que les juges peuvent saisir une autorité pour faire invalider une loi inconstitutionnelle[75]. En revanche, en Chine, l'organe chargé d'interpréter la Constitution est une institution politique placée sous l'autorité du Parti communiste chinois. La Constitution n'a pas pour fonction de limiter le pouvoir du Parti, mais de légitimer son action, et aucune instance indépendante ne peut annuler une loi adoptée par l'APN, ce qui supprime tout contre-pouvoir juridique[76].

Si ce système rompt avec l'État de droit libéral, il ne constitue pas pour autant une innovation totale et présente une certaine similitude avec le légicentrisme français sous la III^{e} République[77]. À cette époque, la loi était considérée comme l'expression suprême de la souveraineté nationale, et aucun contrôle juridictionnel ne pouvait en limiter la portée. Le juge ne pouvait pas censurer une loi, et seul le législateur était perçu comme légitime pour définir le droit. Ce principe fait écho au système chinois actuel, où la loi et le législateur occupent une place prépondérante. Toutefois, une différence essentielle réside dans le fait qu'en France, sous la III^{e} République, la loi était l'émanation du Parlement dans un cadre démocratique et pluraliste, tandis qu'en Chine, elle est directement subordonnée aux impératifs du Parti communiste.

Ainsi, bien que l'interprétation législative chinoise reprenne certains aspects du légicentrisme français, elle s'en distingue par son caractère profondément autoritaire. Là où la III[e] République glorifiait la loi comme une expression de la volonté populaire, la Chine la conçoit avant tout comme un instrument au service du Parti.

Cependant, il est important de noter que la légalité autoritaire et l'État de droit ne sont pas nécessairement incompatibles. Dans certains contextes, l'État peut concilier les deux en adoptant une approche équilibrée, où l'égalité substantielle est promue tout en respectant les garanties fondamentales du droit. C'est notamment ce que Mireille Delmas-Marty[78] qualifie de pluralisme ordonné, une approche où l'intervention étatique est modulée par des mécanismes transparents et participatifs permettant de préserver l'équilibre entre égalité et liberté. Cette idée suggère qu'il est possible de concevoir un État de droit adapté aux exigences contemporaines, intégrant des objectifs égalitaires sans sacrifier les principes fondamentaux de limitation du pouvoir.

En définitive, la théorie de la légalité autoritaire offre une perspective intéressante pour repenser les rapports entre justice sociale et régulation juridique. Néanmoins, elle révèle également des problématiques auxquels l'État de droit est encore confronté face à des modèles alternatifs de gouvernance, où la légalité peut servir de justification à des formes de pouvoir plus intrusives, voire arbitraires. Cette tension souligne l'importance de préserver l'équilibre entre objectifs collectifs et libertés individuelles, un défi majeur à l'ère des transformations sociales et technologiques.

Partant, la *Digital Silk Road* ne se contente pas d'étendre les infrastructures numériques chinoises à l'échelle mondiale, elle génère également un processus de convergence des régulations. Cette convergence repose sur l'exportation des normes juridiques chinoises en matière de souveraineté numérique, de censure et de surveillance, que les pays partenaires de la BRI sont invités à adopter.

2. L'intégration des entreprises nationales à la stratégie de gouvernance numérique

La stratégie chinoise actuelle de domination numérique, incarnée par la DSR, présente des parallèles avec la démarche américaine des années 1990, bien que les contextes et les approches diffèrent. Les États-Unis ont à cette époque consolidé leur hégémonie mondiale en tirant parti de la mondialisation néolibérale et de l'essor des technologies numériques[79]. Des entreprises comme *Microsoft*, *Intel* ou plus tard *Google* ont joué un rôle crucial dans l'imposition des normes américaines en matière de technologie et de gouvernance de l'Internet. Cette période a vu émerger un cadre international dominé par les États-Unis, où les institutions comme l'Organisation Mondiale du Commerce (OMC), le Fonds Monétaire International (FMI) et *l'Internet Corporation for Assigned Names and Numbers* (ICANN) ont été utilisées pour renforcer une dépendance systémique au modèle américain[80]. Les accords commerciaux, souvent conditionnés par l'adoption de ces normes, ont permis aux États-Unis de diffuser une idéologie centrée

sur le libre marché, la démocratisation et la libéralisation économique, instaurant ainsi une forme d'hégémonie normative.

La *Digital Silk Road*, bien que s'inscrivant dans une logique similaire de diffusion normative, adopte une stratégie distincte. À travers l'exportation de technologies numériques avancées, telles que la 5G, les centres de données et les infrastructures de communication, la Chine cherche à étendre son influence en créant des dépendances technologiques dans des régions clés comme l'Asie et l'Afrique. Cette initiative s'accompagne d'une diffusion des normes technologiques chinoises, souvent centrées sur le contrôle étatique et la cybersécurité, au détriment des cadres libéraux de gouvernance numérique. Comme le souligne la géopoliticienne Nadège Rolland[81], la DSR reflète une vision souverainiste et pragmatique, où la technologie devient un levier de puissance géopolitique, permettant à la Chine de remodeler l'ordre mondial en contournant les institutions internationales dominées par l'Occident. Contrairement aux États-Unis, qui ont promu un idéal d'universalité démocratique, la Chine insiste sur le respect des *caractéristiques locales* et sur l'absence de conditions politiques[82].

Cependant, il convient de nuancer cette comparaison. Comme il a été mentionné, les États-Unis ont historiquement inscrit leur domination dans des institutions internationales qu'ils ont contribué à développer. La Chine, en revanche, privilégie une approche multipolaire, cherchant à contourner ces cadres[83] au moyen d'un ensemble d'institutions à l'image des BRICS+ (Brésil, Russie, Inde, Chine, Afrique du Sud, Iran, Égypte, Émirats arabes unis, Indonésie et Éthiopie) ou de l'Association des Nations de l'Asie du Sud-Est (ASEAN). En outre, la rhétorique chinoise met davantage l'accent sur le partenariat et le développement mutuel, notamment en Afrique, où la DSR est présentée comme une opportunité pour combler le fossé technologique, bien que cette dépendance suscite des inquiétudes quant à la souveraineté numérique des États bénéficiaires[84].

Ainsi, bien que les deux puissances partagent une ambition commune de domination globale par la technologie, leurs stratégies reflètent des visions différentes du rôle des normes dans l'ordre mondial : l'une centrée sur l'universalisme libéral, l'autre sur la redéfinition souverainiste et multipolaire des règles.

L'approche de la gouvernance numérique chinoise, qui est intrinsèquement liée à ses objectifs politiques et économiques, se fait ainsi sous l'égide du PCC afin de mettre en avant le nationalisme technologique. La légitimité du PCC repose en partie sur sa capacité à assurer la croissance économique, la stabilité sociale et le nationalisme[85]. Le Parti communiste chinois accorde une importance primordiale au développement technologique, qu'il considère comme un outil essentiel pour renforcer la puissance et la compétitivité de la nation chinoise sur la scène internationale. Dans une perspective stratégique à long terme, le PCC perçoit l'innovation technologique comme un vecteur clé pour asseoir la souveraineté du pays, réduire sa dépendance vis-à-vis des technologies étrangères et combler son retard dans certains domaines de pointe[86]. Cette dynamique s'est inscrite dans une trajectoire progressive : dans un premier temps, les autorités chinoises ont adopté une politique de régulation permissive et accommodante à l'égard des grandes entreprises technologiques, dans le but stratégique de favoriser l'émergence d'acteurs nationaux capables de concurrencer, voire de surpasser, leurs homologues

étrangers. Cette orientation a permis l'ascension de conglomérats technologiques majeurs tels qu'*Alibaba*, *Tencent* et *ByteDance*. Cependant, à partir de 2020, une inflexion notable de la politique de régulation a été observée, impulsée par le gouvernement central dans le cadre d'une stratégie visant à consolider l'autonomie technologique du pays[87].

Les sanctions imposées par les États-Unis à l'encontre des entreprises technologiques chinoises, notamment *Huawei* et *ZTE*, ont non seulement intensifié le nationalisme au sein de la population chinoise, mais ont également renforcé la détermination stratégique du gouvernement à réduire sa dépendance vis-à-vis des technologies étrangères. Ces tensions géopolitiques ont également conduit à une réorganisation des chaînes d'approvisionnement, favorisant le développement d'écosystèmes technologiques locaux et le renforcement des partenariats publics-privés[88].

La Professeure Angela Zhang a pu expliquer que les entreprises technologiques chinoises exercent une influence significative sur l'élaboration des politiques publiques en mobilisant des mécanismes d'interaction formels, tels que l'adhésion au Parti communiste chinois ou la participation aux conférences consultatives, et informels, incluant les relations privilégiées avec les élites politiques et les entreprises publiques[89]. Elles pratiquent également des stratégies de lobbying pour obtenir des avantages réglementaires ou exploiter les failles juridiques existantes. La cession stratégique de participations aux élites politiques et aux entreprises publiques constitue une pratique répandue, permettant d'assurer un soutien institutionnel et politique[90]. En définitive, le modèle de gouvernance numérique chinois repose sur une structure étatique fortement centralisée, étroitement intégrée au PCC, tandis que les entreprises technologiques ajustent leurs stratégies en fonction des orientations politiques nationales[91]. De cette façon l'État est à la fois un investisseur, un développeur et un bénéficiaire de l'économie numérique, ce qui lui confère un rôle central dans ce secteur.

Ainsi, la Chine, par des accords de coopération avec les pays partenaires de la BRI, propose un modèle alternatif de gouvernance basé sur un contrôle étatique renforcé et un isolement numérique partiel vis-à-vis des influences étrangères. La régulation numérique proposée par la Chine devient un moyen de consolider un pouvoir autoritaire à travers l'exportation de technologies et de cadres législatifs qui garantissent une gestion étatique des informations.

II. La *Digital Silk Road* : un levier pour étendre la souveraineté numérique chinoise

La DSR, qui suppose la construction d'infrastructures de communication dans les pays de la BRI, permet au gouvernement chinois d'accéder, de collecter, d'analyser et d'utiliser largement les informations et

renseignements disponibles en provenance de ces pays (A).

Cette connectivité croissante a d'abord été renforcée par le développement de la législation interne. Puis par l'exportation du modèle de régulation numérique chinois à l'échelle régionale (en offrant aux pays partenaires des technologies et des mécanismes juridiques) et international (par la présence de plus ne plus régulière de la Chine au sein d'instances internationales) (B).

A. Les moyens d'expansion du contrôle sur les infrastructures numériques

Le Plan d'action pour la connectivité et les normes de la BRI 2018-2020, publié par l'Administration chinoise de normalisation en 2017, affichait déjà l'intention de promouvoir la sagesse chinoise dans les normes internationales[92]. En d'autres termes, le gouvernement chinois souhaite promouvoir l'alignement des normes dans le cadre de son initiative *Belt and Road Initiative*. L'objectif de cette approche standardisée est d'instaurer des normes uniformes entre les États bénéficiaires, notamment en ce qui concerne les technologies clés telles que la 5G, l'IA et les systèmes de navigation par satellite. Pour cela, la Chine a eu besoin d'un corpus législatif solide et convaincant quant à son adéquation avec les défis que soulève le domaine numérique (1). Au-delà des avantages techniques, Pékin voit également dans l'établissement de normes communes un moyen de renforcer son influence et son leadership dans la gouvernance de ces technologies émergentes à l'échelle mondiale (2). Cela lui donnerait un rôle central dans la définition des protocoles qui façonneront l'avenir numérique des pays impliqués dans la BRI. La Chine cherche ainsi à faire en sorte que les États partenaires adoptent ses technologies phares, ce qui lui permettrait d'étendre son empreinte géopolitique et d'affirmer sa position de puissance technologique dominante sur la scène internationale.

1. L'adaptation du modèle législatif européen aux priorités nationales chinoises

La Loi sur la protection des informations personnelles précédemment mentionnée (*Personal Information Protection Law,* PIPL*)*[93], adoptée le 20 août 2021 et entrée en vigueur le 1er novembre 2021, vise à fournir un cadre juridique solide pour la protection de la vie privée des citoyens. Selon l'article 2 de cette loi, « les informations personnelles des personnes physiques bénéficient d'une protection juridique ; aucune organisation ou individu ne peut porter atteinte aux droits et intérêts des personnes physiques en matière d'information personnelle[94] ».

Cet article démontre la volonté du gouvernement chinois d'affirmer son respect des droits fondamentaux en matière de traitement éthique et sécurisé des données personnelles et sensibles. La PIPL est destinée à apporter une protection, basée sur le modèle du Règlement Européen sur la Protection des Données

(RGPD)[95]. Comme le RGPD, il prévoit le consentement au transfert de données (art. 14) ainsi que le droit de le retirer (art. 15) ; il comprend l'obligation d'informer la personne concernée (art. 17 et 18) et prévoit un cadre pour le transfert de données en dehors de la République populaire de Chine (Chap. III Art. 38 à 43).

Il convient néanmoins de s'interroger sur la réelle portée pratique de ces nouvelles dispositions juridiques. Sont-elles réellement mises en œuvre de manière efficace et contraignante, ou s'agit-il plutôt d'un exercice de communication destiné à apaiser les inquiétudes de la population et de la communauté internationale ?

PIPL	RGPD
Chapitre I : Dispositions générales (Art. 1-12)	Chapitre I : Dispositions générales (Art. 1-4)
Chapitre II : Règles de traitement des informations personnelles (Art. 13-37) Y compris : → *consentement de la personne concernée (Art. 14)* → *droit de retirer le consentement (Art. 15)* → *obligation d'information (Art. 17-18)*	Chapitre II : Principes (Art. 5-11)
Chapitre III : Règles relatives à la fourniture transfrontalière d'informations personnelles (Art. 38 à 43) *Y compris les règles relatives au transfert de données en dehors de la République populaire de Chine*	Chapitre V : Transferts de données personnelles vers des pays tiers ou des organisations internationales (Art. 44-50)
Chapitre IV : Droits des personnes physiques dans les activités de traitement des informations personnelles (Art. 44-50)	Chapitre III : Droits de la personne concernée (Art. 12-23)
Chapitre V : Obligations des gestionnaires d'informations personnelles (Art. 51-59)	Chapitre IV : Responsable du traitement et sous-traitants (Art. 24-43)
Chapitre VI : Autorités exerçant des fonctions de protection des informations personnelles (Art. 60-65)	Chapitre VI : Autorités de contrôle indépendantes (Art. 51-59)
Chapitre VII : Responsabilité juridique (Art. 66-71)	Chapitre VII : Recours, responsabilité et sanctions (Art. 77-84)

Figure 2 : Tableau comparatif démontrant les principales similitudes entre la réglementation chinoise sur la protection des données personnelles (PIPL) et celle de l'Union européenne (RGPD).

Un aspect particulièrement notable de ce règlement réside dans le fait qu'il couvre également les activités hors de Chine qui concernent des ressortissants chinois, soit en leur proposant des produits ou services, soit en traitant les données personnelles d'individus situés en Chine[96].

La Chine continue donc d'imposer sa politique de gestion des données aux partenaires qui souhaitent bénéficier de son expertise technologique. Ce contrat est largement déséquilibré si l'on considère le contrôle de la Chine à travers ses infrastructures dans les territoires partenaires, et l'utilisation des données capturées pour le développement et le raffinement algorithmique. Cette captation permet également d'optimiser les stratégies d'investissement et de commerce extérieur[97], l'alignement législatif et donc la diffusion du modèle chinois dans le pays contractant.

En outre, la PIPL renforce la surveillance des données en octroyant au gouvernement chinois un pouvoir étendu pour accéder à ces informations dans le cadre de la protection de l'ordre public. En ce sens, elle va bien au-delà de la simple protection des droits individuels, en permettant à l'État d'utiliser les données personnelles comme un levier pour affirmer sa domination numérique tout en prétendant protéger la vie privée des citoyens. Ainsi, loin de représenter une réconciliation entre la protection des droits et la sécurité nationale, la PIPL illustre une hiérarchisation où la sécurité du régime prime sur les droits individuels.

Mais bien que cette pratique crée un environnement uniforme en termes de ressources numériques, et même si les États partenaires adoptent certains aspects ou idéologies des approches chinoises en matière de gouvernance, il n'y a pas d'exportation totale et mondiale de ce modèle. La Chine a établi une frontière numérique pour garantir sa souveraineté numérique sur son territoire, le contrôle et la maintenance des données à l'intérieur du pays et la prééminence des entreprises chinoises sur le marché national[98]. Cette politique de cloisonnement ne peut être adoptée et appliquée sur les territoires des pays partenaires, qui ont contractuellement accepté le transfert de leurs données vers la Chine et l'ouverture de leurs frontières aux infrastructures numériques étrangères. Ce contrat est donc déséquilibré du point de vue des pays hébergeant ces infrastructures.

En exportant ses normes et ses pratiques de régulation, la Chine favorise un environnement où les gouvernements étrangers adoptent des stratégies similaires à celles utilisées en Chine, garantissant ainsi une forme de convergence numérique sous le contrôle de Pékin. À travers cette initiative, la Chine ne se contente pas de promouvoir son *leadership* technologique, elle redéfinit également les rapports de force internationaux, en particulier dans les régions stratégiques que sont l'Asie et l'Afrique. Cependant, cette démarche soulève des interrogations profondes quant à son effet sur l'État de droit et les souverainetés numériques des pays partenaires.

Dans les pays d'Asie et d'Afrique, la DSR offre des opportunités significatives de développement numérique, permettant de combler le fossé technologique et d'accélérer la transformation digitale. Néanmoins, cette dépendance aux technologies chinoises peut entraîner une érosion de la souveraineté numérique des États bénéficiaires. Les accords conclus dans le cadre de la DSR sont souvent asymétriques, favorisant des entreprises chinoises comme *Huawei* ou *ZTE*, et permettant à la Chine de renforcer son influence économique, politique et technologique. En outre, les critiques soulignent que ces partenariats s'accompagnent parfois d'un transfert implicite des normes chinoises en matière de gouvernance numérique, notamment en matière de cybersurveillance et de contrôle étatique des

infrastructures numériques, ce qui peut compromettre les libertés fondamentales et la transparence[99].

Sur le plan international, la DSR soulève également la question d'un nouvel ordre numérique mondial où la Chine tenterait de contourner les cadres normatifs dominés par l'Occident. En exportant son modèle technologique, Pékin vise à éroder les standards internationaux établis par des institutions comme l'OCDE ou les Nations unies, en promouvant des normes plus compatibles avec sa vision souverainiste du cyberespace. Cette dynamique met en lumière une tension entre la coopération technologique transnationale et la fragmentation normative mondiale, où la technologie devient un levier de pouvoir géopolitique[100]. Ainsi, l'analyse de la DSR révèle que la Chine utilise le numérique non seulement comme un outil de développement, mais également comme un moyen d'asseoir son influence et de remodeler l'équilibre des relations internationales, parfois au détriment de l'État de droit dans les pays partenaires.

2. La construction des normes numériques des États partenaires selon l'exemple chinois

L'initiative *Smart Burkina* financée par la Chine a permis au Burkina Faso d'établir et d'améliorer sa connectivité numérique[101]. En fournissant des systèmes numériques via *Huawei* et *ZTE*, l'objectif de la Chine était d'aider le pays à faire face à ses problèmes de sécurité et de terrorisme[102]. Mais cette collaboration est largement dans l'intérêt de la Chine, puisque nombre de ses partenaires en Afrique s'inspirent de ses normes faute de disposer de cadres complets de protection[103]. Dans ce cas, les pays partenaires s'inspirent des normes pour renforcer ou construire leur corpus législatif en matière de gouvernance numérique et de cybersécurité.

Ces changements dans les politiques nationales favorisent les intérêts chinois au détriment des priorités locales des États ciblés. Par exemple, pour soutenir son développement technologique, le Pakistan a introduit en 2023 de nouvelles réglementations régissant l'utilisation et l'échange de données.

En effet, la Chine a investi massivement dans la construction de câbles sous-marins reliant les pays partenaires de la BRI. Ces câbles servent non seulement à améliorer les connexions Internet, mais aussi à renforcer le contrôle de l'État chinois sur les flux de données internationaux. En 2017 particulièrement, la Chine a lancé un projet de câble sous-marin dans le cadre du *China-Pakistan Economic Corridor* (CPEC) qui a développé les connexions du Pakistan avec le monde[104].

C'est dans ce contexte que le Pakistan a souhaité régir l'utilisation et l'échange des données des citoyens à l'image de la PIPL par la mise en place d'une Loi pakistanaise sur la protection des données personnelles (PDP)[105]. À cet égard, la réglementation pakistanaise propose la création d'un « contrôleur de données ou d'un sous-traitant »[106] tel que le délégué à la protection des données (DPO). Le texte comprend entre autres des dispositions sur le consentement explicite[107], le « droit à

l'effacement »[108] et la portabilité des données[109]. Cette législation prévoit également la création de la Commission Nationale pour la Protection des Données Personnelles (NCPDP),[110] chargée de superviser la mise en œuvre de la réglementation et de veiller au respect des droits des citoyens à la confidentialité et à la sécurité des données.

Ce projet de loi, qui vise à renforcer la confiance du public dans l'économie numérique pakistanaise, est né à un moment critique, où les droits des citoyens ont été mis en péril par le gouvernement. Les autorités ont restreint l'Internet mobile et le haut débit pendant quatre jours en mai 2023, après l'arrestation de l'ancien Premier ministre Imran Khan[111]. Le gouvernement avait également bloqué l'accès à plusieurs plateformes de réseaux sociaux telles que Facebook, X et YouTube. Ce scénario s'est répété à la suite des élections législatives houleuses du 8 février 2024[112]. Les votes ont été marqués par la suspension des services Internet mobiles par le gouvernement. Les coupures du réseau Internet se sont produites malgré les assurances de son fonctionnement par l'Autorité des télécommunications du Pakistan (PTA) le jour du scrutin.

Cette régulation s'inscrit dans une logique de contrôle étatique des infrastructures numériques. C'est une illustration de la multipolarité législative dans la gouvernance technologique. Les mesures prises par le gouvernement pakistanais sont justifiées par des préoccupations de sécurité et de maintien de l'ordre public, et témoignent d'une conception où l'accès à l'information et la gestion des réseaux numériques sont étroitement liés aux enjeux politiques internes. Il est possible de faire un parallèle avec l'approche de l'Union européenne de la gestion des crises numériques.

L'article 36 du *Digital Services Act* prévoit à ce titre, un mécanisme de réponse aux crises permettant à la Commission européenne d'imposer temporairement des obligations spécifiques aux très grandes plateformes en ligne (VLOPs) et aux très grands moteurs de recherche (VLOSEs) en cas de menace grave pour la sécurité publique ou la santé dans l'Union européenne.[113] Tout en maintenant un cadre normatif axé sur la transparence et la proportionnalité, ces mesures s'effectuent sous la supervision de la Commission européenne et dans le respect des droits fondamentaux.

Ces mécanismes d'urgence illustrent la coexistence de modèles réglementaires variés, certains États privilégiant une intervention directe et souveraine, tandis que d'autres mettent en place des mécanismes institutionnels de supervision. Cette diversité pose la question de l'articulation entre ces approches dans un espace numérique globalisé, où les cadres nationaux doivent composer avec des plateformes opérant à une échelle transnationale.

Aussi, la section 54 de la Loi pakistanaise sur les télécommunications de 1996 prévoit par exemple que « le gouvernement fédéral peut autoriser toute personne ou personnes à intercepter des appels et des messages ou à retracer les appels via n'importe quel système de télécommunication »[114] , dans le cas d'intérêts de sécurité nationale. Cette loi fait donc référence à d'éventuelles restrictions en cas d'état d'urgence. En pratique, le recours à cet article a été observé dans le cadre de coupures de réseau injustifiées ou routinières[115]. Les tribunaux ont annulé le pouvoir de la PTA de suspendre les services

au motif que « […] la suspension des services de téléphonie mobile par l'Autorité est *ultra vires* de la section 54 ; les droits fondamentaux garantis par les articles 10-A, 9, 15, 16, 17, 18, 19 et 19-A sont violés lorsque les utilisateurs de téléphones mobiles sont privés de l'utilisation des services ; l'accès aux services de télécommunications est devenu un droit fondamental »[116]. Cependant, en avril 2020, la Cour suprême a confirmé le droit du gouvernement de suspendre les réseaux mobiles, estimant que ces services étaient « fermés pour éviter des incidents désagréables, le terrorisme »[117].

Cette gouvernance n'est pas sans rappeler celle de la Chine qui tend vers un protectionnisme numérique national grâce à un contrôle strict de l'Internet chinois. Le gouvernement chinois a choisi de censurer les plateformes comme Facebook et les moteurs de recherche comme *Google*, au profit du développement de plateformes nationales comme *Wechat* et *Weibo*[118]. Le *Great Firewall of China*[119], qui bloque les contenus jugés indésirables par le gouvernement sur l'Internet chinois, est l'outil qui démontre le mieux cette souveraineté numérique. De ce fait, les recherches sur Internet et autres activités en ligne dépendent presque exclusivement d'applications chinoises, elles-mêmes disponibles via des plateformes chinoises, compte tenu des règles strictes que doivent respecter les plateformes étrangères[120].

Selon Matthew S. Erie et Thomas Streinz, « Bien que les entreprises chinoises ne soient pas intrinsèquement des instruments de l'État chinois, elles restent intégrées aux systèmes de contrôle de l'État-Parti, dont les différentes méthodes méritent d'être réexaminées »[121]. En conséquence, de nombreux pays réagissent au risque de cybersécurité qui pèse sur leurs infrastructures de communication et les données de leurs citoyens. En janvier 2024, la société vietnamienne *Viettel* a par exemple annoncé qu'elle deviendrait indépendante des infrastructures chinoises et étrangères afin de fournir la 5G au sein même du pays.[122] D'autres pays, manquant de ressources financières ou techniques pour s'émanciper à l'instar du Vietnam, ont plutôt décidé de faire appel à leurs grands concurrents américains. Par exemple, en 2021, la licence de service de télécommunications privatisée de l'Éthiopie a été attribuée à un consortium financé par les États-Unis comprenant *Vodafone*, *Vodacom*, *Safaricom* et *Sumitomo Corporation*. Le sud-africain *MTN Group Ltd*, financé par la Chine, a perdu le contrat[123]. La perte de ce marché n'est pas négligeable. La fourniture d'infrastructures numériques par la Chine a une influence sur les flux de données et les pratiques de stockage.

Selon un groupe de réflexion du *Lowy Institute* en Australie, l'importation de technologies chinoises présente un risque important car « Le danger pour les autres pays qui importent les solutions technologiques chinoises est qu'il en résulte une acceptation croissante de la surveillance de masse, une accoutumance aux restrictions des libertés et une diminution des contrôles sur la collecte et l'utilisation des données personnelles par l'État, même après que la crise de la santé publique se soit résorbée »[124]. Conscient des critiques qui lui sont adressées, le gouvernement chinois a déployé des efforts considérables pour élaborer des normes et des réglementations respectueuses des principes fondamentaux des droits de l'homme comme le démontre la PIPL.

B. L'exportation d'un modèle de gouvernance numérique chinois

Alors que la BRI s'intéresse principalement aux infrastructures physiques (routes, ports, chemins de fer), la DSR se concentre sur la connexion numérique entre la Chine et le reste du monde, en particulier les pays en développement. Les pays hôtes de ces projets d'infrastructures chinois sont confrontés à un dilemme. D'une part, ils bénéficient des retombées économiques et technologiques importantes générées par ces investissements massifs en termes de développement des réseaux, de transferts de technologies de pointe et de création d'emplois. Mais d'un autre côté, ils s'inquiètent légitimement des risques liés à une dépendance technologique excessive à l'égard de la Chine, ainsi que des implications potentielles sur leur souveraineté numérique et leur capacité à contrôler les flux d'informations transitant par ces infrastructures (1).

Au-delà des enjeux purement économiques et technologiques, ces partenariats permettent également à la Chine de diffuser et de promouvoir ses propres standards légaux et techniques, parfois en contradiction avec les principes démocratiques et les libertés fondamentales défendues par les pays occidentaux (2). Ce faisant, la Chine cherche progressivement à façonner un écosystème numérique mondial plus favorable à ses intérêts géopolitiques et idéologiques.

1. La création de nouvelles formes de collaborations étatiques pour le partage technologique

L'entrée en vigueur du PIPL en 2021 n'a entraîné aucun changement dans les mesures de surveillance invasives de la Chine. Pourtant, les principes éthiques liés soulignent l'importance de l'équité, notamment lorsqu'il s'agit de l'utilisation des données personnelles : « la transparence de la prise de décision ainsi que l'équité et la justice des résultats doivent être assurées »[125]. En témoignent les nombreuses condamnations des pratiques chinoises en matière de traitement des données et de surveillance par les États-Unis. Le gouvernement américain a ainsi sanctionné les entreprises chinoises qui ne respectent pas les droits de l'homme, les empêchant ainsi de faire des affaires avec des entreprises américaines[126].

Pierre Bellanger estime que cette dynamique de la politique chinoise s'explique par la recherche du maintien des particularités locales et la création d'une interdépendance entre états, face à la mondialisation. Selon lui, « l'État moderne doit également garantir la survie de l'écosystème social et économique qu'il forme dans un environnement international »[127]. Il semble cependant que le modèle chinois décrit par cet auteur en 2012[128] soit allé au-delà de cette interdépendance. La Chine a réussi à créer un partenariat déséquilibré avec les pays cocontractants grâce à un besoin continu de ses technologies et de son infrastructure numérique. Cette situation lui permet d'asseoir sa souveraineté numérique et d'accroître son influence géopolitique. Cette dépendance technologique de nombreux pays

vis-à-vis de la Chine donne à cette dernière un levier de négociation stratégique. Pékin peut ainsi dicter ses conditions et faire valoir ses intérêts, que ce soit en matière de politique commerciale, de sécurité ou de gouvernance des données. Cette situation lui permet également de mieux contrôler les flux d'information et les écosystèmes numériques à l'échelle mondiale, renforçant ainsi son soft power au détriment du déclin de la souveraineté – au moins sur le plan numérique – de ses partenaires.

La souveraineté des États, fondement du système international westphalien, repose sur l'autorité exclusive d'un État sur son territoire et ses affaires intérieures, ainsi que sur la reconnaissance mutuelle entre États de leur indépendance juridique. De là, la souveraineté numérique émerge comme un enjeu majeur pour la protection de l'espace numérique national, incluant la régulation des données, la gestion des infrastructures numériques critiques et la protection contre les cybermenaces. Alors que la mondialisation numérique efface les frontières physiques traditionnelles, le docteur Nir Kshetri explique que les données personnelles sont devenues des cibles stratégiques, conduisant les gouvernements à développer de nouveaux mécanismes pour exercer leur autorité et leur contrôle dans le cyberespace[129]. En outre, Milton Mueller[130] souligne que la tension entre la nécessité d'un contrôle étatique et la nature intrinsèquement transnationale du cyberespace remet en question les paradigmes traditionnels de souveraineté, obligeant les États à repenser leurs modes d'action et de coopération. C'est dans cette optique que la Chine a très tôt voulu affirmer sa position de leader dans ce domaine et exporte aujourd'hui son modèle de surveillance et de contrôle de masse grâce à ses grandes entreprises.

Le PCC utilise ainsi ces technologies de surveillance numérique à l'étranger, par exemple via *Huawei Technologies*[131]. « En 2017, Huawei a répertorié 40 pays dans lesquels ses technologies de ville intelligente avaient été introduites ; 45 en 2018, cette portée aurait plus que doublé pour atteindre 90 pays (dont 230 villes) »[132]. *Huawei* a remporté un certain nombre de contrats de plusieurs millions de dollars, notamment celui du réseau cellulaire public *NetOne* au Zimbabwe[133]. Ce déploiement massif à l'étranger soulève des questions sur l'équilibre des intérêts entre la souveraineté nationale, qui implique le contrôle d'un État sur ses affaires intérieures et extérieures, et les bénéfices d'un tel contrat en termes d'accès à une technologie innovante et le bien-être citoyen.

À cet égard, nous proposons une typologie des statuts qu'un État partenaire peut adopter dans le cadre d'un contrat de collaboration avec la Chine au sein de la DSR. Cette classification repose sur une distinction fondée sur le degré d'autonomie – et donc de souveraineté numérique – accordé à cet État. Notre proposition offre ainsi un cadre d'analyse permettant d'appréhender sous un nouvel angle la diversité des relations établies entre la Chine et ses partenaires dans ce domaine.

Le premier type de statut correspond à une position de « dépendance étroite » à l'égard de la Chine. Dans ce cas, l'État partenaire se retrouve dans une situation de forte subordination technique et économique par rapport à la Chine. La prédominance chinoise dans la relation réduit l'autonomie décisionnelle et la souveraineté numérique de l'État concerné. Ce phénomène s'illustre par exemple par la perte de contrôle des infrastructures chinoises installées sur les territoires des pays partenaires, incapables de remplir financièrement leur part de marché[134]. Par exemple, de 2010 à 2015, la Chine a accordé un prêt total

de 4,8 milliards de dollars pour financer un certain nombre de projets de développement au Sri Lanka, notamment la construction du port en eau profonde de Hambantota. Ce projet phare visait à transformer ce port de pêche en une plaque tournante du commerce maritime régional. En 2016, la Chine a encore augmenté son prêt au Sri Lanka à 6 milliards de dollars. Cependant, le gouvernement sri lankais n'a pas été en mesure de rembourser ces dettes colossales. Se trouvant acculé, ce pays a accepté la proposition chinoise de céder le contrôle du port de Hambantota. Ainsi, en 2017, 1,12 milliard de dollars de dette du Sri Lanka ont été annulés et remplacés par un nouveau prêt de 1,5 milliard de dollars de la Chine. En échange, Pékin a obtenu une participation majoritaire de 70 % dans le port d'Hambantota, ainsi qu'un bail de 99 ans pour l'exploiter[135]. Le Sri Lanka se retrouve alors largement dépendant des infrastructures et des financements chinois, limitant drastiquement sa capacité à définir souverainement sa propre stratégie géopolitique.

Le deuxième type de statut fait référence à un phénomène que nous désignons sous le terme d' « acquiescement de l'État ». Cette notion nouvelle permet d'éclairer sous un prisme inédit la dynamique de consentement et d'alignement stratégique observée dans certaines collaborations au sein de la DSR. L'acquiescement de l'État correspond à un État qui, bien que conscient des risques encourus concernant sa sécurité intérieure et le respect des droits de ses citoyens, choisit de participer à l'initiative DSR pour d'autres intérêts qu'il juge prioritaires. Il serait erroné d'occulter la complexité des dynamiques géopolitiques et économiques en jeu. En effet, si la Chine adopte une approche interventionniste en matière de contrôle des infrastructures numériques et de gouvernance des données, cette politique ne se réduit pas nécessairement à une pure imposition. De nombreux États, notamment ceux du Sud global, voient dans le modèle chinois un cadre attractif en raison de son efficacité perçue, de ses financements massifs et de l'absence de conditionnalités politiques strictes comparables à celles imposées par les institutions occidentales. Premièrement, il ne s'agit pas de qualifier la Chine uniquement d'État autoritaire imposant sa volonté et subordonnant ses partenaires, sans reconnaître les motivations et les bénéfices potentiels pour ces pays.

Deuxièmement, cela nierait l'autonomie et la volonté de ces États de conclure des contrats et de coopérer avec la Chine dans le cadre de leurs propres stratégies de développement et opportunités économiques. Cette vision unilatérale ignorerait le rôle actif des pays partenaires, qui ne sont pas de simples récepteurs passifs d'une influence chinoise, mais des acteurs stratégiques poursuivant leurs propres intérêts. L'État exerce sa souveraineté en consentant à une collaboration déséquilibrée, en se soumettant aux conditions de son partenaire, pour tenter de combler ses propres lacunes politiques, économiques ou sociales.

Dans le cas du Burkina Faso, l'une des raisons de ce partenariat est « un manque de soutien de la part d'autres bailleurs de fonds majeurs dans le développement des infrastructures critiques de TIC en Afrique »[136], ce qui a conduit ces États africains à « ouvrir la porte à l'investissement de Pékin »[137] leur permettant de jouer « le rôle de premier plan dans le développement de telles infrastructures sur le continent »[138].

L'Allemagne fait partie des pays européens qui ont par exemple collaboré avec la Chine dans le cadre de la BRI. Duisbourg est une ville connue pour son port et pour accueillir le premier train express Chine-Europe (*CR Express*) depuis 2011[139].

Cosco, qui proposait d'acquérir 35% du terminal à conteneurs CTT (*Container terminal Tollerort*) auprès du géant hambourgeois HHLA en septembre 2021, a finalement obtenu 25% des actions demandées. Après plusieurs semaines de réflexion, le gouvernement a autorisé une participation chinoise limitée.[140] L'Allemagne voulait avant tout s'assurer que l'entreprise chinoise ne prenne pas le contrôle de ses infrastructures. En tant qu'acteur numérique de la DSR, *Huawei* avait également signé un protocole d'accord avec la ville allemande en 2019 pour le déploiement d'une ville intelligente qui n'a jamais vu le jour après le recul du gouvernement allemand.[141] Cet exemple n'illustre pas une relation équilibrée entre les partenaires, mais plutôt une inquiétude quant aux véritables intentions de la Chine. En effet, après que la firme chinoise a été accusée d'espionnage, elle est désormais interdite par l'Allemagne pour tout déploiement de son réseau 5G[142].

Dans ce cas, le choix de collaborer avec la Chine reste une manifestation d'autonomie et de la capacité du pays à définir et poursuivre ses propres intérêts stratégiques. Il est cependant possible de douter de la pertinence de l'évaluation des risques et des avantages potentiels de ces partenariats en fonction de leurs propres priorités nationales et économiques.[143] Existe-t-il réellement une volonté autonome de contracter avec la Chine si aucun autre partenaire du pays n'a répondu à leur demande de développement de la connectivité et de l'économie du territoire ? La frontière entre acceptation autonome et dépendance est donc ténue.

La notion d'acquiescement de l'État permet avant tout de mettre en évidence la balance entre les risques et les bénéfices pour les citoyens. Cette théorie met en évidence la manière dont les gouvernements arbitrent entre les opportunités et les risques liés à l'adoption d'une technologie. Dans le cas du déploiement de la 5G, cela se traduit par un équilibre entre la promotion de l'innovation et la préservation des intérêts nationaux. L'un des principes clés souvent évoqués dans ce contexte est celui de la neutralité technologique[144], qui implique que les États ne favorisent pas une technologie ou un fournisseur spécifique, mais laissent place à une concurrence ouverte et à une adoption basée sur la performance et les besoins nationaux.

Toutefois, cette neutralité n'est jamais absolue et comporte une contrepartie. Si elle facilite l'intégration de technologies avancées, favorisant l'innovation, l'efficacité économique et l'amélioration des services publics (par exemple via des infrastructures plus performantes pour les villes intelligentes ou les communications d'urgence), elle pose également des défis stratégiques. Les États doivent ainsi s'assurer que cette ouverture ne les expose pas à des risques en matière de sécurité nationale, de souveraineté numérique et de protection des données personnelles. Dans un contexte où les infrastructures de télécommunications sont devenues un enjeu géopolitique, certaines puissances privilégient une approche plus interventionniste, conditionnant l'accès aux marchés à des garanties spécifiques (audit des équipements, restrictions sur certains fournisseurs). L'acquiescement étatique devient alors une forme de

validation stratégique, où l'adoption technologique ne se limite pas à des considérations purement économiques, mais reflète également des choix politiques et sécuritaires de long terme. Les décideurs politiques doivent donc procéder à une analyse approfondie des impacts à court et à long terme de leurs décisions concernant le déploiement des réseaux 5G.

Le troisième type correspond à une « adhésion à la philosophie chinoise » par l'État partenaire. Il s'agit d'une forme d'alignement idéologique dans laquelle l'État étranger adopte le modèle de gouvernance chinois. Chaque État ayant ses propres valeurs et objectifs personnels, l'intégration profonde et totale des principes, institutions et pratiques socio-économiques chinoises au sein du pays partenaire reste hypothétique. Il existe cependant des exemples de pays qui ont opté pour le DSR et ont volontairement utilisé le modèle chinois de surveillance numérique. Les sociétés chinoises *Dahua Technology* et *Hangzhou Hikvision Digital Technology*, détenues en partie par l'État chinois, ont contribué à implanter la technologie de reconnaissance faciale[145] sur le territoire chinois, afin de mettre en place des villes intelligentes. À Foz do Iguaçu, par exemple, l'Agence fédérale brésilienne pour le développement industriel s'est chargée d'installer des caméras chinoises *Hikvision* avec reconnaissance faciale, dans le cadre du projet FronteiraTech[146]. L'objectif de ce projet était notamment de surveiller la frontière avec le Paraguay. Cette entreprise chinoise, comme Dahua, est accusée de fournir des caméras de reconnaissance faciale permettant aux forces de police de reconnaître certains groupes ethniques au sein de la population et de contribuer à leur répression en Chine[147] ou ailleurs[148]. Cela alerte sur un risque inhérent aux technologies de surveillance par reconnaissance faciale, de discrimination et de contrôle excessif de la part des autorités, qui porterait atteinte à la vie privée.

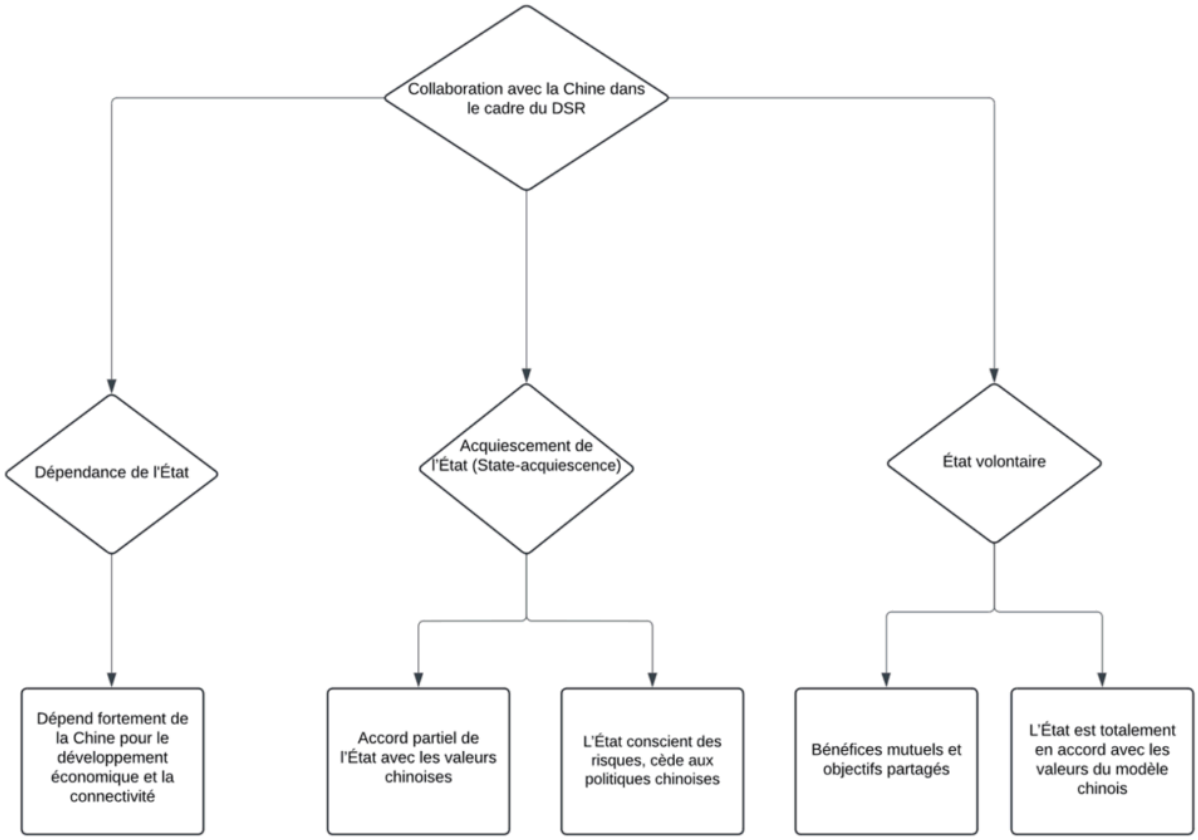

Figure 3 : Types de statut d'un État partenaire de la Chine dans le cadre de l'initiative des Nouvelles Routes de la Soie

Ainsi, l'équilibre recherché doit prendre en compte non seulement les avantages économiques et sociaux immédiats pour les citoyens, mais également les implications à long terme pour l'indépendance et la résilience de l'État. Une approche équilibrée devrait plutôt impliquer de développer des partenariats qui encouragent l'adoption de technologies neutres tout en garantissant que ces technologies respectent les lois nationales du pays dans lequel la technologie est déployée et protègent les intérêts souverains de l'État. En fin de compte, la clé réside dans une gouvernance technologique qui harmonise les aspirations à une meilleure qualité de vie des citoyens, avec les impératifs de souveraineté et de sécurité nationale. Il faut pouvoir s'assurer que les technologies déployées répondent à des critères et standards valables à grande échelle. À cette fin, la Chine s'engage activement au sein des organismes internationaux pour travailler à l'établissement de ces normes. Des normes qui renforceront la légitimité des technologies numériques déployées au sein de la DSR.

2. L'influence chinoise dans la normalisation numérique mondiale

L'adoption de technologies et de normes chinoises dans les pays de la BRI et ailleurs permet à la Chine de faire valoir avec force la pertinence de sa position sur le marché et la maturité de ses technologies lorsqu'elle promeut l'adoption internationale des normes chinoises. Cette approche a permis à la Chine de réussir à établir des normes techniques internationales dans des domaines critiques tels que les villes intelligentes et la 5G. Déjà en 2020, l'Administration de normalisation de la République populaire de Chine (SAC), avait proposé des *Principaux points du travail national de normalisation en 2020*[149] pour fixer les objectifs à atteindre par ses experts, en vue de standardiser l'IA. Il a été clairement annoncé que le pays, en tant que membre permanent de l'ISO et de la CEI, entendait contribuer activement à ces organismes. En ce sens, le Président, soutenu par ses départements, joue un rôle moteur dans la réforme de la gouvernance au sein des organismes internationaux de normalisation. Dans ce processus, la Chine souhaitait déjà partager les pratiques chinoises et proposer des solutions chinoises[150].

L'année suivante, un *Schéma national de développement de la normalisation* est mis en place[151]. Le plan considère la normalisation comme un moyen de renforcer la compétitivité nationale globale, c'est-à-dire de « promouvoir un développement de haute qualité et construire un pays socialiste moderne dans la nouvelle ère »[152]. La Chine souhaitait accélérer son développement économique et social grâce à ces normes.

En mettant particulièrement l'accent sur l'intelligence artificielle, la RPC a publié des Lignes directrices pour la construction de normes nationales sur les systèmes d'intelligence artificielle de nouvelle génération.[153] Ce projet, comme son nom l'indique, proposait la construction d'un appareil de normalisation pour l'IA et les technologies liées à l'IA afin de « guider le développement ordonné de la normalisation de l'IA » et, en outre, « d'étudier les règles générales de construction et d'élaboration de systèmes de normes »[154]. Pour 2023, il était prévu « un système de normes sur l'IA »[155]. Le programme de normalisation ITU-T de l'Union internationale des télécommunications (UIT) présente alors un intérêt particulier pour la Chine. Depuis 2012, le nombre de membres chinois de cette organisation a été multiplié par six, renforçant ainsi la contribution du pays aux débats.[156] La Chine compte désormais plus de membres de l'UIT-T que les États-Unis et coparraine la majorité des sujets soumis à l'UIT-T[157]. Selon le rapport du NIST, sur les 2 766 travaux de l'UIT-T en cours entre 2017 et 2022, dans tous les secteurs, des entreprises chinoises ont été impliquées en tant que « membres de soutien » dans 646 d'entre eux[158].

Cependant, certains chercheurs comme Sorina Teleanu, estiment que ce nombre croissant fait partie d'une stratégie d'influence de la Chine, car bon nombre des propositions avancées ne résolvent pas de problèmes réels et ne proposent pas non plus de solutions techniques[159]. Reste que les membres chinois ont néanmoins contribué à de nombreux documents importants. La Chine a rédigé de nombreux

rapports techniques et recommandations clés dans le cadre de normalisation des villes intelligentes de l'UIT. Les éditeurs de *Wuhan FiberHome International Technology Co*, Ltd ont par exemple rédigé la seule recommandation « générale » actuellement en vigueur relative aux villes intelligentes, qui définit le « Vocabulaire des villes et communautés intelligentes »[160]. De même, en tant que membre de l'ISO, la Chine a réussi à rédiger plusieurs normes fondamentales pour l'Internet des objets (IoT), telles que l'architecture de référence « ISO/IEC 30141 : 2018 pour l'Internet des objets (IoT) »[161].

Dans le domaine spécifique de l'intelligence artificielle, le SAC a dirigé le projet ISO/IEC 30150-31 Technologies de l'information – Interface utilisateur d'informatique affective (AUI) – Partie 31 : Annotation des émotions,[162] approuvé comme élément de travail en janvier 2020[163]. Également ISO/ L'IEC TR 24372:2021 Technologies de l'information – Intelligence artificielle (IA) – Vue d'ensemble des approches informatiques pour les systèmes d'IA, a été publiée en 2021, suite à un rapport technique réalisé dans ce domaine pour le première fois par la Chine. Le pays bénéficie en effet d'une certaine légitimité en la matière grâce à son expérience dans de nombreuses exportations de technologies de smart city et dans la construction de projets de smart city à l'étranger comme ce fut le cas au Burkina Faso. Un rapport de janvier 2020 a identifié 398 projets exportant des technologies de villes intelligentes par des entreprises chinoises (impliquant 106 pays)[164]. Cette expertise renforce la pertinence de sa participation et de son leadership dans la promotion des normes techniques en intelligence artificielle et autres technologies informatiques auprès des organismes de normalisation internationaux.

En réponse aux résistances institutionnelles qu'elle rencontre dans sa tentative de façonner des normes techniques mondiales, la Chine participe à des groupes de gouvernance spécifiques à la région asiatique. À cette occasion, les normes régionales asiatiques, aux côtés de celles proposées par les organismes internationaux, pourraient créer des normes incompatibles[165]. Il convient toutefois de rappeler que promouvoir ses propres intérêts nationaux et mettre en valeur les entreprises nationales sont des stratégies également utilisées par d'autres États, notamment les États-Unis[166]. Si la Chine est de plus en plus active dans les cercles de gouvernance numérique, elle a également cherché à contrer certains éléments du *statu quo* actuel, notamment la prééminence des États-Unis. Même si la Chine n'exporte pas nécessairement son propre système politique via des systèmes numériques, les dirigeants chinois souhaitent remettre en question l'ordre mondial défini par les nations occidentales.

De manière générale, la BRI cherche à forger des liens économiques plus étroits entre la Chine et ses voisins, principalement membres d'Asie centrale et de l'Organisation de coopération de Shanghai (OCS). Cependant, à travers cette approche, la Chine tente non seulement de rivaliser avec le G7, mais aussi à s'en inspirer afin de gagner en crédibilité et en influence sur la scène internationale[167]. Cette volonté de se positionner comme un acteur majeur sur la scène géopolitique mondiale s'est traduite par la tenue, en juin 2018, du sommet de l'OCS à Qingdao, en Chine, alors même que se tenait le G7 au Canada[168]. Cet événement illustre l'ambition de Pékin de promouvoir une vision alternative de la coopération internationale, centrée sur le développement économique et la connectivité régionale.

Il s'agit de la première organisation internationale directement inspirée et créée à l'initiative de Pékin.

L'organisation a été créée en 2001, réunissant initialement la Russie, la Chine et les quatre États d'Asie centrale à l'exception du Turkménistan, pour assurer la sécurité dans la région d'Asie centrale[169].

Cependant, bien que l'OCS ait été créée dans le but de promouvoir la coopération et la stabilité régionale, les États membres sont confrontés à des tensions qui ralentissent, voire parfois empêchent, des discussions ouvertes. La guerre en Ukraine déclenchée par la Russie a par exemple marqué le discours du Président russe lors du 22e sommet de l'OCS à Samarkand les 15 et 16 septembre 2022[170]. Cette situation délicate illustre les rivalités internes qui mettent à mal le partenariat stratégique entre la Russie et la Chine, même s'il est considéré comme le cœur de l'organisation. L'OCS reste un tremplin essentiel pour la Chine qui souhaite affirmer son *leadership* régional. En effet, l'organisation représente une vitrine importante pour la promotion de la DSR. Maintenir les relations de la Chine avec la Russie, l'un des principaux territoires de la BRI, est donc fondamental pour garantir un accès privilégié à l'Europe.

La *Digital Silk Road* incarne une stratégie géopolitique ambitieuse de la Chine visant à étendre sa souveraineté numérique à l'échelle mondiale en développant des infrastructures numériques et en exportant des cadres normatifs comme la PIPL. La Chine cherche à imposer un modèle de gouvernance numérique fondé sur un contrôle étatique centralisé. Cette approche, qui repose sur une interprétation autoritaire de la légalité, contraste avec les conceptions occidentales fondées sur l'État de droit, où la protection des droits fondamentaux et la séparation des pouvoirs structurent la régulation du numérique.

Dans ce contexte, la diffusion extraterritoriale des régulations chinoises à travers la DSR conduit à un alignement juridique de certains États partenaires sur un modèle où la souveraineté nationale est exercée par un contrôle renforcé des données et des flux d'informations. Cette influence normative questionne l'équilibre entre sécurité nationale et libertés fondamentales, dans un monde où la gouvernance d'Internet oscille entre des visions décentralisées et multilatérales et des approches étatiques et unilatérales.

L'exportation du modèle chinois pousse à définir les contours de la légalité autoritaire, où le droit devient un instrument de pouvoir plutôt qu'un garant de la protection des individus. Ainsi, l'avenir de la régulation numérique mondiale dépendra de la capacité des acteurs internationaux à promouvoir une gouvernance respectant à la fois les principes fondamentaux de l'État de droit et les impératifs de sécurité et de souveraineté nationale, tout en évitant une fragmentation normative excessive du cyberespace.

Emma MIQUEL,

Doctorante en droit privé, C3RD

Co-présidente ADICL

[1] KERVÉGAN, Jean-François. Hegel, l'État, le droit. *Droits*, 1992, n°16, p. 21.

[2] La notion de souveraineté trouve son origine chez Jean Bodin, dans *Les Six Livres de la République* (1576), où il la distingue du pouvoir absolu et perpétuel. Selon Richard Falk, la souveraineté est un concept dynamique, en perpétuelle transformation. Dans sa conception moderne, elle fait référence à la capacité d'un État à définir librement ses actions et politiques à l'intérieur de ses frontières, sans être soumis à des pressions juridiques extérieures. En matière de relations internationales, Falk avance que l'État souverain est caractérisé par son indépendance totale vis-à-vis de toute autorité supérieure, agissant avant tout dans l'intérêt de sa propre préservation et de ses objectifs nationaux. Voir : Falk, R. « Sovereignty. » *The Oxford Companion to Politics in the World*, edited by J. Krieger, 2nd ed., Oxford University Press, 2001.

[3] BAECHLER, Jean. Souveraineté et mondialisation. *Commentaire*, 2007, vol. 30, n°2, p. 353-362.

[4] ADONIS, Abid A. International law on cyber security in the age of digital sovereignty. *E-International Relations*, 2020, vol. 14, p. 1-5.

[5] BAECHLER, Jean. Souveraineté et mondialisation, o*p. cit.*

[6] KERR, Pauline. China's diplomacy: Towards ASEAN way norms in the South China Sea. *The Hague Journal of Diplomacy*, 2021, vol. 16, n°2-3, p. 224-252.

[7] La Digital Silk Road englobe une série de projets stratégiques visant à établir un contrôle numérique global tout en permettant à la Chine de dominer les nouvelles infrastructures numériques. Ces initiatives vont de la construction de data centers et de réseaux 5G, à l'exportation de technologies numériques, en passant par l'exportation de normes et de modèles de régulation.

[8] KARMAZIN, Aleš. China's Approach to Sovereignty: A General Overview. *Liquid Sovereignty: Post-Colonial Statehood of China and India in the New International Order*, 2023, p. 65-95.

[9] Standing Committee of the National People's Congress of China, *Cybersecurity Law of the People's Republic of China* (2016).

[10] Standing Committee of the National People's Congress of China, *Personal Information Protection Law of the People's Republic of China* (2021).

[11] ZHANG, Chunxiao. Imbalance in the institutional design of the Chinese data governance system. *Law, Ethics & Technology*, 2024, vol. 1, n°2, p. 19-20.

[12] Communist Party of China Central Committee, *Plan on building the rule of law in China (*法治中国建设规划（*2020–2025*年*)*), 2021, jan.10.

[13] State Council of the People's Republic of China. *Xi stresses sticking to socialist rule of law with Chinese characteristics*, 17 Nov. 2020, State Council of the People's Republic of China,

[14] 法治 (fazhì).

[15] CABESTAN, Jean-Pierre. Chine : un État de lois sans État de droit. *Revue tiers monde*, 1996, p. 649-668.

[16] United Nations. *Report of the Secretary-General on the restoration of the rule of law and administration of justice in post-conflict societies*, A/59/3, 2004

[17] 国特色社会主义法治 (Zhōngguó tèsè shèhuì zhǔyì fǎzhì), DELURY, John. "'Rule of Law' or 'Rule by Law'? In China, a Preposition Makes All the Difference." *The Wall Street Journal*, 17 Nov. 2021.

[18] Jean-Pierre Cabestan, dans son article « Chine: un État de lois sans État de droit », considère que « l'état de droit n'est pas une réalité statique mais plutôt un processus dynamique, un idéal vers lequel une société tend. »

[19] The State Council of the People's Republic of China, "国务院关于积极推进"互联网+"行动的指导意见" (Guiding Opinions of the State Council on Actively Promoting the « Internet + » Action, Year 2015 – 40 years old), 2015年07月04日.

[20] *Ibid.* Article 2 "二、推动信息技术产业跨越发展，拓展网络经济新空间" (Promouvoir le développement rapide de l'industrie des technologies de l'information et ouvrir de nouveaux domaines pour l'économie de réseau).

[21] KELSEN, Hans. General Theory of Law and State (Théorie générale du droit et de l'État), 1945, p. 110-115.

[22] WANG, Howard. 'Security is a prerequisite for development': consensus-building toward a new top priority in the Chinese Communist Party. *Journal of Contemporary China*, 2023, vol. 32, n°142, p. 525-539.

[23] Standing Committee of the National People's Congress of China, *Constitution of the People's Republic of China* (1982, amended 2018).

[24] *Ibid.* Art. 5.

[25] KARMAZIN, Aleš. China's Approach to Sovereignty: A General Overview, *op. cit.*

[26] C'est par exemple le cas du Règlement européen de 2016 sur la protection des données personnelles.

[27] HE, Lifeng. "Report on the Development of the Digital Economy", presented at the 37th meeting of the Standing Committee of the 13th National People's Congress, National Development and Reform Commission, October 28, 2022.

[28] Xinhua, "Jointly Build a Community with a Shared Future in Cyberspace," *China Daily*, November 7, 2022, https://www.chinadaily.com.cn/a/202211/07/WS63687246a3105ca1f2274748.html (Consulté le 22 juillet 2024).

[29] *Ibid.*

[30] Standing Committee of the National People's Congress of China, *Cybersecurity Law of the People's Republic of China, op. cit.*

[31] GABAUDE, Jean-Marc. L'État au XXe siècle. Regards sur la pensée juridique et politique du monde occidental. Études réunies par Simone Goyard-Fabre. *Revue Philosophique de Louvain*, 2006, vol. 104, n°3, p. 647-649.

[32] BLANQUER, Jean-Michel et MILET, Marc. *L'invention de l'état: Léon Duguit, Maurice Hauriou et la naissance du droit public moderne*. Odile Jacob, 2015.

[33] HEUSCHLING, Luc. De la démocratie et de l'État de droit, une étude théorique. *Of democracy and rule of law: a theoretical study »], in Etat de droit, Rechtsstaat, Rule of Law, Paris, Dalloz, Col. Nouvelle Bibliotheque de Theses*, 2002, p. 573-608.

[34] *Ibid.*

[35] LIU, Jinhe. China's data localization. In: *China's Globalizing Internet*. Routledge, 2022. p. 83-102.

[36] Standing Committee of the National People's Congress of China, *Personal Information Protection Law of the People's Republic of China*, *op. cit.* Art 54.

[37] CALZADA, Igor. Citizens' data privacy in China: The state of the art of the personal information protection law (PIPL). *Smart Cities*, 2022, vol. 5, no 3, p. 1129-1150.

[38] Standing Committee of the National People's Congress of China, *Cybersecurity Law of the People's Republic of China, op. cit. Art. 66.*

[39] *Ibid.* Art. 49.

[40] *Ibid.* Art. 40.

[41] Standing Committee of the National People's Congress of China, *Personal Information Protection Law of the People's Republic of China, op. cit*, Art. 53.

[42] CADELL, Cate. Amazon sells off China cloud assets as tough new rules bite. *Reuters. com*, 2017.

[43]CREEMERS, Rogier. « *El sistema de crédito social en China* ». Iberchina. Consulté le 28 juillet 2024. https://iberchina.org/index.php/polca-contenidos-34/1533-el-sistema-de-credito-social-en-china.

[44] LABRIE, Ryan C., STEINKE, Gerhard H., LI, Xiangmin, *et al.* Big data analytics sentiment: US-China reaction to data collection by business and government. *Technological Forecasting and Social Change*, 2018, vol. 130, p. 45-55.

[45] « Il y a aujourd'hui environ 600 000 abonnés WeChat en Australie, 1,3 million au Royaume-Uni et 1,5 million aux États-Unis » : HERMAN, Alex. "WeChat: China's Other Trojan Horse," *Forbes,* 2023.

[46] LI, Wan. Data Privacy and China's "Super App" WeChat. *Penn State Journal of Law & International Affairs*, 2024, vol. 12, n°1, p. 6.

[47] *Ibid.*

[48] CHASE, Steven. China demands proof that Canada's WeChat ban is justified. *The Globe and Mail web edition*, 2023.

[49] CRAMER, Benjamin W. Entity of the State: The Transparency of Restricting Telecommunications Firms as Threats to America's National Security. *Notre Dame J. on Emerging Tech.*, 2023, vol. 4, p. 56.

[50] Juridiction spécialisée, créée le 9 septembre 2018, pour traiter exclusivement les litiges liés à Internet et aux technologies numériques en Chine. Il fait partie d'une série de tribunaux internet lancés en Chine, les deux autres étant à Hangzhou (2017) et à Guangzhou (2018).

[51] Beijing Internet Court, "Huang Mou v. Tencent Technology (Shenzhen) Co., Ltd., Judgement of the First Instance of the Case between Huang and Tencent regarding the Internet Infringement Liability Dispute over Privacy Rights and Personal Information Interests", (2019) Jing 0491 Min Chu Zi, No°16142 (China).

[52] Tencent Micro-Insurance, *WeSure Privacy Policy*, "Article 6: How we share, transfer and publicly disclose information", point (6) : Service personnalisé : Afin d'améliorer nos services et optimiser nos

produits, nous vous fournirons des services personnalisés. Votre identifiant de connexion, votre parcours de navigation, votre mode de fonctionnement et d'autres informations sur la plateforme WeSure seront enregistrés. Nous désensibiliserons, dépersonnaliserons et rendrons anonymes les informations susmentionnées, puis les partagerons avec les organisations partenaires de WeSure et les parties liées (telles que Shenzhen Tencent Computer System Co., Ltd., Tenpay Payment Technology Co., Ltd., etc.) dans le but de vous fournir des services personnalisés, tels que des recommandations marketing et l'affichage d'informations. Si vous n'êtes pas d'accord, vous pouvez désactiver le bouton de service personnalisé dans « WeSure App – My Avatar – Privacy Management ». https://static.wesure.cn/app1/pdf-viewer/index.html?pdfKey=WESURE_PRIVATE (consulté le 02 août 2024).

[53] GRAVETT, Willem H. Digital neocolonialism: the Chinese surveillance state in Africa. *African Journal of International and Comparative Law*, 2022, vol. 30, n°1, p. 39-58.

[54] MEHTA, Raj Shekhar. China's Techno-Politics: The Impact on Belt and Road Partners. *India Quarterly*, 2023, vol. 79, n°3, p. 336-355.

[55] Yarden, Daniel. *Huawei Technologies' Imprint in African Global Cities*. Bachelor thesis, Haute école de gestion de Genève, 2021.

[56] SCHNEIDER, Florian. China's digital nationalism. In: *The Routledge Handbook of Nationalism in East and Southeast Asia*. Routledge, 2023. p. 167-180.

[57] ZHANG, Angela Huyue. *High Wire: How China Regulates Big Tech and Governs Its Economy*. Oxford University Press, 2024.

[58] BLOUET, Alexis. Doing away with the rule of law?. *-115 Droit et Societe*, 2023, vol. 114, p. 361.

[59] WANG, Shucheng. *Law as an Instrument: Sources of Chinese Law for Authoritarian Legality*. Cambridge University Press, 2022.

[60] *Ibid.*

[61] FRAENKEL, Ernst et MEIERHENRICH, Jens. *The dual state: a contribution to the theory of dictatorship*. Oxford University Press, 2018.

[62] JOWELL, Jeffrey. The rule of law and its underlying values. *The changing constitution*, 2007, vol. 6, p. 5-23.

[63] DELMAS-MARTY, Mireille. Libertés et sûreté : les mutations de l'État de droit. *Revue de synthèse*, 2009, vol. 130, n° 3, p. 465-491.

[64] BOUTANG, Yann Moulier et SELIM, Monique. Fragments politiques et économiques de Chine. *Multitudes*, 2013, vol. 54, n°3, p. 105-109.

[65] CLARKE, Donald. Order and law in China. *U. Ill. L. Rev.*, 2022, p. 541.

[66] Standing Committee of the National People's Congress of China, *Constitution of the People's Republic of China*, *op. cit.* Art 1.

[67] BANGGUI Jin, "La Cour suprême de Chine", *op. cit.*

[68] LIN, Yan et GINSBURG, Tom. Constitutional interpretation in lawmaking: China's invisible constitutional enforcement mechanism. *The American Journal of Comparative Law*, 2015, vol. 63, n°2, p. 467-492.

[69] XIAONAN, Yang. Legislative Interpretations by the Standing Committee of the National People's Congress in China. *Hong Kong LJ*, 2008, vol. 38, p. 255.

[70] *Ibid.*

[71] YI-CHONG, Xu et WELLER, Patrick. The challenges of governing: The state council in China. *The China Journal*, 2016, vol. 76, n°1, p. 1-23.

[72] *Ibid.*

[73] BANGGUI Jin, "La Cour suprême de Chine", *op. cit.*

[74] *Ibid.*

[75] RENOUX, Thierry S. Le Conseil constitutionnel et le pouvoir judiciaire en France dans le modèle européen de contrôle de constitutionnalité des lois. *Revue internationale de droit comparé*, 1994, vol. 46, n°3, p. 891-899.

[76] XIAONAN, Yang. Legislative Interpretations by the Standing Committee of the National People's Congress in China, *op. cit.*

[77] MACHELON, Jean-Pierre. Parlementarisme absolu, État de droit relatif : À Propos Du Contrôle De La Constitutionnalité Des Lois En France Sous La Troisième République (Positions Et Controverses). *La Revue administrative*, 1995, vol. 48, n°288, p. 628-634.

[78] DELMAS-MARTY, Mireille. *Le Pluralisme ordonné, op. cit.*

[79] BÜRBAUMER, Benjamin et GODIN, Romaric. *Chine/États-Unis, le capitalisme contre la mondialisation*. La Découverte, 2024.

[80] BRADFORD, Anu. *Digital empires: The global battle to regulate technology*. Oxford University Press, 2023.

[81] ROLLAND, Nadège. L'Afrique dans la stratégie chinoise. *Revue Défense Nationale*, 2022, n°1, p. 98-103.

[82] CREEMERS, Rogier. The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy. *Journal of Contemporary China*, 2024, vol. 33, n°146, p. 173-188.

[83] Voir les développements ci-après à propos de l'OCS.

[84] ROLLAND, Nadège. L'Afrique dans la stratégie chinoise, *op. cit.*

[85] ZHANG, Angela Huyue. *High Wire: How China Regulates Big Tech and Governs Its Economy*, *op. cit*, p. 34.

[86] *Ibid.* p. 35

[87] *Ibid.* p. 10

[88] Ibid. p. 35

[89] *Ibid.* p. 53

[90] *Ibid.* p. 54

[91] *Ibid.* p. 272

[92] State Council of the People's Republic of China, *Action Plan on Connectivity of BRI Construction Standards (2018-2020)*, December, 26 2017.

[93] Standing Committee of the National People's Congress of China, *Personal Information Protection Law of the People's Republic of China*, *op. cit.*

[94] *Ibid*. Art. 2

[95] 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, abrogeant la directive 95/46/CE (Règlement général sur la protection des données), JO L 119 du 4 mai 2016, p. 1.

[96] *Ibid.* Art. 3 « La présente loi s'applique également lorsque l'une des circonstances suivantes est présente dans les activités de traitement, hors des frontières de la République populaire de Chine, de données à caractère personnel concernant des personnes physiques se trouvant à l'intérieur des frontières de la République populaire de Chine :

– Lorsque l'objectif est de fournir des produits ou des services à des personnes physiques à l'intérieur des frontières ;

– Lorsque l'analyse ou l'évaluation des activités de personnes physiques à l'intérieur des frontières l'analyse ou l'évaluation des activités de personnes physiques à l'intérieur des frontières ;

– Dans d'autres circonstances prévues par les lois ou les règlements administratifs. »

[97] MENDEZ, A., et ESTRADA, G. *État des lieux de la présence chinoise en Amérique latine et aux Caraïbes*. Note d'analyse. Observatoire stratégique de l'Amérique latine, CERI, Sciences Po, 2023.

[98] ATKINSON, Robert D. et CORY, Nigel. Cross-Border Data Policy: Opportunities and Challenges. *Consensus or Conflict? China and Globalization in the 21st Century*, 2021, p. 217-232.

[99] ROLLAND, Nadège. L'Afrique dans la stratégie chinoise*, op. cit.*

[100] SEAMAN, John. Normes et standards chinois, nouveau facteur de puissance ?. In : *Ramses 2019*. Institut français des relations internationales, 2018. p. 130-135.

[101] AGBEBI, Motolani. China's Digital Silk Road and Africa's technological future. 2022.

[102] ALT Advisory. *Mapping the Progress (and Delays) for Data Protection in Africa*. Data Protection Africa, 14 Nov. 2023, https://dataprotection.africa/data-protection-in-africa-progress/ (Consulté le 14 Juin 2024).

[103] *Ibid.* : En janvier 2024, 65 % des États africains bénéficient d'une loi sur la protection des données.

[104] KHAN, Muhammad Asghar, RABBANI, Ali Hadi, UL HUSSAIN, Zamir, *et al.* Effects of the China-Pakistan Economic Corridor (CPEC) on the Economies of China and Pakistan. *Bulletin of Business and Economics (BBE)*, 2023, vol. 12, n°4, p. 341-347.

[105] Ministry of Information Technology & Telecommunication. *Draft of The Personal Data Protection Bill*. Vol. 19523, 2023.

https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf. (Consulté le 14 juin 2024).

[106] *Ibid.* Art. 3 « Scope and applicability » p.11.

[107] *Ibid.* Chap. IV, Art. 15 (1) (a), p.18.

[108] *Ibid.* Chap. V, Art. 26, p.27.

[109] *bid.* Chap. V, Art. 29, p.28.

[110] *bid.* Chap. VIII, Art. 35, p.32.

[111] NAEEM, Waqasia, SHAZIA Noureen, et TAHIRA Munir. « News Media Discourse of Imran Khan's Arrest in May 2023: Discourse Historical Approach. » *PalArch's Journal of Archaeology of Egypt/Egyptology*, vol. 20, n°2, 2023, pp. 1736-1755.

[112] ARSHAD, Rabya. The crisis of democracy in Pakistan–The general elections of February 2024. *International Journal of Scientific Engineering and Science*, 2024, vol. 8, n°4, p. 6-14.

[113] European Union. *Digital Services Act (Regulation (EU) 2022/2065 on a Single Market for Digital Services)*. Official Journal of the European Union, L 277 (October 27, 2022), Art. 36.

[114]Pakistan Telecommunication (Re-organization) Act. (1996). *Chapter VIII, Article 54*. https://www.na.gov.pk/uploads/documents/1329727963_180.pdf (consulté le 18 juin 2024).

[115] Freedom House. *Freedom of the Press 2022: Pakistan – Country Report.* 2022.

[116] Islamabad High Court. (2017, November 28). *CM Pak Limited v. Pakistan Telecommunication Authority* (HCJD/C-121, No. 42). Islamabad Judicial Department.

[117] Aqeel, Mian. « SC Sets Aside IHC Order on Cellular Service Suspension: Supreme Court Says Mobile Phone Service Is Closed to Prevent Unpleasant Incidents, Terrorism. » *The Express Tribune*, 23 Apr. 2020, https://tribune.com.pk/story/2204770/1-sc-sets-aside-ihc-order-cellular.

[118] LI, Guanying. Internet censorship in China: A functioning digital panopticon. In : *Communications in Contemporary China*. Routledge, 2023. p. 11-26.

[119] AKDUMAN, Birol. From the Great Wall to the Great Firewall: A Historical Analysis of Surveillance. *Uluslararası Sosyal Bilimler Dergisi*, 2023, vol. 7, n°28, p. 442-469.

[120] CREEMERS, Rogier. Comment la Chine projette de devenir une cyber-puissance. Hérodote, 2020/2 n° 177-178, p. 297-311.

[121] ERIE, Matthew S. et STREINZ, Thomas. The Beijing effect: China's Digital Silk Road as transnational data governance. *NYUJ Int'l L. & Pol.*, 2021, vol. 54, p. 1.

[122] TRINH, Viet Dung. Vietnam's Securitisation of Cybersecurity Under the Influence of a Rising China. *Australian Journal of International Affairs*, 2024, p. 1-20.

[123] CAO, Ruixing et NOESSELT, Nele. Political Settlement and China's Overseas Operation: The Case of Ethiopia. *Foreign Policy Analysis*, 2024, vol. 20, n°3, p. 14.

[124] KHALIL, L. « Digital Authoritarianism, China and COVID. » *Lowy Institute*, 2 Nov. 2020.

[125] Standing Committee of the National People's Congress of China, *Personal Information Protection Law of the People's Republic of China, op. cit.,* Art. 24.

[126] MIAO, Yanliang, FEI, Xuan, SUN, Jingyi, *et al.* The Impact of the US-China Trade War on Chinese Firms' Investment. *International Economic Journal*, 2023, vol. 37, n°3, p. 485-510.

[127] BELLANGER, Pierre. *De la souveraineté numérique.* Le Débat, 2012/3 n° 170, p.149-159.

[128] Pierre Bellanger a proposé le terme « synétat » pour qualifier les nouvelles formes de coopération entre États pour partager leurs connaissances et informations, et pour sous-traiter des pans entiers de leurs missions respectives.

[129] KSHETRI, Nir. *Cybercrime and Cybersecurity in the Global South*. Springer, 2013.

[130] MUELLER, Milton. *Will the Internet Fragment?: Sovereignty, Globalization, and Cyberspace*. John Wiley & Sons, 2017.

[131] MAIZLAND, Lindsay et CHATZKY Andrew. « Huawei: China's Controversial Tech Giant. » *Council on Foreign Relations*, 6 Août 2020, dernière mise à jour Fev. 2023, https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant. (Consulté le 6 Dec. 2024).

[132] CAVE, Danielle, et al. *Mapping China's Technology Giants: AI and Surveillance*. Australian Strategic Policy Institute, Avril 2019.

[133] RUHANYA, Pedzisai, GUMBO, Bekezela, *et al.* Data Accessibility and Digital Democracy: Unpacking the Political Transformation Problem in Zimbabwe. In : *Political Communication in Sub-Saharan Africa, Volume I*. Palgrave Macmillan, Cham, 2024. p. 171-196.

[134] WIBISONO, Adhe Nuansa. « China's *Belt and Road Initiative* in Sri Lanka: Debt Diplomacy in Hambantota Port Investment. » *Mandala: Jurnal Ilmu Hubungan Internasional*, vol. 2, n°2, 2019.

[135] *Ibid.*

[136] AGBEBI, Motolani. China's Digital Silk Road and Africa's technological future*, op. cit.*

[137] *Ibid.*

[138] *Ibid.*

[139] LI, Yuan, KLEIMANN, Martin, et SCHMERER, Hans-Jörg. Estimating causal effects of BRI infrastructure projects based on the synthetic control method. *Asia Europe Journal*, 2021, vol. 19, n°Suppl 1, p. 103-129.

[140] DÉVOLUY, Michel. Éditorial—Rapport Draghi : innover sans avancer. 2024.

[141] YIGITCANLAR, Tan et KANKANAMGE, Nayomi. City as a Sensor for Platform Urbanism. In : *Urban Analytics with Social Media Data*. CRC Press, 2022. p. 357-388.

[142] WALTER, Moritz F. et TRAMPUSCH, Christine. Economic statecraft by design and by default: The political economy of the 5G-Huawei bans in the United States, United Kingdom and Germany. *Competition & Change*, 2024, vol. 28, n°5, p. 539-560.

[143] STARK, Hans. Une Allemagne déboussolée, en voie de reconstruction. *Commentaire*, 2023, n°2, p. 349-356.

[144] BLANDIN-OBERNESSER, Annie. « Le Principe de Neutralité Technologique. » *Le Droit de l'Union Européenne en Principes: Liber Amicorum en l'Honneur de Jean Raux*, Apogée, 2006, pp. 243-259.

[145] MILLWARD, James, et PETERSON Dahlia. *China's System of Oppression in Xinjiang: How it Developed and How to Curb It*. Brookings Institution, 2020, https://www.brookings.edu/wp-content/uploads/2020/09/FP_20200914_china_oppression_xinjiang_millward_peterson.pdf. (Consulté le 6 Décembre 2024).

[146] MAJEROWICZ, Esther et DE CARVALHO, Miguel Henriques. China's expansion into Brazilian digital surveillance markets. *The Information Society*, 2024, vol. 40, n°2, p. 168-185.

[147] MILLWARD, James, et PETERSON Dahlia. *China's System of Oppression in Xinjiang: How it Developed and How to Curb It, op. cit.*

[148] PETERSON, Dahlia. AI and the surveillance state. In: *Chinese Power and Artificial Intelligence*.

Routledge, 2022. p. 205-222.

[149] Standardization Administration of the People's Republic of China. *Main Points of National Standardization Work in 2020*, 2020 : https://www.gov.cn/zhengce/zhengceku/2020-03/24/5494968/files/cb56eedbcacf41bd98aa286511214ff0.pdf » \t « _new (Consulté le 24 Juin 2024).

[150] *Ibid.* Art. 78 : Assumer activement les responsabilités de mon pays en tant que membre permanent de l'ISO et de la CEI, fournir un soutien au président de la CEI pour qu'il puisse s'acquitter de ses fonctions, partager les pratiques chinoises et proposer des solutions chinoises dans la réforme de la gouvernance et l'amélioration des capacités de gouvernance des organisations internationales de normalisation.

[151] Standardization Administration of the People's Republic of China. *Main Points of National Standardization Work in 2020*, *op. cit.*

[152] *Ibid.*

[153] Central Committee of the Chinese Communist Party and the State Council. *Guidelines for the Construction of the National New Generation Artificial Intelligence Standard System*, August 09, 2020.

[154] *Ibid.* Art. 1 (2).

[155] *Ibid.*

[156] Center for Intelligence Research and Analysis (CIRA). *A New "Great Game?": China's Role in International Standards for Emerging Technologies.* NIST Final Report, August 2022.

[157] NEGRO, Gianluigi. China and the ITU: A History of Standards. *Global Governance: A Review of Multilateralism and International Organizations*, 2023, vol. 29, n°3, p. 367-391.

[158] Center for Intelligence Research and Analysis (CIRA). *A New "Great Game?": China's Role in International Standards for Emerging Technologies, op. cit.*

[159] TELEANU, Sorina. *The Geopolitics of Digital Standards: China's Role in Standards-Setting Organizations*. DiploFoundation/Geneva Internet Platform, 2021.

[160] International Telecommunication Union. *Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities, Internet of Things and Smart Cities and Communities – Definitions and Terminologies: Standardization Administration of China. Build the Bridge of Standards and Connect the 'One Belt One Road'* (Recommendation ITU-T Y.4600),

2022.

[161] "ISO/IEC 30141:2018 Internet of Things (IoT) — Reference Architecture," ISO, available here: https://www.iso.org/standard/65695.html (Consulté le 17 Juin 2024).

[162] "Plenary meeting in Shanghai resolutions," *ISO*, ISO/TC IEC JTC1/SC 35, 8 February 2019, https://www.open- std.org/JTC1/SC35/docs/SC35_N2973_Shanghai_SC_35_meeting_resolutions.pdf (Consulté le 16 Juin 2024).

[163] CAS Institute of Automation. *AI Interaction Team Participates in ISO/IEC JTC1/SC35 Plenary and Discusses Two Proposals for International Standards*, August, 02, 2019.

[164] CTIA. *Comments of CTIA in the Matter of Study on People's Republic of China Policies and Influence in the Development of International Standards for Emerging Technologies.* 6 Dec. 2021.

[165] TRIOLO, Peter, et al. « The Digital Silk Road: Expanding China's Digital Footprint. » *Eurasia Group*, vol. 8, 2020, pp. 1-13.

[166] GAO, Henry S. « Digital or Trade? The Contrasting Approaches of China and the US to Digital Trade. » *Journal of International Economic Law*, 2018.

[167] CARLSON, Brian G. L'Asie centrale et la rivalité entre grandes puissances. *Politique de sécurité : analyses du CSS*, 2023, n°327.

[168] *Ibid.*

[169] L'organisation initialement composée de la République du Kazakhstan, de la République populaire de Chine, de la République kirghize, de la Fédération de Russie, de la République du Tadjikistan et de la République d'Ouzbékistan compte aujourd'hui huit membres permanents : l'Inde, le Kazakhstan, la Chine, le Kirghizistan, la Russie, le Pakistan, le Tadjikistan et l'Ouzbékistan. Ces derniers, ainsi que l'Afghanistan, la Biélorussie, l'Iran et la Mongolie, détiennent également le statut d'observateurs. En outre, plusieurs pays, dont l'Azerbaïdjan, l'Arménie, le Cambodge, le Népal, la Turquie et le Sri Lanka, figurent parmi les partenaires de dialogue.

[170] ALEXEEVA, Olga V. et LASSERRE, Frédéric. Le sommet de l'Organisation de coopération de Shanghai à Samarcande, ou les conséquences de l'invasion de l'Ukraine sur l'Asie centrale. *Revue internationale et stratégique*, 2022, n°4, p. 17-27.