# INTERNATIONAL JOURNAL OF **DIGITAL AND DATA LAW**

# REVUE INTERNATIONALE DE DROIT **DES DONNÉES ET DU NUMÉRIQUE**

ISSN 2553-6893

IMODEV
LES ÉDITIONS

Vol. 8 - 2022

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

**Direction :**
**Irène Bouhadana & William Gilles**

ISSN : 2553-6893

**IMODEV**
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

*Les propos publiés dans cet article n'engagent que leur auteur.*

*The statements published in this article are the sole responsibility of the author.*

**Droits d'utilisation et de réutilisation**

Licence Creative Commons – Creative Commons License -

CC-**BY-NC-ND**

Attribution
Pas d'utilisation commerciale – Non Commercial
Pas de modification – No Derivatives

# À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

**Irène Bouhadana**, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiateure professionnelle agréée par le CNMA.

**William Gilles**, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

**IMODEV** est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

# ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

**Irène Bouhadana**, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

**William Gilles**, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

**IMODEV** is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

# LA SOUVERAINETÉ DE L'ÉTAT À L'ÈRE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION : UN BASCULEMENT ENTRE THÉORIE ET PRATIQUE

Par **Valentin Ulrich BIWOLE**, Chercheur au Centre d'Études et de Recherches Constitutionnelles, Administratives et Financières (CERCAF) de l'Université de Yaoundé II

---

À l'ère d'Internet, d'une part, la souveraineté nationale a été contestée dans une certaine mesure ; d'autre part, la théorie de la souveraineté nationale a également obtenu l'opportunité de continuer à se développer dans le processus de faire face au défi de la mondialisation. La cyber souveraineté est une extension de la souveraineté nationale dans le cyberespace. C'est-à-dire, le droit d'un pays de mener des activités dans le cyberespace de manière indépendante et sans ingérence d'autres pays, de gérer les affaires du cyberespace et de se défendre contre les cyberattaques. La cyber souveraineté est un concept subordonné de la souveraineté nationale. Le caractère relatif et international de la cyber souveraineté est plus évident au regard de la pratique. Mais la théorie pose le socle fondamental de l'indépendance de l'État. Il y'a donc là un déphasage entre la théorie et la pratique de la souveraineté à l'aune des technologies. Deux pans qui doivent être en accord car la cyber-souveraineté est le dernier développement et une partie importante de la souveraineté nationale. L'exercice et le maintien effectif de la souveraineté nationale à l'ère du cyber espace ne peuvent être séparés de la cyber-souveraineté. La cyber-souveraineté et la souveraineté nationale se complètent et se soutiennent mutuellement.

Tout au long de l'histoire de la civilisation mondiale, le sens de la souveraineté a changé et s'est enrichi au fil du temps. L'humanité a connu successivement la révolution agricole, la révolution industrielle et la révolution de l'information. Chaque révolution, agricole, technologique, industrielle a eu un impact énorme et profond sur la connotation et l'extension de la souveraineté nationale[1]. À l'ère agricole, l'espace des activités humaines est principalement concentré sur la terre, et l'objectif de la souveraineté est de défendre l'intégrité territoriale. À l'ère industrielle, l'espace pour les activités humaines s'est étendu de la

---

[1] F. CHALTIEL, *La souveraineté de l'État et l'Union Européenne, l'exemple français. Recherches sur la souveraineté de l'État membre*, LGDJ, 2000, p. 60.

terre à la mer et au ciel, et la portée de la souveraineté s'est également étendue. À l'ère de l'information, le cyberespace a été fortement intégré à l'espace réel des activités humaines et est devenu le domaine de domination des pays modernes[2], un nouveau domaine de gouvernance mondiale, et la cyber souveraineté en a émergé. Cependant, La souveraineté fait référence à l'attribut le plus important de l'État qui le distingue des autres groupes sociaux[3] : C'est le pouvoir suprême inhérent à celui-ci[4].

Les États souverains sont des acteurs clés dans la conduite des activités du cyberespace et le maintien de l'ordre du cyberespace. Le principe de l'égalité souveraine établi dans la Charte des Nations Unies[5] est la norme de base des relations internationales contemporaines, couvrant tous les domaines des échanges d'État à État, ses principes et son esprit sont également applicables au cyberespace. Dans la pratique, tous les pays étendent la souveraineté nationale au cyberespace, mais il existe encore des conceptions différentes et des méthodes spécifiques d'exercice de la souveraineté dans le cyberespace. Afin de promouvoir la gouvernance mondiale de l'Internet dans une direction plus juste et raisonnable et de construire une communauté de destin dans le cyberespace, la communauté internationale devrait adhérer au bien-être commun de l'humanité comme fondement. En plus, défendre le concept de cyber souveraineté, négocier sur un pied d'égalité, rechercher un terrain d'entente tout en réservant les différences en appliquant activement les règles fondamentales qui fortifient le principe de souveraineté.

Avec le développement rapide de la technologie, la nourriture, les vêtements, le logement et les transports des gens sont étroitement liés au réseau. La politique, l'économie, la culture et la diplomatie de l'État sont indissociables du réseau. Le processus de mondialisation s'accélère également avec le développement du réseau[6]. L'ère du numérique est inévitablement arrivée. D'après de ce qui précède il est important de se demander qu'au regard de la violence observer dans les relations cyber spatiales, quel est l'implémentation théorique de la cyber souveraineté ? Il est donc question dans ce travail de d'élucider le concept nouveau de cyber souveraineté afin de dénoter ses implications au regard du droit

---

[2] Par pays moderne nous désignons les grandes puissances puisqu'elles détiennent de moyens forts pour booster le développement technologique.

[3] F. PERIN, *Introduction au droit public : théorie générale de l'État*, Presses universitaires de Liège, 1971, p.305

[4] R. CARRÉ DE MALBERG, *Contribution à la théorie générale de l'État,* tome 1, Dalloz, 2004, pp.70-71.

[5] La Charte a été signée à San Francisco le 26 juin 1945, à la fin de la Conférence des Nations Unies pour l'Organisation internationale, et est entrée en vigueur le 24 octobre 1945. Le Statut de la Cour internationale de Justice fait partie intégrante de la Charte.

[6] J.R. BENIGER, « La révolution de contrôle : les origines technologiques et économiques de la société de l'information », *Harvard University Press*, Cambridge, MA, 1986, p. 25.

posé et de la pratique. Car l'ère du numérique est arrivée avec une variété de problèmes liés au réseau, dont l'un est le problème juridique lié à Internet, qui est divisé en deux aspects : d'une part, il s'agit de la réglementation juridique nationale dans le domaine de l'Internet. Les recherches sur ce domaine ont été relativement approfondies et un certain nombre de lois y relatives ont été introduites. Un autre aspect est la question de la souveraineté de l'État dans le cyberespace. L'émergence du cyberespace entraînera inévitablement le problème de la division des compétences dans ce domaine. En raison de la particularité du cyberespace, la division des compétences ici ne peut pas être aussi clairement définie que dans la souveraineté traditionnelle[7]. Par conséquent, les conflits de compétence dans le cyberespace sont inévitables. Ces conflits sont essentiellement des conflits entre la souveraineté de différents pays. Ces dernières années, les conflits de souveraineté nationale dans le cyberespace se sont intensifiés. Par exemple, en juillet 2010, la centrifugeuse de la centrale nucléaire iranienne a été attaquée par le virus « Stuxnet »[8], causant des pertes aux installations de la centrale nucléaire iranienne. Un autre exemple est l'exposition du plan américain Prism[9] en 2013, qui a provoqué un tollé dans le monde. L'émergence continue, de tels conflits ont amené la question de la souveraineté dans le cyberespace à recevoir de plus en plus d'attention. Pour résoudre efficacement la question de la souveraineté dans le cyberespace, il est particulièrement important de le comprendre (§ 1) et présenter ses implications juridiques (§ 2).

## § 1 – LA CONTEXTUALISATION DU CONCEPT DE CYBER SOUVERAINETÉ

La cyber souveraineté est une extension naturelle de la souveraineté nationale dans le cyberespace. Il s'agit du pouvoir suprême et de l'indépendance externe dont un pays jouit sur les installations du réseau, les entités du réseau, les comportements du réseau et les données et informations de réseau associées sur son territoire sur la base de la souveraineté nationale.

### A) La justification de la naissance du concept de cyber souveraineté

Les grands changements en Europe de l'Est et la désintégration de l'Union soviétique ont marqué la fin de la guerre froide et des

[7] T. ZICK, « les États sont-ils souverains ? », *Journal of University Law Quarterly*, Washington, 2005, p. 77.

[8] Stuxnet est un virus espion découvert en juin 2010 qui s'est attaqué au nucléaire iranien.

[9] Prism est un programme de surveillance qui permet de collecter des informations sur internet en surveillant l'ensemble des communications à travers le monde. Tweets, post, photos, mails, vidéo ou encore fichier audio.

changements majeurs dans la structure internationale. Le principe de souveraineté, qui est la pierre angulaire de l'État tant sur le plan interne qu'externe, a également été fortement impacté. La souveraineté a connu une évolution et de nombreuses questions liées ont émergées avec plusieurs théories. Ainsi, l'on récence la théorie de l'interdépendance morale, la théorie de l'affaiblissement de la souveraineté, la théorie du transfert de souveraineté, la théorie des droits de l'homme sur la souveraineté, et d'autres de nouvelles pensées qui remettent en cause la souveraineté nationale[10]. L'émergence de ces nouveaux courants de pensée est indissociable de l'arrière-plan du modèle international et de la mondialisation auxquels nous sommes confrontés avec les technologies.

On ne peut nier que la mondialisation est la caractéristique première de l'ère des Technologies de l'Information et de la Communication. La mondialisation a eu un grand impact ou un impact sur les États souverains traditionnels. En effet, l'« économie sans frontières », les flux de capitaux ignorent les barrières frontalières, diluant ainsi la souveraineté territoriale traditionnelle . Il est devenu de plus en plus difficile de maintenir des intérêts économiques unilatéraux avec la souveraineté territoriale comme barrière. De plus, Le développement d'Internet a restreint la capacité d'un pays à exercer sa souveraineté car le pays ne peut plus contrôler la diffusion de l'information avec une autorité absolue et interférer avec les échanges internationaux. En raison du renforcement continu de l'interdépendance, le traitement de nombreux problèmes communs, tels que l'environnement, les maladies, les activités terroristes, ne relève plus de la souveraineté d'un pays et ne peut être entrepris par un seul pays. Il est nécessaire d'accroître l'autorité internationale. On observe aussi qu'à l'heure de la mondialisation que les perturbations sur le territoire d'un pays affectent souvent les pays voisins[11]. Par conséquent, les relations entre le gouvernement d'un pays, son peuple et la question de savoir s'il peut maintenir l'ordre public ne peuvent plus être considérés comme les affaires intérieures d'un pays, car aucun autre pays ne peut s'en mêler[12]. La technologie saisissant ces problèmes dans un univers cyber qui les catalyse a fait ressortir une crise de la souveraineté traditionnelle au profit de la cyber souveraineté.

En raison des caractéristiques de décentralisation, d'ouverture, d'internationalité, de fiction et d'infinité du cyberespace[13], la

---

[10] O. BEAUD, *La puissance de l'État,* PUF, 1994, coll. Léviathan, p. 41.

[11] S. TCHAMENI NGAMO, *Stratégies organisationnelles d'intégration des TIC dans l'enseignement secondaire au Cameroun : Étude d'écoles pionnières*, Thèse de doctorat, Université de Montréal, 2007, p. 214.

[12] *Ibidem*.

[13] L. HOUDE, *Internet et le paradigme juridictionnel*, mémoire de maîtrise en droit, Université de Montréal, 2002, p. 47.

théorie de la souveraineté territoriale à l'ère du cyber a été remise en cause dans une certaine mesure. D'abord, en raison de la nature illimitée du cyberespace, car elle ne peut pas être facilement divisé comme les limites géographiques, de sorte qu'il existe certaines difficultés à déterminer les limites de la juridiction nationale. Ensuite, l'exercice de la souveraineté économique nationale est soumis à certaines restrictions, telles que les difficultés de perception des tarifs nationaux en raison de la prévalence des « achats en ligne ». Enfin, la souveraineté culturelle de l'État est soumise à certains impacts, tels que les conflits culturels causés par le multiculturalisme en réseau[14].

C'est précisément en raison de l'existence de ces défis que certains chercheurs ont commencé à défendre la théorie de l'autonomie des réseaux et la disparition de la souveraineté. Par exemple, David Johnson et David Post estiment que la particularité d'Internet rend inefficace le contrôle de l'État sur Internet[15]. Le cyberespace est un espace autonome. Le cyberespace a besoin et peut créer ses propres lois et institutions juridiques, puis mener une gestion autonome[16]. Ils estiment également que la mondialisation économique, l'expansion rapide des sociétés multinationales, la désintégration de l'identité culturelle nationale et la perte de la juridiction nationale et de la souveraineté suprême sur les territoires nationaux ont amené la souveraineté à se fragiliser[17]. Alors que la relation entre les frontières géographiques et la portée des actions de l'État se rétrécit, les institutions étatiques souveraines qui ont dirigé l'arène politique et juridique internationale pendant plus de 500 ans seront elles-mêmes balayées dans le dépotoir de l'histoire[18]. La théorie de l'autonomie des réseaux et de la disparition de la souveraineté survalorise la particularité du cyberespace tout en ignorant le lien entre Internet et les États souverains. Cette proposition radicale est en contradiction avec la réalité.

En effet, Internet ne peut pas s'affranchir totalement du contrôle de la souveraineté, et la souveraineté ne s'éteindra pas du fait de l'existence de ces défis. D'une part, la souveraineté est l'attribut essentiel d'un État[19]. En même temps, la souveraineté est une catégorie historique, et elle continue à se développer avec les changements du temps. À l'ère du cyberespace, non seulement la souveraineté nationale ne s'éteindra pas en raison des défis du

---

[14] P.Y. GAUTIER, « De la prescription des infractions commises sur Internet…et dans le monde physique », *Recueil Dalloz*, n°23/7076 du 13 juin .2002, chron. p. 1852.

[15] J. DAVID, and D. « Post. Law and Borders: The Rise of Law in Cyberspace." *Stanford Law Review*, vol. 48, no. 5, 1996, pp. 1367–1402. JSTOR: www.jstor.org/stable/1229390. Accessed 25 July 2021.

[16] *Ibidem*.

[17] *Ibid.*

[18] T. MAYER, « Les frontières nationales comptent...mais de moins en moins », *Le lettre du CEPII*, n° 207, décembre 2001, p. 1

[19] P. BELLANGER, « De la souveraineté en général et de la souveraineté numérique en particulier », *Les Échos*, 30 août 2011 : archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm.

cyberespace, mais elle aura également des opportunités de développement ultérieur. D'un autre côté, objectivement parlant, le cyberespace est créé par des personnes, et ses propres caractéristiques déterminent qu'il aura inévitablement de nombreux problèmes juridiques, et la solution de ces problèmes nécessite l'intervention de l'État, et le développement durable et sain du cyberespace[20]. Les règles régissant l'espace traditionnel conduiront inévitablement à un résultat : l'extension objective de la souveraineté traditionnelle au cyberespace et la naissance du concept de cyber souveraineté.

### B) L'élucidation du concept de cyber souveraineté

Il est généralement admis que la cyber souveraineté est une extension de la souveraineté nationale dans le cyberespace, c'est-à-dire le droit d'un pays de mener des activités dans le cyberespace de manière indépendante et sans ingérence d'autres pays, de gérer les affaires y relatives et de se défendre contre les cyberattaques[21]. Le droit de gérer et de contrôler le flux transfrontalier d'informations dans le cyberespace, le droit de profiter de manière égale des ressources du cyberespace et le droit de prévenir et de combattre les cyberattaques.
Il ressort de la définition ci-dessus que la cyber-souveraineté comprend principalement quatre principes, à savoir le principe d'égalité, Le principe de justice, le principe de coopération et le principe de paix.

#### *1) Le principe d'égalité*

Le principe d'égalité souveraine proposé dans la Charte des Nations Unies est le principe premier que les pays devraient suivre dans l'exercice de la cyber souveraineté. Les pays souverains, grands ou petits, forts ou faibles, riches ou pauvres, sont égaux en droit, ont le droit de participer aux affaires internationales du cyberespace sur un pied d'égalité, ont également le droit d'être traités sur un pied d'égalité par les autres pays et sont davantage obligés de traiter les autres pays sur un pied d'égalité[22]. Ils ont le droit de participer à la gouvernance internationale du cyberespace sur un pied d'égalité et de formuler conjointement des règles internationales.

---

[20] Institut de la souveraineté numérique, « Les nouveaux enjeux européens de la souveraineté numérique »,
*Cahiers de la souveraineté numérique*, n° 1, 2015, p. 34 :
www.souverainetenumerique.fr/sites/default/files/Cahiersde-la-SouveraineteNumeriqueN1.pdf.
[21] B. BENHAMOU, « Les contresens de la souveraineté numérique », *Les Échos*, 29 janvier 2016 :
www.lesechos.fr/idees-debats/cercle/cercle-148468-le-contresens-de-la-souverainete-numerique-1196326.php.
[22] *Ibidem*

Cela fait également fait référence au droit de tous les pays de partager et d'utiliser les ressources du réseau sur un pied d'égalité. Par rapport aux autres médias traditionnels de diffusion de l'information, la principale caractéristique du réseau est qu'il peut atteindre un degré élevé de partage des ressources d'information à l'échelle mondiale[23]. Les ressources d'information sont les éléments essentiels de diverses ressources dans le cyberespace. Les ressources d'information sont différentes des ressources matérielles générales. Elles sont intangibles, rapides à transmettre et difficiles à contrôler. Il est irréaliste pour l'État de les posséder et de les contrôler exclusivement. En fait, les ressources d'information réalisent souvent leur valeur ou même créent plus de valeur nouvelle en raison du partage. De plus, comme certains chercheurs l'ont dit, Internet est essentiellement la richesse commune de toute l'humanité, et aucun pays n'a le droit de le posséder[24]. Par conséquent, en plus de la protection des informations secrètes d'État en raison de facteurs de sécurité nationale, il est difficile et ne devrait pas être exclusif à un certain pays pour les ressources d'information dans le cyberespace. Tous les pays devraient partager les ressources d'information dans le cyberespace sur un pied d'égalité.

### *2) Le principe de justice*

Les pays devraient défendre l'équité et la justice du cyberespace, et promouvoir le développement du système de gouvernance de l'Internet dans une direction juste et raisonnable, afin qu'il reflète les souhaits et les intérêts de la plupart des pays du monde, en particulier pour protéger les droits et intérêts légitimes des pays en développement et assurer le développement du cyberespace, contrôlé par les peuples de tous les pays[25]. Les pays ne devraient pas abuser de leurs propres avantages dans le domaine des réseaux d'installations, de technologies, de systèmes et de données, interférer dans l'exercice de la cyber souveraineté par d'autres pays ou poursuivre des comportements déloyaux tels que la cyber hégémonie et le cyber isolement.

Ainsi, Les pays souverains ont le droit de formuler des lois et des réglementations sur les installations de réseau, les sujets de réseau, les comportements de réseau et les données et informations de réseau connexes sur leur territoire afin de protéger la sécurité nationale, les intérêts publics sociaux et les droits et intérêts légitimes des citoyens, personnes morales et autres

---

[23] *Le Cyberespace, enjeu de souveraineté et de sécurité*, actes du 5e Forum international de la cybersécurité, 2013 : www.observatoire-fic.com/wp-content/uploads/2014/01/Actes-du-FIC2013.pdf.

[24] P. BOURE, *Le droit et Internet. Les enjeux présents et futurs de la société de l'information*, Guides Essentiels Droit sous la direction de : A. Chatty, Collection Doctrine, Textes et jurisprudence, 1re édition L'Hermès 2002, p. 8.

[25] *Ibidem*

organisations[26]. Afin de maintenir un bon ordre dans le cyberespace, un État souverain a le droit d'administrer les installations du réseau, les sujets du réseau, le comportement du réseau et les données et informations de réseau connexes sur son territoire conformément à la loi[27]. Les pays souverains ont le droit d'exercer une juridiction judiciaire sur les installations de réseau, les entités de réseau, les comportements de réseau et les données et informations de réseau connexes sur leur territoire conformément à la loi.

De même, les pays souverains ont le droit d'exercer une compétence personnelle nécessaire et raisonnable, une compétence de protection, sur la base des principes généralement reconnus du droit international, sur des comportements de réseau spécifiques qui ont des liens réels et suffisants entre les frontières de leur pays. Ainsi que sur les installations de réseau connexes à compétence universelle[28]. Afin de mettre en œuvre avec succès une telle juridiction, les États souverains peuvent demander l'aide des pays et régions concernés dans un esprit de retenue, de courtoisie et de réciprocité. Ce qui peut garantir la gestion par l'État de ses propres installations de réseau et de ses informations sur le réseau. Ce qui caractérise le contenu le plus fondamental de la souveraineté du réseau national et l'incarnation centrale du pouvoir interne le plus élevé de la souveraineté.

### 3) Principes de coopération

Le cyberespace est mondial et il est difficile pour un pays de parvenir à lui seul à une gouvernance efficace du cyberespace. Sur la base du principe de « coopération de bonne foi » prôné par la Charte des Nations Unies[29], les pays doivent respecter le statut des autres pays en tant que sujets de droit international, défendre les concepts de consultation étendue, de construction conjointe et de partage, adhérer à la participation multilatérale, la participation multipartite et la création multi-domaines, multi-niveaux et complète. Par-là, le système de gouvernance s'engage à maintenir la sécurité et le développement du cyberespace.

### 4) Le principe de paix

Le cyberespace est interconnecté et les intérêts de tous les pays sont profondément intégrés. Tous les pays doivent respecter les

---

[26] A. B. OBERNESSER, *Droits et Souveraineté numérique en Europe*, Bruylant, 2016, p. 83.

[27] *Ibidem.*

[28] Ak OURAL, « Gouvernance des politiques numériques dans les territoires », rapport à la secrétaire d'État en charge du Numérique, juillet 2015, pp. 20-21 : www.ladocumentationfrancaise.fr/var/storage/rapportspublics/154000509.pdf.

[29] L'article 2 (2) de la Charte des Nations Unies dispose : « Les Membres de l'Organisation, afin d'assurer à tous la jouissance des droits et avantages résultant de leur qualité de membre, doivent remplir de bonne foi les obligations qu'ils ont assumées aux termes de la présente Charte »

buts et principes de la Charte des Nations Unies, utiliser Internet de manière pacifique et résoudre les différends dans le cyberespace de manière pacifique. Les pays devraient prendre des mesures efficaces pour empêcher l'utilisation des technologies de l'information et de la communication pour s'engager dans des opérations qui perturbent la paix, empêcher une course aux armements dans le cyberespace, prévenir et combattre la cybercriminalité et le cyberterrorisme, et maintenir la paix et la sécurité du cyberespace[30].

Les pays devraient promouvoir l'état de droit dans la gouvernance internationale du cyberespace, maintenir conjointement l'autorité du droit international et s'opposer à deux poids deux mesures. Les pays devraient également améliorer leur législation nationale, exercer leur cyber souveraineté conformément à la loi, protéger en interne les droits légaux de leurs citoyens, personnes morales et autres organisations dans le cyberespace. En outre, ils doivent respecter la cyber souveraineté des autres pays à l'extérieur, se conformer aux règles et principes internationaux, et ne doivent pas utiliser Internet pour interférer dans les affaires internes d'autres pays ou s'engager dans des activités, tolérer ou soutenir des activités de réseau qui nuisent à la sécurité nationale et aux intérêts d'autres pays[31].

Il est donc soulignable qu'au regard théorique du droit international, et de la pratique féroce des activités dangereuse dans le cyberespace, les pays souverains ont le droit de choisir indépendamment la voie du développement des réseaux, des modèles de gouvernance et des politiques publiques sans aucune ingérence extérieure. Car, le droit à l'indépendance dans le cyberespace fait référence au droit d'un pays de s'assurer que son réseau et sa gestion sont indépendants et libres de toute ingérence d'autres pays. L'indépendance est le sens propre de la souveraineté, et un pays avec une souveraineté non indépendante ne peut pas être appelé un pays souverain[32]. La cyber souveraineté est un élément important de la souveraineté nationale, et l'indépendance du cyberespace est également une exigence inévitable de la cyber souveraineté. Plus précisément, le droit à l'indépendance dans le cyberespace fait référence au droit d'un pays de s'assurer que son réseau est indépendant et non contrôlé

---

[30] É. GEFFRAY « Le "Privacy Shield", exemple de la souveraineté européenne en matière numérique ? », *La Lettre de la DAJ* [Direction des affaires juridiques], lettre d'actualité des ministères économiques et financiers, nº 215, 8 septembre 2016 : www.economie.gouv.fr/files/files/directions_services/daj/publications/lettre-daj/2016/lettre215/PDF/edito.pdf.

[31] P. CLERC, « Souveraineté des données – "Innovation ouverte, cloud, big data : entrer dans la révolution numérique tout en gardant nos données souveraines est déterminant pour l'économie française" », interview, services.wiggam.com, 29 juin 2014 : services.wiggwam.com/interview-philippe-clerc-cci-Francesouverainetedes-donnees-cloud-big-data-revolution-numerique-engardant-nos-donnees-souveraines/.

[32] A.F. LELE, *Les agences de régulation au Cameroun*, Mémoire de Master en Administration publique des fonctionnaires internationaux à l'École Nationale d'Administration de Paris, Session 2002-2005, p. 69.

par d'autres pays, ainsi que le droit de gérer et de contrôler son réseau de manière indépendante et sans ingérence d'autres pays. C'est la manifestation de la souveraineté et de l'indépendance extérieure dans le cyberespace.
Les pays souverains ont le droit de développer leurs propres capacités de cybersécurité et ont le droit de prendre des mesures légales et raisonnables dans le cadre de la Charte des Nations Unies pour protéger leurs droits et intérêts légitimes dans le cyberespace contre les violations externes. Le droit de cyber-autodéfense fait référence au droit d'un pays de prendre les mesures de protection et de grève nécessaires pour se défendre, protéger son propre réseau des attaques ou empêcher que son propre réseau ne soit paralysé. Le droit à la cyber-autodéfense est le droit d'un pays à se protéger des cyberattaques en dehors du territoire. Ce droit n'exclut pas la possibilité d'une présence militaire d'un pays dans le cyberespace.

## § 2 – LES IMPLICATIONS JURIDIQUES DE LA CYBER SOUVERAINETÉ

Nous ne saurons finir ce travail de recherche sans évoquer les rapports entre la souveraineté traditionnelle et la cyber souveraineté, ce qui nous permettra de présenter l'éparsité des instruments juridiques relatifs à l'application de la souveraineté nationale dans le cyber espace et ses conséquences.

### A) Les rapports entre la cyber souveraineté et la souveraineté traditionnelle

La cyber souveraineté et la souveraineté traditionnelle sont à la fois différentes et liées. D'une part, les deux sont des concepts de niveaux différents, et cyber souveraineté a certaines caractéristiques que le contenu traditionnel de la souveraineté nationale n'a pas. D'un autre côté, la cyber souveraineté est un nouveau développement et une partie importante de la souveraineté nationale, alors les deux se complètent et se soutiennent mutuellement[33].
En ce qui concerne la différenciation, en premier lieu, le niveau conceptuel des deux est différent. Il faut dire que la cyber souveraineté est un concept subordonné de la souveraineté nationale. La cyber souveraineté a émergé avec l'avènement de l'ère du cyber, tout comme la souveraineté environnementale a émergé avec la gravité croissante des problèmes environnementaux internationaux. Ce sont tous des concepts proposés à une époque spécifique pour enrichir et améliorer encore la théorie de la souveraineté.
En second lieu, la relativité de la cyber souveraineté est plus évidente. La souveraineté nationale est conditionnelle de bout en

[33] P. TRUDEL, « Quel droit et quelle régulation dans le cyberespace ? », *Sociologie et sociétés*, vol 22, n° 2, automne 2000, p. 189.

bout. Même avec les partisans de la souveraineté absolue que prônent Bodin[34] et Hobbes[35], la souveraineté n'est pas absolue, du moins elle ne peut violer le droit naturel. Par conséquent, le contenu traditionnel de la souveraineté nationale se rattache à l'État. La souveraineté politique, souveraineté économique, souveraineté culturelle, souveraineté environnementale, etc., ont tous un certain degré de relativité[36]. Bien que le contenu traditionnel de la souveraineté nationale soit relatif, il a encore une certaine certitude dans le domaine de la compétence. Par exemple, la compétence territoriale peut être déterminée en fonction de la division des frontières géographiques. La « frontière » qui est à la base de la division de la souveraineté du réseau ne peut pas être aussi clairement visible que la frontière terrestre[37]. Par conséquent, dans le contexte de la souveraineté du réseau, la relativité du contenu traditionnel de la souveraineté nationale n'existe pas seulement, même ceux déterministes les facteurs du contenu traditionnel de la souveraineté nationale sont dans le réseau. La souveraineté a aussi une relativité forte, qui rend la relativité de la souveraineté du réseau plus évidente que le contenu traditionnel de la souveraineté.

Et en troisième lieu, la nature internationale de la cyber souveraineté est plus évidente. Ceci est déterminé par la nature globale du cyberespace. La souveraineté nationale elle-même a un caractère international, et sa souveraineté extérieure, à savoir le droit à l'indépendance, est elle-même une manifestation internationale de la souveraineté nationale[38]. La relativité de la souveraineté nationale est également déterminée par son internationalité, c'est-à-dire qu'un pays doit exercer sa souveraineté dans une certaine limite, et cette limite signifie ne pas s'ingérer dans la souveraineté des autres pays. Concernant le cyber souveraineté, puisque le cyberespace qui est à la base de sa génération a un caractère international très particulier, cela détermine que d'une part, l'exercice de la cyber souveraineté doit être limité à la non-ingérence dans d'autres pays ; avec un seul pays, et cela doit passer par la coopération internationale. Cela rend l'exercice et le maintien de la cyber souveraineté plus apparent à l'international.

---

[34] J. BODIN écrit que le souverain a la « puissance de donner et casser la loi à tous en général, et à chacun en particulier ». Les six livres de la République, livre I, p. 306.

[35] E. TUCHSCHERER, « Le Léviathan dans la doctrine de l'État de Thomas Hobbes : sens et échec du décisionnisme politique », *Astérion* [En ligne], n° 2, 2004, mis en ligne le 29 juin 2011, consulté le 4 août 2021 : http://journals.openedition.org/asterion/93 ; DOI : https://doi.org/10.4000/asterion.93.

[36] C. SCHMITT, *Le Léviathan dans la doctrine de Thomas Hobbes. Sens et échec d'un symbole politique*, trad. D. Trierweiler, Paris, Éditions du Seuil (coll. « L'ordre philosophique », 2002, p. 27

[37] Hent KALMO, « Une question de fait ? Les nombreux visages de la souveraineté », *souveraineté en fragments : le passé, le présent et l'avenir d'un concept contesté*, éd. Hent Kalmo et Quentin Qkinner, 2010. p. 114.

[38] C. SCHMITT, *Les trois types de pensée juridique*, trad. D. Séglard, Paris, PUF (coll. « Droit, éthique, société »), 1995, p. 81.

Pour ce qui du rapprochement entre les deux concepts, tout d'abord, la cyber souveraineté est le dernier développement et une partie importante de la souveraineté nationale. Comme mentionné précédemment, la souveraineté nationale est une catégorie historique qui a connu un développement et un changement continus. Lorsque l'histoire entrera dans l'ère du cyber, la théorie de la souveraineté nationale changera naturellement en conséquence. L'extension de la souveraineté nationale au domaine du cyberespace est devenue une tendance inévitable, et la souveraineté du cyber est naturellement devenue un nouveau développement de la souveraineté nationale à l'ère de la technologie. Elle est également devenue un élément important de la souveraineté nationale[39]. Dans le même temps, l'avènement de l'ère d'Internet a amené certains défis à la souveraineté nationale. Pour faire face à ces défis, la théorie de la souveraineté nationale subira inévitablement des ajustements correspondants. Le résultat de ces ajustements est que la théorie de la souveraineté nationale a été développé et son contenu est enrichi. Par conséquent, la cyber souveraineté peut être considérée comme le double résultat d'un développement actif et d'un ajustement passif de la souveraineté nationale. La forte vitalité internationale de la théorie de la souveraineté nationale fait que la cyber souveraineté devient inévitablement le résultat et une partie de son développement.

Ensuite, l'exercice effectif et le maintien de la souveraineté nationale à l'ère cybernétique ne peuvent être séparés de la cyber souveraineté. D'une part, la réalisation de la souveraineté politique, de la souveraineté économique, de la souveraineté culturelle et de la souveraineté environnementale d'un pays à l'ère du cyber ne peut se faire sans le cyberespace de manière objective. La souveraineté nationale est devenue indissociable du cyberespace. On peut dire que le réseau est devenu indispensable à la sauvegarde de la souveraineté nationale. En ce sens, la réalisation d'autres contenus de souveraineté nationale est indissociable de la cyber souveraineté. D'autre part, c'est précisément parce que la cyber souveraineté est une partie importante de la souveraineté nationale, et que la sauvegarde de la cyber souveraineté elle-même sauvegarde la souveraineté nationale. L'intégrité de la cyber souveraineté est devenue une partie et une avancée importante de la sauvegarde de l'intégrité de la souveraineté nationale. Par conséquent, pour exercer et maintenir efficacement l'intégrité de la souveraineté nationale à l'ère cybernétique, le contenu important de la cyber souveraineté ne peut pas manquer.

---

[39] P. CLERC, « Souveraineté des données – "Innovation ouverte, cloud, big data : entrer dans la révolution numérique tout en gardant nos données souveraines est déterminant pour l'économie française" », *op. cit.*, p. 6.

Enfin, la cyber souveraineté et la souveraineté nationale se complètent et se soutiennent mutuellement. D'une part, l'émergence de la souveraineté des réseaux est la promotion du développement des réseaux, et la seconde repose sur la théorie de la souveraineté nationale. Sans la théorie de la souveraineté nationale, la souveraineté des réseaux ne peut pas être discutée. D'autre part, la cyber souveraineté est propice au renforcement du statut de souveraineté nationale dans le droit international à l'ère du cyber. Comme mentionné ci-dessus, la souveraineté nationale a été contestée en raison de l'avènement de l'ère d'Internet, de sorte qu'il y a eu des points de vue sur la théorie de l'autonomie d'Internet[40] et la théorie de la disparition souveraine[41]. Certains chercheurs affirment même que la théorie de la souveraineté est dépassée et que l'avènement de l'ère d'Internet entraînera inévitablement la disparition du pays et la fin de la souveraineté[42]. Le point extrême de ce point de vue est qu'il ignore non seulement la persistance de la théorie de la souveraineté nationale, mais ignore également le lien objectif entre le cyberespace et la souveraineté nationale, et ignore la dépendance du développement sain du réseau sur la souveraineté nationale, et en même temps, le temps l'ignore. Le réseau peut être unifié avec la souveraineté nationale dans une certaine mesure. Par conséquent, la proposition de la cyber souveraineté est une preuve forte du lien objectif entre le cyberespace et la souveraineté nationale. La cyber souveraineté est une réfutation puissante de la théorie de la disparition de la souveraineté par contre elle subit juste des atteintes. La cyber souveraineté a un effet très positif sur le renforcement du statut de souveraineté nationale en droit international à l'ère du cyberespace.

### B) L'éparsité des instruments juridiques relatifs à l'application de la souveraineté nationale dans le cyber espace

De nombreux instruments internationaux importants ont confirmé que le principe de souveraineté nationale s'applique au cyberespace.

En 2003, la « Déclaration de principes de Genève »[43] adoptée par le Sommet mondial des Nations Unies sur la société de l'information a déclaré que « le pouvoir de décision des politiques publiques de l'Internet est la souveraineté de tous les pays »[44], l'« Agenda de la Tunisie » adopté par le sommet en 2005 met

---

[40] Le Cyberespace, enjeu de souveraineté et de sécurité, actes du 5e Forum international de la cybersécurité, 2013, *op. cit.*, p. 5.

[41] *Ibidem*

[42] A. B. OBERNESSER, *Droits et Souveraineté numérique en Europe*, Bruylant, 2016, *op. cit.*, p. 5.

[43] Déclaration de principes du Sommet mondial sur la société de l'information à Genève du 10 au 12 décembre 2003.

[44] *Ibidem*

l'accent sur le rôle clé des gouvernements dans le processus du sommet.

En 2011 et 2015, la Chine, la Russie et d'autres pays ont déclaré dans le « Code de conduite international pour la sécurité de l'information » que « réaffirmant que le pouvoir de décision sur les questions de politique publique liées à Internet est la souveraineté de chaque pays »[45].

En 2013 et 2015, le Groupe d'experts gouvernementaux des Nations Unies sur la sécurité de l'information a souligné dans son rapport que « la souveraineté nationale et les normes et principes internationaux dérivés de la souveraineté sont applicables aux activités TIC menées par le pays »[46]. Améliorer l'utilisation de l'information par le pays. Le fondement de la sécurité des technologies de la communication ».

En 2015, les dirigeants du G20 ont déclaré dans le « Communiqué du Sommet d'Antalya » : « Confirmez que le droit international, en particulier la Charte des Nations Unies, est applicable au comportement des États et à l'utilisation des technologies de l'information et de la communication, et ont promis que tous les pays devraient se conformer avec une confirmation supplémentaire d'un code de conduite national responsable volontaire et non contraignant dans l'utilisation des technologies de l'information et de la communication »[47].

En 2016, la « Déclaration de Goa »[48] des dirigeants du BRICS réaffirmait : « Sur la base des principes reconnus du droit international, dont la Charte des Nations Unies, à travers la coopération internationale et régionale, l'utilisation et le développement des technologies de l'information et de la communication. Ces principes comprennent l'indépendance politique, l'intégrité territoriale, l'égalité de la souveraineté nationale, le règlement des différends par des moyens pacifiques, la non-ingérence dans les affaires intérieures d'autres pays, le respect des droits de l'homme et des libertés fondamentales et de la vie privée, etc. Ceci est essentiel pour maintenir la paix, la sécurité et ouvrir le cyberespace ».

Les pays du monde entier exercent également leur cyber souveraineté par le biais d'activités législatives, administratives, judiciaires et autres. En défendant et en mettant en pratique le principe de la cyber-souveraineté, la Chine a proposé lors de la deuxième Conférence mondiale de l'Internet en 2015 que le respect de la cyber-souveraineté est un principe important pour faire avancer la réforme du système mondial de gouvernance de

---

[45] https://digitallibrary.un.org/record/710973/files/A_66_359-FR.pdf, consulté le 12 juin 2021.

[46] B. DELCOURT, « Le principe de souveraineté à l'épreuve des nouvelles formes d'administration internationale de territoires », *Pyramides*, n° 9, 2005, p. 95

[47] G. LONGUET, Rapport n° 7 (2019-2020) fait au nom de la commission d'enquête, déposé le 1er octobre 2019.

[48] La Déclaration de Goa est le fruit du 8e Sommet des BRICS, qui s'est tenu les 15 et 16 octobre dans l'État de Goa, dans l'Ouest de l'Inde.

l'Internet ; la loi sur la cybersécurité a été adoptée[49] dans ce pays alors qu'au Cameroun elle a été adoptée en 2010[50],ces textes existent pour rappeler que « Maintenir la souveraineté du cyberespace » est l'objectif fondamental de la législation sur le cyberespace. En outre, en 2016, la « Stratégie nationale de sécurité du cyberespace » a été publiée proposant que « la souveraineté nationale s'étend au cyberespace », et la souveraineté du cyberespace est une partie importante de la souveraineté traditionnelle. Ainsi elle a inscrit le principe de souveraineté comme l'un des principes de base de la coopération internationale dans le cyberespace, et a fait du « maintien de la souveraineté et de la sécurité » l'objectif stratégique principal de la participation à la coopération internationale dans le cyberespace.
Par ailleurs plusieurs autres pays vont dans le même sens, en effet, En termes d'exploration de la voie de développement et du modèle de gestion de réseau d'Internet, le Vietnam a introduit la loi sur la cybersécurité en 2018[51], qui définit clairement « le respect mutuel de l'indépendance, de la souveraineté, de l'intégrité territoriale, de la non-ingérence dans les affaires intérieures de chacun, de l'égalité et bénéfice mutuel » comme principes de base de la coopération en matière de cybersécurité, et les détails ont énuméré diverses interdictions d'Internet, notamment la distorsion de l'histoire, la atteinte à l'unité nationale et la violation des religions qui violent la souveraineté, les intérêts et la sécurité nationaux. En Afrique plusieurs textes[52] scellent le principe de souveraineté. L'Union européenne a proposé la « souveraineté technique » en février 2020 pour renforcer le contrôle et la domination de l'Union européenne sur la technologie, les règles et les valeurs du cyberespace.
En termes de protection du réseau du pays contre les menaces, les interférences, les attaques et le sabotage, la Russie a promulgué en mai 2019 le « Stable Runet Act » pour assurer l'autonomie et la fiabilité des ressources Internet russes. Dans le cas des serveurs étrangers, le fonctionnement normal du Le réseau russe peut toujours être garanti[53].

---

[49] La Chine a promulgué la loi sur la cybersécurité le 7 novembre 2016. La loi sur la cybersécurité est entrée en vigueur le 1er juin 2017.
[50] Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et la cybercriminalité au Cameroun.
[51]Adoptée en juin 2018, le 1er janvier 2019 est da date d'entrée en vigueur de la loi sur la cybersécurité au Vietnam.
[52] À titre d'exemple dans la CEMAC, il y a : la Directive n° 08/08/UEAC -133-CM-18 relative à l'interconnexion et à l'accès des réseaux et des services de Communications électroniques dans les pays membres, le règlement n° 21/08-UEAC -133-18 relatif à l'harmonisation des réglementations et des politiques de régulation des communications électroniques au sein des États membres de la CEMAC. Dans la CEDEAO nous pouvons citer Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.
[53] D. V. VINNIK, « Souveraineté numérique : régimes politiques et juridiques dans le raffinement des données », *Filosofiya Nauki*, numéro 2, 2014, pp. 95-113 (en russe).

En termes de protection des droits et des intérêts de ses citoyens dans le cyberespace, les États ont mis en œuvre des règlements sur la protection des données et le respect de la souveraineté, qui contrôlent strictement les flux transfrontaliers de données personnelles et étendent les frontières souveraines grâce à une compétence extraterritoriale sur le traitement des données personnelles.

### C) Les conséquences de la souveraineté nationale et de l'encadrement juridique de la cyber souveraineté

#### *1) le renforcement du rôle de État pour la protection de la souveraineté*

Que ce soit dans le monde physique ou dans le cyberespace, la souveraineté signifie l'unité des droits et des obligations. L'interconnexion et l'interdépendance des pays dans le cyberespace exigent que, tout en jouissant des droits découlant de la cyber souveraineté, les pays doivent respecter les principes de base et les règles générales du droit international et s'acquitter sérieusement de leurs obligations en vertu du droit international. De ce fait, les pays ne sont pas autorisés à entrer dans l'infrastructure réseau critique d'un autre pays ou les systèmes de réseau étroitement liés à la sécurité souveraine et aux intérêts de développement d'un autre pays sans autorisation, et ne doivent pas mener d'activités de surveillance de réseau, de vol ou de sabotage[54].

Aussi, Les pays ne doivent pas interférer avec les droits d'autres pays à survivre, à assurer la sécurité et le développement dans le cyberespace, et ne doivent pas interférer avec les droits d'autres pays à maintenir l'ordre, la sécurité et le développement de leur réseau[55]. Ce qui implique qu'ils ne doivent pas délibérément permettre que leurs territoires, ou installations de réseau, données de réseau et informations sous contrôle gouvernemental, soient utilisés pour des activités de réseau qui nuisent à la sécurité nationale et aux intérêts d'autres pays. Ils donc ont l'obligation de protéger les droits et intérêts légitimes des entités de réseau concernées relevant de leur juridiction, et ont également l'obligation de promouvoir l'ouverture et la liberté du cyberespace tout en garantissant l'ordre, la sécurité et le développement du cyberespace[56].

---

[54] P.-Y. GAUTIER, « De la prescription des infractions commises sur Internet…et dans le monde physique », *Recueil Dalloz*, 2002, chron. p.185

[55] *Ibidem*

[56] V. GAUTRAIS, « Sécurité juridique et sécurité technique : indépendance ou métissage », *Conférence organisée par le Programme international de coopération scientifique (CRDP / CECOJI)*, Montréal, 30 septembre 2003 ; p. 2.

Le principe de souveraineté nationale s'étend au cyberespace, et la cyber souveraineté est incarnée par des activités nationales dans les trois catégories d'installations et d'opérations de réseau, de données et d'informations de réseau, et de société et de personnes. Ainsi, l'État gère et utilise l'infrastructure du réseau national pour prendre en charge les applications, les données et les protocoles du système pour la diffusion de l'information[57], il maintient l'infrastructure du réseau national et la sécurité du système pour éviter les interférences ou les intrusions illégales et participe à la gouvernance, au développement de l'infrastructure et des systèmes de réseau profitez de la coopération internationale[58].

D'après ce qui précède, Le rôle joué par l'État pour la sauvegarde de sa souveraineté et le respect de la souveraineté des autres États est important, et dans car l'État protège, gère et guide la diffusion d'information en ligne nationale, restreint la diffusion d'informations qui portent atteinte aux droits légaux ou aux intérêts sociaux, il empêche les organisations étrangères de fabriquer, déformer ou diffuser des informations en ligne qui menacent la sécurité sociale dans le pays[59]. Relevons aussi, que la participation de l'État à la coordination et coopération internationales pour les flux transfrontaliers, la gouvernance de l'information et le développement de l'industrie de l'information de réseau et la protection des données et informations de réseau légitimes contre le vol ; ou détruit contribue à la bonne gouvernance du cyber espace, gage de la protection de la souveraineté traditionnelle.

La société et les personnes se réfèrent à l'environnement social et aux sujets sociaux qui interagissent avec le cyberespace. C'est pourquoi, l'État gère de manière autonome l'interaction de ses propres changements sociaux et de son cyberespace, cultive des entités de réseau et des environnements sociaux compatibles avec le développement du réseau ; maintient son propre système indépendant de gouvernance d'Internet et participe à part égale à la coopération internationale pour améliorer les modèles de gouvernance d'Internet et maintient, développe le cyberespace[60].

L'esprit de l'État de droit international empêche le populisme et l'isolationnisme d'entraver et de saper le développement de l'État de droit international dans le cyberespace.

Le respect de l'intégrité des activités de la cyber souveraineté est propice à la promotion d'une coopération ordonnée dans le

---

[57] *Ibidem*

[58] V. GAUTRAIS, « Sécurité juridique et sécurité technique : indépendance ou métissage », *Conférence organisée par le Programme international de coopération scientifique (CRDP / CECOJI)*, *op.cit.*, p.11

[59] S. GHERNAOUTI-HELIE, « La cybercriminalité. Le visible et l'invisible », *Presses polytechniques et universitaires romande*s, Collection Le savoir suisse, 2009, p.56

[60] M. GOUPY, « Peut-on encore parler d'état d'exception à l'heure des « sociétés de surveillance ? », *in* P.-A. Chardel (ed.), *Politiques sécuritaires et surveillance numérique*, Paris, CNRS, 2014, p. 85.

cyberespace, au maintien de l'harmonie et de la stabilité du cyberespace et à la promotion de la durabilité du cyberespace.

### 2) Vers une cyber souveraineté renforcée

À l'heure actuelle, le développement du cyberespace a posé d'énormes défis à la structure traditionnelle de gouvernance politique, économique et sociale. Cependant, le droit international du cyberespace et les réglementations pertinentes de divers pays ne sont pas encore complets et ne suffisent pas à répondre les besoins croissants de gouvernance du cyberespace. La proposition du principe de la cyber souveraineté clarifie davantage les droits et les intérêts de divers sujets, aide à réguler les comportements dans le cyberespace des gouvernements, des partis politiques, des organisations internationales, des secteurs privés, des groupes de recherche, des organisations sociales et des citoyens individuels, et promeut la souveraineté nationale égalité et avantage mutuel[61]. Une coopération internationale efficace sur la base de la non-agression joue un rôle important pour répondre efficacement aux divers défis de la cybersécurité et pour établir et maintenir un bon ordre dans le cyberespace.

Respecter la cyber souveraineté signifie respecter le droit des pays à choisir de manière indépendante la voie de développement et le modèle de gouvernance du cyberespace, et à participer de manière égale à la gouvernance internationale du cyberespace. Aucun pays ne devrait s'engager dans la cyber hégémonie, ne devrait pas utiliser Internet pour s'ingérer dans les affaires intérieures d'autres pays, ne devrait pas s'engager, tolérer ou soutenir des cyber activités qui mettent en danger la sécurité nationale d'autres pays et ne devrait pas empiéter sur l'infrastructure de l'information d'autres pays. Certains pays placent leurs propres intérêts au-dessus des intérêts d'autres pays et des intérêts communs de la communauté internationale, ne remplissent pas les obligations pertinentes en vertu du droit international, mettent en œuvre la juridiction au bras long, poursuivent l'unilatéralisme, érigent des barrières commerciales et portent atteinte aux droits et intérêts légitimes d'autres pays et la cyber souveraineté de la communauté internationale[62]. Les États doivent conjointement empêcher les boycotts et formuler des sanctions correspondantes.

L'essence de la cyber souveraineté réside dans le respect mutuel, l'égalité, l'ouverture et la tolérance de tous les pays. Défendre et pratiquer la cyber souveraineté ne signifie pas que les pays mendient leurs voisins dans le cyberespace. Il y aura inévitablement une diversité dans l'exercice de la souveraineté des pays dans le cyberespace, et cette diversité existera pour

---

[61] J GUISNEL, *Guerres dans le cyberespace : Services secrets et Internet*, La découverte, Paris, 2012, p. 5.

[62] E. HANNES et T. MAURER, « Revendications sur le cyberespace et puissances émergentes » *Hérodote*, vol. 52-153, no 1, 2014, p. 276.

longtemps[63]. Sur la base du respect de la souveraineté de tous les pays, comment équilibrer les droits et obligations souverains de tous les pays, partager les dividendes du développement de l'ère numérique et maintenir la paix et la stabilité dans le cyberespace sont de nouvelles propositions auxquelles la communauté internationale est confrontée.

L'espace construit par l'homme sur la base des technologies de l'information, le cyberespace a les caractéristiques de multidimensionnel, multi domaine et multi sujet. Il brise la frontière géographique traditionnelle et exerce une souveraineté fondée sur la compétence territoriale et complétée par les autres espaces. Le cyberespace a également subi un impact plus important. Par exemple, la connotation et l'extension du cyberespace sont toujours en pleine expansion. L'exercice des principes de souveraineté dans le cyberespace nécessite une adaptation constante aux nouvelles conditions et changements. Certains pouvoirs sont toujours en cours de transfert et d'ajustement entre les acteurs étatiques ou institutions non étatiques[64]. Face à l'ère numérique au potentiel énorme, le maintien efficace et l'exercice précis de la cyber souveraineté sont de nouvelles propositions auxquelles la communauté internationale est confrontée et nécessitent une exploration conjointe de toutes les parties dans la pratique.

Défendre et pratiquer la cyber souveraineté ne nie pas le rôle d'autres sujets que les gouvernements dans la gouvernance du cyberespace, ni l'interconnexion et l'interopérabilité du cyberespace, la libre circulation et l'innovation de l'information basée sur l'ordre nécessaire, ni ne le nie. Cela signifie fermer ou séparer le cyberespace, mais construire un ordre international juste et raisonnable dans le cyberespace sur la base de la souveraineté nationale, et construire conjointement une communauté de destin dans le cyberespace. Il serait donc souhaitable que tous les pays renforcent la communication, négocient sur un pied d'égalité, cherchent un terrain d'entente tout en réservant leurs divergences et coordonneront leurs positions dans le cadre des Nations Unies[65]. Sur la base de la sauvegarde de la souveraineté nationale du cyberespace, qu'ils élaborent un cyberespace universellement accepté avec les règles internationales et les codes de conduite nationaux, forger un large consensus, contribuer à la sagesse et construire ensemble un cyberespace pacifique, sûr, ouvert, coopératif et ordonné.

## CONCLUSION

---

[63] J. HUET, « Ordre public et loi de police et du for dans le droit international de la communication numérique », *RLDI* 2010, n° 2100, p. 25.

[64] M. HUMBERT, « Technologie et industrialisation face aux programmes d'ajustement structurel en Afrique », *Revue Tiers-Monde*, tome 31, n° 122, 1994, p. 245.

[65] H. ISAAC, « La donnée numérique, bien public ou instrument de profit », *Pouvoirs*, n° 160, numéro spécial, La *Datacratie*, pp. 75-86, janvier 2018, p. 51.

La cyber souveraineté est un nouveau développement de la souveraineté nationale à l'ère du cyber et un concept subordonné de la souveraineté nationale. Sa relativité et son internationalité sont plus évidentes. L'exercice effectif et le maintien de la souveraineté nationale à l'ère du cyberespace ne peuvent se passer de la cyber souveraineté. La cyber souveraineté est propice au renforcement du statut de souveraineté nationale en droit international à l'ère du cyber. Accorder toute son attention à l'importance de la souveraineté du réseau est important à la sauvegarde de l'intégrité de la souveraineté nationale.

## BIBLIOGRAPHIE

### Ouvrages

BEAUD O., *La puissance de l'État*, PUF, 1994, coll. Léviathan, p. 41

BELLANGER P., *La souveraineté numérique*, Paris, Stock, 2014, 264 p.

BENIGER J. R., *La révolution de contrôle : les origines technologiques et économiques de la société de l'information*, Harvard University Press, Cambridge, MA, 1986, p. 25

BODIN J., *Les six livres de la République*, livre I, p. 306

BOURE P., *Le droit et Internet. Les enjeux présents et futurs de la société de l'information*, Guides Essentiels Droit sous la direction de A. CHATTY, Collection Doctrine, Textes et jurisprudence, 1ère édition L'Hermès 2002, p. 8

CARRÉ DE MALBERG R., *Contribution à la théorie générale de l'État,* tome 1, Dalloz, 2004, pp. 70-71

GAUTIER P.-Y., « De la prescription des infractions commises sur Internet…et dans le monde physique » *Recueil Dalloz*, 2002, chron. p. 185

OBERNESSER A. B., *Droits et Souveraineté numérique en Europe*, Bruylant, 2016, p. 83

PERIN F., *Introduction au droit public : théorie générale de l'État, Presses universitaires de Liège*, 1971, p. 305

SCHMITT C., *Le Léviathan dans la doctrine de Thomas Hobbes. Sens et échec d'un symbole politique*, trad. D. TRIERWEILER, Paris, Éditions du Seuil (coll. « L'ordre philosophique », 2002, p. 27

SCHMITT C., Les trois types de pensée juridique, trad. D. Séglard, Paris, PUF (coll. « Droit, éthique, société »), 1995, p. 81

### Articles

BELLANGER P., « Souveraineté numérique et ordre public », *Archives de philosophie du droit*, tome 58, 2015, p. 287

DELCOURT B., « Le principe de souveraineté à l'épreuve des nouvelles formes d'administration internationale de territoires », *Pyramides*, n° 9, 2005, p. 95

GHERNAOUTI-HELIE S., « La cybercriminalité. Le visible et l'invisible », *Presses polytechniques et universitaires romandes, Collection Le savoir suisse*, 2009, p. 56

GUISNEL J., *Guerres dans le cyberespace : Services secrets et Internet*, La découverte, Paris, 2012, p. 5

GOUPY M., « Peut-on encore parler d'état d'exception à l'heure des « sociétés de surveillance ? », *in* P.-A. Chardel (ed.), *Politiques sécuritaires et surveillance numérique*, Paris, CNRS, 2014, p. 85

HANNES E., T. MAURER, « Revendications sur le cyberespace et puissances émergentes » *Hérodote*, vol. 52-153, n° 1, 2014, p. 276

HUET J., « Ordre public et loi de police et du for dans le droit international de la communication numérique », *RLDI,* 2010, n° 2100, p. 25

HUMBERT M., « Technologie et industrialisation face aux programmes d'ajustement structurel en Afrique », *Revue Tiers-Monde*, tome 31, n° 122, 1994, p. 245

ISAAC H., « La donnée numérique, bien public ou instrument de profit », *Pouvoirs*, n° 160, numéro spécial, La Datacratie, pp. 75-86, janvier 2018, p. 51

KALMO Hent, « Une question de fait ? Les nombreux visages de la souveraineté », *souveraineté en fragments : le passé, le présent et l'avenir d'un concept contesté*, éd. Hent Kalmo et Quentin Skinner, 2010, p. 114

MAYER T., « Les frontières nationales comptent...mais de moins en moins », *Le lettre du CEPII*, n° 207, décembre 2001, p. 1

TRUDEL P., « Quel droit et quelle régulation dans le cyberespace ? », *Sociologie et sociétés*, vol 22, n° 2, automne 2000, p. 189

VINNIK D. V., « Souveraineté numérique : régimes politiques et juridiques dans le raffinement des données », *Filosofiya Nauki*, numéro 2, 2014, pp. 95-113 (en russe)

ZICK T., « Les états sont-ils souverains ? », *journal of University Law Quarterly*, Washington, 2005, p.77.

## Thèse et mémoires

HOUDE L., *Internet et le paradigme juridictionnel*, mémoire de maîtrise en droit, Université de Montréal, 2002, p. 47

LELE A. F., *Les agences de régulation au Cameroun*, Mémoire de Master en Administration publique des fonctionnaires internationaux à l'Ecole Nationale d'Administration de Paris, Session 2002-2005, p. 69

TCHAMENI NGAMO S., *Stratégies organisationnelles d'intégration des TIC dans l'enseignement secondaire au Cameroun : Étude d'écoles pionnières*, Thèse de doctorat, Université de Montréal, 2007, p. 214

## Textes juridiques

Charte des Nations Unies de 1945

Déclaration de principes du Sommet mondial sur la société de l'information à Genève du 10 au 12 décembre 2003

Règlement n° 21/08-UEAC-133-18 relatif à l'harmonisation des réglementations et des politiques de régulation des communications électroniques au sein des États membres de la CEMAC

Loi du 1er juin 2017 portant sur la cybersécurité en Chine

Loi du 1er janvier 2019 portant sur sur la cybersécurité au Vietnam

Loi n° 2010/012 du 21 décembre 2010 relative à la cybersécurité et la cybercriminalité au Cameroun

Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO

Directive n° 08/08/UEAC -133-CM-18 relative à l'interconnexion et à l'accès des réseaux et des services de Communications électroniques dans les pays membres.

## Sitographie:

BENHAMOU B., « Les contresens de la souveraineté numérique », *Les Échos*, 29 janvier 2016 : www.lesechos.fr/idees-debats/cercle/cercle-148468-le-contresens-de-la-souverainete-numerique-1196326.php

CLERC P., « Souveraineté des données – "Innovation ouverte, cloud, big data : entrer dans la révolution numérique tout en gardant nos données souveraines est déterminant pour l'économie française" », *Interview*, services.wiggam.com, 29 juin 2014 : services.wiggwam.com/interview-philippe-clerc-cci-France souverainetedes-donnees-cloud-big-data-revolution-numerique-en-gardant-nos-donnees-souveraines/

CHALTIEL F., *La souveraineté de l'État et l'Union Européenne, l'exemple français. Recherches sur la souveraineté de l'État membre*, LGDJ, 2000, p. 60 : lesechos.fr/idees-debats/cercle/cercle-148468-le-contresens-de-la-souverainete-numerique-1196326.php

GEFFRAY É. « Le "Privacy Shield", exemple de la souveraineté européenne en matière numérique ? », *La Lettre de la DAJ [Direction des affaires juridiques]*, lettre d'actualité des ministères économiques et financiers, n° 2016 : www.economie.gouv.fr/files/files/directions_services/daj/publications/lettre-daj/2016/lettre215/PDF/edito.pdf

OURAL Ak, « Gouvernance des politiques numériques dans les territoires », *rapport à la secrétaire d'État en charge du Numérique*, juillet 2015, p. 20 : www.ladocumentationfrancaise.fr/var/storage/rapportspublics

TUCHSCHERER E., « Le Léviathan dans la doctrine de l'État de Thomas Hobbes : sens et échec du décisionnisme politique », *Astérion*, n° 2, 2004, mis en ligne le 29 juin 2011 : http://journals.openedition.org/asterion/93 ; DOI : https://doi.org/10.4000/asterion.93

## Rapport et conferences

GAUTRAIS V., « Sécurité juridique et sécurité technique : indépendance ou métissage », *Conférence organisée par le Programme*

*international de coopération scientifique (CRDP / CECOJI)*, Montréal, 30 septembre 2003, p. 2

LONGUET G., Rapport n° 7 (2019-2020) fait au nom de la commission d'enquête, déposé le 1er octobre 2019