Disiplinlerarası Afrika Çalışmaları Dergisi
Journal of Interdisciplinary African Studies
Haziran / June 2025, 3 (Özel Sayı): 59-71

Evolution Du Concept De Souveraineté Territoriale à L'ère Du Numérique

The evolution of the Concept of Territorial Sovereignty in the Digital age

Dr. Mamadou BALLOBALLO

Maître-Assistant à la Faculté de Droit Public (FDPu)
Université de Kurukanfuga de Bamako (UKB)
madouballo8@yahoo.fr
ORCID: 0009-0007-0239-3361

Makale Bilgisi / *Article Information*

Makale Türü / *Article Types*: Araştırma Makalesi / *Research Article*
Geliş Tarihi / *Received*: 17.02.2025
Kabul Tarihi / *Accepted*: 20.03.2025
Yayın Tarihi / *Published*: 06.06.2025
Yayın Sezonu / *Pub Date Season*: Haziran / *June*
Numéro spécial des Journées Scientifiques de la Science Politique au Mali (JSPM)
Cilt / *Volume*: 3 • **Sayı / *Issue*:** Özel Sayı-*Special Issue* • **Sayfa / *Pages*:** 59-71

Atıf / *Cite as*
BALLOBALLO, M. Evolution Du Concept De Souveraineté Territoriale à L'ère Du Numérique. Disiplinlerarası Afrika Çalışmaları Dergisi, 3/Özel Sayı (2025), 59-71

Doi: 10.5281/zenodo.15569428

İntihal / *Plagiarism*
Bu makale, en az iki hakem tarafından incelendi ve intihal içermediği teyit edildi.
This article has been reviewed by at least two referees and scanned via a plagiarism software.

Résumé: Le basculement du monde impulsé par le développement du numérique comporte certainement des enjeux pour les Etats et donc pour le droit international. Les mutations opérées par les TIC dans les rapports entre les Etats commandent le renouvellement de la réflexion sur le contenu de certains aspects de la souveraineté de l'Etat, en l'occurrence la souveraineté territoriale, à l'aune de la révolution numérique. Cette réflexion part de l'idée que le contenu du concept de souveraineté territoriale doit évoluer au regard du contexte actuel des relations internationales marquée par l'accélération constante du développement des technologies numériques. En effet, la dynamique internationale actuelle, marquée par un processus de déterritorialisation et de reterritorialisation, due, entre autres, à la numérisation des territoires, au développement des objets nomades, des moyens de géolocalisation stratégiques (comme le GPS), des banques de données, dépasse largement le cadre classique des atteintes à l'intégrité territoriale et à l'inviolabilité des frontières. La démarche

empruntée consiste, alors, à démontrer que le cyberespace fait partie intégrante du domaine de validité des compétences de l'Etat et qu'il apparait par conséquent nécessaire d'intégrer l'espace numérique dans la définition de la souveraineté territoriale.

Mots clés: Souveraineté, Territoire, Numérique, Etat, Agression

Abstract: The shift of the world due to the development of digital technology certainly poses challenges for States and therefore for international law. The changes brought about by ICT in relations between States call for renewed reflection on the content of certain aspects of State sovereignty, in this case territorial sovereignty, in the light of the digital revolution. This reflection starts from the idea that the content of the concept of territorial sovereignty must evolve in view of the current context of international relations marked by the constant acceleration of the development of digital technologies. Indeed, the current international dynamic, marked by a process of deterritorialization and reterritorialization, due, among other things, to the digitization of territories, the development of nomadic objects, strategic geolocation means (such as GPS), and data banks, goes far beyond the classic framework of attacks on territorial integrity and the inviolability of borders. The approach taken consists, then, of demonstrating that cyberspace is an integral part of the field of validity of the State's powers and that it therefore appears necessary to integrate digital space into the definition of territorial sovereignty.

Keywords: Sovereignty, Territory, Digital, State, Aggression

Introduction

Le basculement du monde impulsé par le développement du numérique comporte certainement des enjeux pour les Etats et, par voie de conséquence, pour le droit international. Les mutations opérées, par les Technologies de l'Information et de la Communication (TIC), dans les rapports entre les Etats commandent le renouvellement des réflexions sur le contenu de certaines dimensions de la souveraineté de l'Etat, en l'occurrence la souveraineté territoriale, à l'aune de la révolution numérique.

Du point de vue juridique, le territoire de l'Etat a fait l'objet de plusieurs tentatives de théorisation avec plus ou moins de fortunes. Il ne nous parait ni opportun, ni pertinent de rappeler ces théories territoriales d'une manière exhaustive dans le cadre de la présente réflexion. On pourrait tout au plus rappeler que le territoire fut d'abord considéré comme un objet et constituer à ce titre un bien réel. Il pouvait ainsi intégrer le patrimoine du souverain. Il a ensuite été théorisé dans une perspective sociologique comme un élément constitutif de l'Etat à l'image d'une personne physique. Toutes ces deux approches ont montré des insuffisances ayant conduit à leur abandon. La véritable remise en cause a été soutenue par Ernst Radnisky qui a fondé son analyse sur la structuration des éléments constitutifs de l'Etat en domaines de compétences matérielles, personnelles et spatiales. Cette approche, fondamentalement juridique, a été adoptée puis améliorée par l'auteur de la "théorie pure du droit" qui a substitué la no-

tion de "domaine de validité" à celle de domaine de compétences du pouvoir de l'Etat proposé par Radnisky. En outre, Hans Kelsen ajoute aux trois domaines précédemment distingués par Radnisky le domaine temporel qui se définit par la période pendant laquelle une norme juridique est valide. C'est-à-dire la durée pendant laquelle une norme est susceptible de produire des effets de droit. Le territoire est ainsi défini comme le domaine de validité spatiale de l'ordre juridique de l'Etat. Cette définition correspond à l'opinion majoritaire de la doctrine internationale et a par ailleurs fait l'objet de consécration par voie jurisprudentielle[1].

Partant de cette considération, il est possible de définir le concept de souveraineté territoriale comme le droit exclusif pour l'Etat d'exercer ses fonctions régaliennes sur le territoire qui lui est juridiquement reconnu et dont il dispose de droit. Il convient toutefois de distinguer la souveraineté territoriale de la suprématie territoriale qui confère à un Etat tiers le droit d'exercer certaines compétences sur un territoire sans en disposer souverainement. Cette distinction a été faite aussi bien par la doctrine que par la jurisprudence[2].

Quant à l'expression "l'ère du numérique", nous entendons le nouveau millénaire marqué par l'avènement des TIC et leur développement exponentiel qui a irrésistiblement impacté l'ensemble des domaines de la vie sociale et, partant, du système international. La souveraineté, qui est un des attributs essentiels des Etats, s'en trouve menacée dans plusieurs aspects. Toutefois, dans le cadre de la présente réflexion, nous nous intéresserons particulièrement aux enjeux liés à la protection de la souveraineté territoriale.

En réalité, l'essor actuel des sciences et technologies de l'information et de la communication semble prendre au dépourvu la conception classique de la protection de la souveraineté territoriale par l'introduction de nouvelles formes de menaces sur le territoire de l'Etat. La nature complexe et l'envergure de ces menaces justifient, à bien des égards, qu'on interroge la pertinence du contenu actuel de la protection de la souveraineté territoriale inspirée de la Charte des Nations Unies.

Pour mieux appréhender cette problématique, notre démarche consistera à analyser d'abord les limites du contenu actuel de la protection juridique de la souveraineté territoriale (I) nous aborderons ensuite la nécessité d'intégrer ses nouveaux enjeux (II).

Les limites de la protection juridique de la souveraineté territoriale

Par la notion de limite, nous entendons évoquer certaines insuffisances relatives à la protection de la souveraineté territoriale au regard de la Charte des

1 Sentence arbitrale de Max Huber, affaire de l'Ile de Palmas du 4 avril 1928, RSA vol. II, p. 839
2 CPJI, série A/B N°71, Affaire des phares en Crète et Samos 08 octobre 1937 p.103.

Nations Unies et des résolutions pertinentes du Conseil de sécurité et de l'Assemblée Générale. Ces insuffisances tiennent d'une part au caractère essentiellement étatique de l'approche qui fonde les règles de protection de la souveraineté territoriale (A) et, d'autre part, à son caractère essentiellement matériel (B).

Une approche essentiellement stato-centriste

Le respect de la souveraineté territoriale est une constance dans les relations entre nations jouissant d'une certaine reconnaissance réciproque en temps de paix. Toutefois, sa consécration universelle en droit conventionnel et/ou coutumier est relativement récente. En effet, l'interdiction de porter atteinte à la souveraineté territoriale ne s'est renforcée qu'à partir de la fin de la licéité des guerres de conquête territoriale avec notamment la multiplication des initiatives entreprises dans le sens de la pacification des relations internationales au regard des horreurs de la première guerre mondiale. Ce fut d'abord le Pacte de la SDN qui consacre le règlement pacifique des différends internationaux y compris ceux opposant un Etat membre à un Etat non membre. L'article 10 du Pacte protège expressément l'intégrité territoriale et l'indépendance politique des Etats membres contre toute agression extérieure. Dans la même dynamique, la signature du Pacte Briand-Kellog le 27 août 1928 marque un tournant dans le processus d'interdiction du recours à la force dans les relations internationales[3]. Quelles qu'aient été les fortunes du Pacte de Paris[4], il marque un pas important dans les initiatives contemporaines de mettre "hors la loi [5]» la guerre comme le "prolongement de la politique par d'autres moyens [6]». Il ne manquera pas aussi d'inspirer les rédacteurs de la Charte des Nations Unies, intervenue après l'hécatombe de la seconde guerre mondiale et qui fonde le système actuel de protection internationale de la souveraineté territoriale des Etats. La Charte consacre, entre autres, le principe du non recours à la force, le respect de l'intégrité territoriale ainsi que le principe du droit des peuples à disposer d'eux-mêmes. Ces principes protègent plus ou moins directement la souveraineté territoriale des Etats. Au plan communautaire, on peut citer entre autres, le décalogue d'Helsinki, l'Acte constitutif de l'UE, la Charte de l'OUA/UA, la Charte Africaine des Droits de l'Homme et des peuples.

Tous ces instruments internationaux consacrent avec plus ou moins de rigueur le respect de la souveraineté territoriale. Toutefois, Ils le font sous l'angle strict des rapports entre Etats. En effet, il ressort de l'interprétation cumulée de ces différents textes, et bien d'autres que nous saurons citer ici de manière

3 KAMTO Maurice, Extrait de l'ouvrage «l'agression en droit international», Editions A.Pedone, Paris, 2010, p.6 disponible en ligne sur https://pedone.info/kamto/L'agression-intro.pdf consulté le 9 septembre 2024.

4 En réalité, le caractère peu contraignant du Pacte de Paris le rapproche davantage d'une déclaration de philosophie que d'un véritable instrument juridique international. L'avènement de la deuxième guerre mondiale témoigne éloquemment en faveur de cette insuffisance.

5 Expression consacrée par la CIJ dans l'affaire de la Barcelona Traction du 5 février 1970.

6 Allusion à la théorie clausewitzienne de la guerre exposée dans son ouvrage intitulé "De la guerre".

exhaustive, que la violation de la souveraineté territoriale est constitutive d'un acte d'agression. En revanche, ni la Charte, ni les autres instruments sus cités ne proposent une définition d'un acte d'agression. Ainsi, parmi les différentes tentatives de définition de la notion d'agression constitutive d'une atteinte à la souveraineté territoriale, notamment sous l'influence de la diplomatie soviétique, on peut retenir celle adoptée par la résolution 3314 (XXIX) de l'Assemblée Générale de l'ONU en date du 14 décembre 1974. Au terme de cette résolution "L'agression est l'emploi de la force armée, par un État contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un autre État, ou de toute autre manière incompatible avec la Charte des Nations Unies, ainsi qu'il ressort de la présente Définition.». L'article 3 énumère quelques situations constitutives d'un acte d'agression. Il s'agit de "l'invasion ou l'attaque armée, l'occupation et l'annexion par la force; le bombardement ou l'utilisation d'armes contre le territoire; le blocus portuaire ou côtier; les attaques contre les forces armées ou la flotte marchande ou aérienne civile d'un État; les violations armées des accords sur le statut des forces; le fait de permettre à d'autres États d'utiliser son propre territoire pour perpétrer des actes d'agression, et l'envoi de bandes armées, de forces irrégulières ou de mercenaires pour commettre des actes d'agression". L'agression apparait ainsi comme une atteinte portée par un Etat à la souveraineté territoriale d'un autre Etat soit directement, soit par groupes armés interposé qui ne sont pris en compte que parce qu'ils agissent pour le compte d'un Etat et contre un autre Etat. La référence faite aux peuples dépendants qui doivent pouvoir «exercer pacifiquement et librement leur droit à l'indépendance complète, et l'intégrité de leur territoire national" par l'Assemblée Générale n'en constitue pas véritablement un argument contraire. En effet, "ces peuples" par ailleurs désignés sous le vocable de "territoires non autonomes" ne sont pris en compte que dans la mesure où leur destin normal est de devenir un Etat souverain notamment par l'exercice de leur droit à disposer d'eux-mêmes. Ils constituent donc des Etats en puissances (en devenir).

Cette conception stato-centriste de la définition de l'agression fragilise le système de protection internationale de la souveraineté des Etats en ce qu'il omet d'intégrer des acteurs comme les organisations internationales dont certaines (comme l'OTAN) existaient déjà. De même, les organisations terroristes internationales comme Al-Qaida et l'Organisation de l'Etat islamique (DAESH) qui peuvent nourrir des ambitions territoriales n'intègrent pas véritablement la catégorie des acteurs potentiels de l'acte d'agression. Toutefois, notre interrogation fondamentale concerne surtout l'apparition de nouveaux acteurs à la faveur du développement des TIC. En effet, les nouveaux outils de communication que constituent l'internet et les réseaux sociaux s'inscrivent davantage dans une logique de liberté individualiste qui transcende les frontières étatiques. Ces dernières années, les révélations d'Edward Snoden, de Julien Assange et bien d'autres encore, prouvent à suffisance, l'existence de groupes organisés ou de

loups solitaires qui n'obéissent nullement à un projet étatique et qui peuvent porter atteinte à la souveraineté territoriale des Etats et à la sécurité de leurs citoyens. Dans un tel cas de figure, l'acte d'agression serait difficilement imputable à un Etat. Car les auteurs ne sont pas et n'opèrent pas pour le compte d'un Etat y compris leurs Etats d'appartenance ou de résidence. Ce phénomène induit une mutation sémantique du concept d'agression ainsi que le régime de responsabilité internationale qu'elle implique[7].

De même, le développement des groupes paramilitaires qui peuvent appartenir à des personnes ou organisations privées (Hommes d'affaires, multinationales) peuvent porter des projets visant à nuire à l'indépendance politique et à la souveraineté territoriale des Etats alors même qu'ils ne constituent pas des acteurs entrant dans la définition actuelle de l'agression. Il apparait ainsi clairement que l'approche centrée sur l'Etat dans la définition de l'acte constitutif d'agression est insuffisante pour protéger l'intégrité territoriale. Une autre insuffisance concerne les considérations matérielles de l'approche.

Le caractère essentiellement matériel de l'approche

Si l'on s'en tient à la définition adoptée par la résolution 3314 de l'Assemblée Générale sur l'agression, elle repose sur une conception matérielle de la violation de la souveraineté territoriale. En effet, dans les différentes situations énumérées à l'article 3, les frontières de l'Etat victime de l'agression sont franchies par des forces armées d'un Etat ou des bandes armées agissant pour le compte d'un Etat. De même le blocus sur le port ou l'annexion d'une partie du territoire de l'Etat suppose la présence plus ou moins prolongée de forces armées. Enfin, les bombardements ou l'utilisation d'armes constituent des faits matériels qui portent atteinte à l'un des trois éléments constitutifs du territoire de l'État que sont la croute terrestre, les intérieures et a mers territoriales ainsi l'espace aérien surjacent. C'est ainsi par exemple que la présence des forces armées israéliennes au Liban constitue une violation de la souveraineté territoire de cet Etat[8]; Il en va de même pour les incursions militaires sud-africaines en Angola[9] ainsi que les bombardements portugais sur le territoire zambien[10].

En réalité, cette qualification essentiellement matérielle des actes constitutifs d'atteinte à l'intégrité territoriale des Etats opéré par le Conseil de sécurité ne permet pas de couvrir l'ensemble des situations de violation de la souveraineté territoriale des Etats. En effet, il n'est, de nos jours, nullement nécessaire de franchir les frontières d'un Etat pour porter atteinte à son intégrité territoriale.

7 PANCRACIO Jean Paul et PETON Emmanuel-Marie, Un mutant juridique: l'agression internationale, les Cahiers de l'IRSEM N°7, 2011.
8 Les résolutions 508 et 509 des 5 et 6 juin 1982 du Conseil de sécurité de l'ONU.
9 Voir la résolution 387 (1976) du 31 mars 1976 du Conseil de sécurité de l'ONU.
10 Voir la résolution 573 (1985) du 4 octobre 1985 du Conseil de sécurité de l'ONU.

Grace à l'accès ouvert et illimité aux réseaux mondiaux, il est devenu possible de conduire des attaques contre un Etat depuis son appartement ou un "bistro" à l'autre bout du monde. La complexité et l'envergure de certaines de ces attaques commandent bien qu'elles soient considérées comme des actes d'agression. C'est pourquoi l'idée selon laquelle les cyberattaques peuvent constituer des actes attentatoires à la souveraineté des Etats ou de recours à la menace ou l'emploi de la force[11], est de plus en plus admise par les gouvernements ainsi que les experts spécialistes des outils numériques. D'où l'idée de soumettre l'utilisation de certains outils informatiques par les Etats aux normes et principes du droit international[12]. Pourtant, ces attaques normalement constitutives d'actes d'agression peuvent bien être le fait d'un individu ou d'un groupe organisé pour le compte d'un autre Etat, d'une organisation internationale ou d'un réseau de criminalité transfrontalière. L'intervention militaire russe en territoire ukrainien, en cours depuis le 24 février 2022, permet de comprendre l'importance accrue des outils numériques dans la conduite des opérations militaires dans le contexte actuel des relations internationales. Ce qui explique par exemple que le gouvernement ukrainien ait lancé un appel mondial aux groupes de pirate pour aider son armée à protéger les infrastructures critiques de l'Etat. Ce recours de l'Etat aux particuliers pour l'aider à assurer une mission de souveraineté est en soi problématique tout comme les réseaux de pirate d'ailleurs. Mais ce qui nous intéresse davantage dans cette situation est l'extra-territorialité des attaques et des mesures de réponse. En effet, les attaques portées contre les infrastructures stratégiques ukrainiennes sont conduites depuis l'extérieur et ne se traduisent pas nécessairement par le franchissement des frontières territoriales avec des hommes et des armes. Elles sont conduites dans le cyberespace et peuvent provoquer la paralysie ou, à tout le moins, le dysfonctionnement des institutions de l'Etat. Elles peuvent aussi être combinées avec des opérations matérielles en vue de faciliter leur mise en œuvre ou de maximiser leur efficacité. Ils sont donc des armes stratégiques qui peuvent remettre en cause la souveraineté territoriale des Etats alors même qu'ils échappent au contrôle exclusif des Etats.

En juin 2024, plusieurs dizaines de délégations gouvernementales venues de tous les continents, se sont réunies au Conseil de sécurité pour échanger leurs vues et leurs expériences sur les nouveaux enjeux des outils numériques et leurs implications pour les Etats. Il ressort du rapport de cette rencontre de haut niveau que malgré les divergences persistantes entre les Etats sur la détermination de la responsabilité des Etats dans les opérations de cyberattaques, la tendance générale penche vers une certaine *opinio juris* vers le renforcement du cadre juridique international dans le cyberespace. Le progrès fulgurant enregistré ces dernières

11 Telle est la position officielle des Etats comme la France qui se réserve par conséquent le droit de recourir à la légitime défense contre certaines cyberattaques sur le fondement de l'article 51 de la Charte des Nations unies.

12 Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale", A/70/174, 22 juillet 2015, §§ 27-28.

décennies dans les domaines numériques, qu'il s'agisse de l'Intelligence Artificielle (IA) ou de l'Informatique quantique, ont opéré des changements majeurs dans les relations internationales si bien qu'il commande une mutation sémantique des concepts fondamentaux du cadre juridique national et international. Cette mutation est nécessaire pour la prise en charge des nouveaux enjeux de la souveraineté territoriale.

Les nouveaux enjeux de la souveraineté territoriale

De tout ce qui précède, il ressort que le concept de souveraineté territoriale doit intégrer les nouveaux enjeux liés au développement de la technologie numérique et ses implications sur les Etats et les populations. Ces enjeux sont certainement nombreux et multiformes. Dans le cadre de la présente réflexion, nous nous intéresserons d'une part à la protection des données à caractère personnel (A) et d'autre part à la notion de guerre numérique (B).

La protection des données à caractère personnel

Les données à caractère personnel peuvent être globalement définies comme des informations permettant d'identifier une personne vivante. Selon la définition retenue par l'Union Africaine, les données à caractère personnel sont "toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, psychologique, mentale, économique, culturelle et sociale [13]». Ainsi, les prénoms, les noms l'adresse personnelle, l'adresse du courriel, la localisation, une adresse de Protocole Internet (IP), données détenues par un hôpital ou un médecin ou un cookie constitue des données à caractère personnel. Ces informations constituent de nos jours un enjeu stratégique de première importance pour les Etats[14]. L'expansion continue de la démographie mondiale et le développement phénoménal des outils des TIC ont accéléré la croissance des données alors que les mesures de protection semblent de plus en plus obsolètes. A titre d'illustration, en 2023, Dell EMC a dévoilé les résultats de son troisième Global Data Protection Index. Le rapport met en évidence un taux de croissance exponentiel du volume des données dans le monde estimé à plus 569 %. L'un des enjeux majeurs de cette évolution consiste à contrôler la collecte et l'exploitation de ses données personnelles. Or, l'utilisation des données personnelles à des fins commerciales constitue un terreau favorable pour les entreprises technologiques internationales. Ceci explique l'urgence qui sied pour les Etats en développement en particulier les Etats africains de s'engager véritablement dans le processus de construction de leur

13 Voir la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel, p.5.

14 C'est le sens du paragraphe 11 du préambule de la Convention de l'Union Africaine sur la Cybersécurité et la protection des données à caractère personnel.

souveraineté numérique[15]. Malheureusement, l'hyper-dépendance économique et technologique de ces Etats aux puissances mondiales et/ou aux sociétés multinationales dans le domaine numérique, est de nature à compromettre toute affirmation de leur souveraineté numérique au niveau national. L'ampleur des enjeux liés à la protection des données à caractère personnel a inspiré aux Etats européens l'harmonisation des stratégies nationales ainsi la mise en place d'un cadre juridique et institutionnel communautaire face aux géants américains et asiatiques. Ainsi, en 2016, l'Union Européenne (UE) a élaboré le Règlement Général sur la Protection des Données ("RGPD") renforçant ainsi son corpus légal de protection des données personnelles. *A contrario* Les Etats africains peinent à adopter de stratégies similaires à l'échelle continentale. La Convention de Malabo sur la cybersécurité et la protection des données à caractère personnel signé le 27 juin 2014 a pris 9 ans pour recueillir les 15 ratifications nécessaires à son entrée en vigueur[16]. Au niveau régional, la CEDEAO a adopté depuis 2007 une série de mesures pour favoriser l'harmonisation des cadres juridiques et institutionnels relatifs à la sécurisation de l'espace numérique dans les Etats membres de l'Organisation. Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité de la CEDEAO[17]. Au plan national, le Mali a adopté en mai 2013 la Loi N°2013- 0 I 5 /DU 21 mai 2013 portant protection des données à caractère personnel en république du Mali qui a institué l'Autorité de Protection des Données à caractère Personnel[18] devenue opérationnelle en 2015. Toutes ces initiatives communautaires et nationales témoignent des enjeux liés à la gouvernance des données à caractère personnel pour les Etats. Le manque de moyens techniques, technologiques et d'expertises expliquent l'hyper-dépendance des Etats en développement aux multinationales occidentales et asiatiques. Les difficultés liées à l'harmonisation des systèmes nationaux de protection des données à caractère personnel peuvent être expliquées en partie par les divergences des conceptions de la gouvernance de l'Internet/des TIC. Certains mettent l'accent sur la dimension économique du numérique; ou encore sur les aspects relatifs à la promotion des droits de l'homme et des libertés individuelles ainsi que la

15 Par souveraineté numérique, nous entendons la capacité d'un État à agir dans l'espace numérique et de faire respecter leurs règles par les différents acteurs du monde virtuel.

16 L'article 36 de la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel dispose que "la Présente Convention entre en vigueur trente (30) jours après la réception, par le Président de la Commission de l'Union Africaine, du quinzième (15ème) instrument de ratification. Elle est ainsi entrée en vigueur le 08 juin 2023 après sa ratification par la Mauritanie qui a été devancé par le Togo, la Zambie, le Sénégal, le Rwanda, la Namibie, le Niger, l'Île Maurice, le Mozambique, la Guinée, le Ghana, la République Démocratique du Congo, le Cap-Vert, l'Angola et la Côte d'Ivoire

17 L'Acte additionnel A/SA 1/01/07 de la CEDEAO relatif à l'harmonisation des politiques et du cadre règlementaire du secteur des Technologies de l'Information et de la Communication (TIC) du 19 janvier 2007; l'Acte additionnel A/SA 1/01/10 de la CEDEAO relatif à la protection des données à caractère personnel dans l'espace CEDEAO; l'Acte additionnel A/SA 2/01/10 de la CEDEAO relatif aux transactions électronique dans l'espace CEDEAO; la «Directive C/DIR 1/08/11 de la CEDEAO sur la lutte contre la cybercriminalité au sein de l'espace de la CEDEAO» ainsi que la Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité de la CEDEAO.

18 Voir l'article 20 de la Loi N°2013- 0 I 5 /DU 21 mai 2013 portant protection des données à caractère personnel en république du Mali.

protection de la vie privée. D'autres enfin privilégient l'approche sécuritaire qui implique le contrôle du contenu du numérique, l'adoption et la mise en œuvre des politiques restrictives de libertés individuelles sur le fondement de la préservation de la sécurité nationale. Mais le plus grand handicap, quelle que soit l'approche choisie, demeure la dépendance numérique des Etats africains. Cette situation de dépendance témoigne de leur vulnérabilité dans un contexte international marqué par l'importance accrue des outils numériques dans les situations de conflits armés.

L'apparition du concept de "guerre numérique"

Selon le dictionnaire pratique du droit humanitaire "la guerre est un phénomène de violence collective organisée qui affecte les relations entre les sociétés humaines ou les relations de pouvoir à l'intérieur des sociétés [19]». Jusqu'à récemment cette forme de "violence organisée" se traduisait par des hommes, des armes et des stratégies militaires entre les sociétés en guerre. En droit international moderne, le recours à la force est en principe interdit dans les relations entre Etats. Il donne normalement droit à la légitime défense et engage la responsabilité de l'Etat auteur. Le développement des technologies de l'information et de la communication a bouleversé ce postulat classique. D'une part, les stratégies et matériels militaires modernes dépendent de plus en plus du numérique. D'autre part l'instrumentalisation des canaux d'information s'est considérablement développée avec la multiplication des plateformes numériques d'accès plus ou moins libre et facile. En 2018, Guillaume Marine distinguait trois formes de manifestation de conflictualité dans l'espace numérique. La guerre numérique qui vise à détruire les infrastructures critiques de l'adversaire; la guerre informationnelle qui consiste en la manipulation de l'information en vue de déstabiliser l'adversaire et la guerre hybride qui combine les moyens militaires et non militaires dans les stratégies de dissuasion nucléaire. L'intervention militaire russe en Ukraine a fourni l'illustration concrète de cette approche théorique qui paraissait plus proche d'une vision futuriste que de l'actualité. En effet, certains observateurs ont attribué à la Russie plusieurs cyberattaques auxiliaires sur les sites Web du gouvernement ukrainien. En outre les opérateurs d'infrastructures auraient tenté en vain de paralyser les centres de commandement et de contrôle de l'Ukraine. Même dans les opérations de l'armée de terre, l'intégration du numérique dans la conception et le développement des nouveaux équipements militaires connectés témoigne du basculement des conflits dans le cyberespace.

La guerre numérique est une forme de remise en cause de la souveraineté territoriale des Etats. Ce qui explique que les puissances mondiales adaptent leurs stratégies de défense à la nature de ces nouvelles menaces. Ces stratégies

19 Dictionnaire pratique du droit humanitaire, version numérique disponible sur www.dictionnaire-droit-humanitaire.org, consulté dernièrement le 28 décembre 2024.

intègrent désormais les concepts de cyberdéfense et de cybersécurité. On peut ainsi lire dans le Livre Blanc de la Défense Nationale du gouvernement français, "la croissance continue de la menace, l'importance sans cesse accrue des systèmes d'information dans la vie de nos société et l'évolution très rapide des technologies, imposent de franchir une étape supplémentaire pour conserver des capacités de protection et de défense adaptées à ces évolutions. Elles nous imposent aujourd'hui d'augmenter de manière très substantielle le niveau de sécurité et les moyens de défense de nos systèmes d'information, tant pour le maintien de notre souveraineté que pour la défense de notre économie et de l'emploi en France [20]». En effet, l'assimilation des cyberattaques d'une certaine envergure à des actes d'agression ou de recours à la force a pour conséquence l'exercice du droit à la légitime défense qui suppose la capacité de l'Etat agressé de riposter à l'attaque. Mais l'exercice d'un tel droit suppose la capacité d'identifier la source de l'attaque afin d'établir la responsabilité de l'Etat agresseur. Or, dans le domaine numérique, les Etats n'ont pas le monopole de la violence (cyberattaques). Les groupes privés (réseaux de hackeurs) ou des individus isolés (loups solitaires) parfois des mineurs, peuvent en être la source. Pour rappel déjà en 2010, le virus *Stuxnet* , une cyber arme créée la National Security Agency (NSA) en collaboration avec l'unité israélienne 8200, a été introduite dans les centrifugeuses iraniennes pour les rendre inopérantes. Malheureusement, la source véritable de cette attaque n'a pu alors être établie. De même, en début d'année 2024, un groupe d'ingénieurs maliens ont annoncé avoir réussi à récupérer les données biométriques de la population malienne, issues du Recensement Administratif à Vocation d'Etat Civil (RAVEC), alors bloquées par une société française dans un contexte de tensions diplomatiques entre le Mali et la France. Leur prouesse technique a été saluée et décorée par le gouvernement de la Transition au Mali. Toutefois, il expose l'Etat malien à une éventuelle cyberattaque de ladite société en réponse à cette récupération illégale des données. Bien d'autres exemples peuvent illustrer ce déséquilibre entre les Etats dans le domaine numérique que les spécialistes nomment "rupture technologique". Il peut être particulièrement rédhibitoire en matière de défense de la souveraineté territoriale.

Au demeurant, si la confrontation officielle des unités de bataille cybernétiques analogues aux unités de combats militaires, n'est pas encore une réalité avérée, elle demeure potentielle dans les futurs conflits entre Etats. C'est d'ailleurs cette perspective qui sous-tend la création et le financement des cyber-bataillons par certains Etats comme les Etats-Unis, la Chine, la Grande-Bretagne, l'Iran et la Syrie[21].

20 Voir Livre Blanc sur la Défense et Sécurité Nationale, Paris, La documentation française, 2013, p.105.

21 LUIGGI Jean-Sun, Cyberguerre, nouveau visage de la guerre? In Stratégiques, 2016/2 N°112 pp. 91-100 disponible en ligne sur www.shs.cairn.info. Consulté le 11 septembre 2024.

Conclusion

En conclusion, nous retenons que la dynamique impulsée par la révolution numérique dans les rapports entre les hommes et les sociétés ne laisse aucun domaine indifférent. La souveraineté qui constitue la caractéristique fondamentale de l'Etat n'échappe pas à cette réalité. Il n'est plus sérieusement contestable de nos jours de dire que la souveraineté, notamment dans sa dimension territoriale, peut désormais être remise en cause par le fait de groupes privés de divers ordres voire par des individus isolés. Les dimensions traditionnelles du territoire de l'Etat, que sont la croute terrestre, l'espace maritime et l'espace aérien, doivent être étendues à l'espace virtuel devenu le prolongement du territoire naturel et le nouveau champ de confrontation des acteurs publics et privés. Il apparait ainsi évident que le contenu de la souveraineté territoriale doit intégrer la dimension numérique. Cette mutation sémantique induit par la révolution numérique emporte deux conséquences essentielles sur le régime des actes d'agression. D'une part, les Etats ne constituent plus exclusivement les acteurs concernés par l'acte d'agression à la fois comme auteur et victime. D'autre part le régime de la responsabilité internationale inclue désormais une dimension pénale compte du rôle prépondérant pouvant être joué par les individus (personnes physiques et morales de droit privés) en matière d'agression internationale.

Les hésitations actuelles du Conseil de sécurité et de l'Assemblée Générale sur les évolutions conceptuelles induites par le développement du numérique reflètent les divergences entre les conceptions souverainistes et libérales au sein des membres permanents. La nature complexe et le caractère dynamique du cyberespace ainsi que la rupture technologique entre les Etats peuvent aussi constituer des obstacles à l'adoption d'une approche consensuelle internationale.

L'extension de la souveraineté territoriale au cyberespace implique que chaque Etat ait la capacité technique et technologique nécessaire à sa propre défense mais aussi de pouvoir riposter en terme de légitime défense en cas de cyberattaque constitutive d'actes d'agression ou de recours à la force. Pour les Etats africains cette souveraineté numérique devrait être recherchée dans une approche communautaire suffisamment intégrée et cohérente.

Références

Combacau J. Et Sur S. (2019). Droit international public, 15ème éd. Domat, Lgdj.

Perrin de Brichambaut, M., Dobelle, J.-F., & Coulée, F. (2011). *Leçons de droit international public* (2e éd., J. Dalloz, Éd.). Paris: Interforum.

Comité international de la Croix-Rouge. (n.d.). *Dictionnaire pratique du droit humanitaire* [version numérique]. Consulté le 28 décembre 2024 sur http://www.dictionnaire-droit-humanitaire.org

La documentation française. (2013). *Livre blanc sur la défense et la sécurité nationale* (p. 105). Paris: La Documentation française.

Kdhir, M. (2000). *Dictionnaire de la Cour internationale de Justice* (2e éd.). Bruxelles: Bruylant.

Kamto, M. (2010). *L'agression en droit international* (Extrait, p. 6). Paris: A. Pedone.

Luiggi, J.-S. (2016). Cyberguerre, nouveau visage de la guerre ? *Stratégiques*, (112/2), 91–100.

Pancracio, J.-P., & Peton, E.-M. (2011). Un mutant juridique: l'agression internationale. *Les Cahiers de l'IRSEM*, (7).

Textes internationaux et communautaires

Acte additionnel A/SA 1/01/07 de la CEDEAO relatif à l'harmonisation des politiques et du cadre règlementaire du secteur des Technologies de l'Information et de la Communication (TIC) du 19 janvier 2007

Acte additionnel A/SA 2/01/10 de la CEDEAO relatif aux transactions électronique dans l'espace CEDEAO

Charte de l'ONU

Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel du 27 juin 2014 à Malabo (Guinée Equatoriale)

Directive C/DIR 1/08/11 de la CEDEAO sur la lutte contre la cybercriminalité au sein de l'espace de la CEDEAO»

Résolutions 508 et 509 des 5 et 6 juin 1982 du Conseil de sécurité de l'ONU.

Résolution 387 (1976) du 31 mars 1976 du Conseil de sécurité de l'ONU.

Résolution 573 (1985) du 4 octobre 1985 du Conseil de sécurité de l'ONU.

Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité de la CEDEAO.

Jurisprudence

CPJI, série A/B N°71, Affaire des phares en Crète et Samos 08 octobre 1937 p.103.

CIJ dans l'affaire de la Barcelona Traction du 5 février 1970.

Sentence arbitrale de Max Huber, affaire de l'Ile de Palmas du 4 avril 1928, RSA vol. II, p. 839