PROGRAMME
AMÉRIQUE LATINE /
CARAÏBE

LE BRÉSIL, FUTURE CYBERPUISSANCE ?

PAR **Yannick HARREL** /

AUTEUR, CONFÉRENCIER ET CHERCHEUR EN ÉCOSYSTÈME CYBER ET MOBILITÉS 3.0

FÉVRIER 2021

ANALYSE #3

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

Dans le panel des cyberpuissances, les approches des États-Unis, de la Chine, du Royaume-Uni, de la France, d'Israël et de la Russie sont désormais mieux appréhendées au regard des textes officiels et des commentateurs des affaires du cyberespace. D'autres pays plus discrets dans ce milieu stratégique comme le Japon, la Corée du Sud, l'Italie ou l'Allemagne apparaissent moins exposés ou moins volontaristes, ce qui peut amener à des considérations erronées, voire fantasmées. Le Brésil est de ces États éloignés de la lumière des projecteurs médiatiques, lesquels s'emploient pourtant à maîtriser ce milieu stratégique afin d'en exploiter les avantages et mieux en contrer les inconvénients. La rédaction et publication récente d'une cyberstratégie nationale par le Cabinet de sécurité institutionnelle de la présidence brésilienne (Gabinete de Segurança Institucional da Presidência da República) est une étape sérieuse vers une meilleure coordination des ressources de l'État brésilien agrémentée d'un plan d'action pour renforcer ses points faibles et ainsi obtenir la reconnaissance du statut de cyberpuissance.

Pour déterminer quel est le degré de cyberpuissance d'une entité, l'on peut se référer à des outils et des méthodes élaborés par des instituts de recherche (le *Belfer Center* avec son « Cyber Readiness Index version 2.0 ») ou par des institutions internationales (l'Union internationale des télécommunications avec son « Global Cybersecurity Index »). L'on peut aussi se référer à l'adhésion d'un pays à des organes de décision tels que le « Group of Governmental Experts » des Nations unies.

Or si l'on se fonde sur le « National Cyber Power Index » du *Belfer Center*, prolongeant la méthodologie du « Cyber Readiness Index », le Brésil obtient une note de 10. Un score bien éloigné du premier de la classe, à savoir les États-Unis forts de leurs 50 points. Le plus grand pays d'Amérique du Sud est considéré comme une cyberpuissance aux moyens faibles et à la volonté réduite de peser sur ce milieu stratégique.

Le constat est cruel puisque le Brésil s'était doté en 2008 d'un document officiel reconnaissant le cyberespace comme milieu stratégique, tout à fait dans le tempo d'autres pays comme la France (qui l'a consacré dans son Livre blanc sur la défense et sécurité nationale de 2008). Mieux encore, en 1997, un CERT (*Computer Emergency Response Team* ou Équipe d'urgence en réponse informatique) a été créé afin d'alerter sur les cyberattaques pouvant endommager les infrastructures de télécommunication du pays. Le CERT ayant même été renforcé en 2006 par un CTIR (Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo ou Centre de traitement et de réponse aux incidents cybernétiques gouvernementaux). Et sur le plan militaire, un ComDCiber (Comando de Defesa Cibernética ou Commandement de cyberdéfense) placé sous le commandement de l'armée de l'air a été intronisé en 2016, soit seulement six ans après celui du grand frère américain du Nord. L'officialisation du CDCiber (Centro de Defesa Cibernética ou Centre

de défense cybernétique) date pour sa part de 2012 et il peut être considéré comme le bras armé technique du ComDciber.

Las, il semblerait que les moyens normatifs, techniques, financiers et humains ne soient pas en nombre suffisant pour peser si l'on en croit les différents graphiques du NCPI 2020. Malgré tout, il ne faudrait pas se méprendre et la situation cyber du Brésil pourrait bien évoluer singulièrement ces prochaines années en raison d'un regain d'ambition depuis 2020. Celle-ci s'est manifestée par la publication officielle, le 5 février 2020, d'une « Stratégie nationale de sécurité cybernétique » (Estratégia Nacional de Segurança Cibernética, abrégée en E-Ciber). En d'autres termes, une cyberstratégie nationale dont le programme s'étend sur quatre ans (2020-2024). À noter que celle-ci a fait l'objet d'une consultation préalable sur Internet le 10 septembre 2019, et ce pendant vingt jours, recueillant 170 propositions.

Rappelons préalablement les définitions du cyberespace, puis de la cyberstratégie. Le cyberespace est l'ensemble des systèmes d'information, de communication et de contrôle, civils et militaires, ainsi que des données y transitant. La cyberstratégie quant à elle est l'art de gouverner/commander/piloter par l'entremise d'actions efficaces au travers de systèmes d'information, de communication et de contrôle sur les plans civils et militaires. Comme il est précisé dans l'introduction, le texte réglementaire n'a pas pour vocation unique de combler les lacunes des précédents textes, mais est au contraire fort d'une vision plus large et plus roborative. Le pouvoir a ainsi pris bonne note que le cadre normatif n'était pas assez étoffé et solide, de même qu'il manquait singulièrement d'unité, nuisant à l'intérêt des remontées d'expériences des différentes unités consacrées à la lutte cybernétique.

Le plan d'action est rationalisé et confié à trois sous-groupes de travail : le premier chargé de l'aspect normatif et pédagogique ; le second dédié aux cybermenaces ; le troisième focalisé sur la protection des sites et infrastructures.

Il en ressort neuf thématiques traitées par la cyberstratégie brésilienne :

- Les axes de cybersécurité (*eixos de proteção e segurança*)
- La gouvernance de la cybersécurité (*governança da segurança cibernética nacional*)
- La prévention et l'atténuation des cybermenaces (*universo conectado e seguro: prevenção e mitigação de ameaças cibernéticas*)
- La protection stratégique (*proteção estratégica*)
- Les axes de transformation (*eixos Transformadores*)
- La dimension normative (*dimensão normativa*)
- L'aspect éducatif (*educação*)
- Les partenariats stratégiques internationaux (*dimensão internacional e parcerias estratégicas*)

- La recherche et le développement (*pesquisa, desenvolvimento e inovação*)

Les trois objectifs visés sont l'amélioration et la prospérité du Brésil dans l'espace numérique, la résilience du pays face aux cyberattaques et l'amélioration de sa reconnaissance internationale dans les problématiques du cyberespace.

Pour ce faire, les solutions envisagées sont relativement classiques, mais ont le mérite d'être éprouvées, comme l'application de normes internationales par les entreprises brésiliennes (il est évoqué le « *privacy* » et le « *security by design* » ou encore la norme ISO/IEC 17799 :2005) ou la délivrance de certifications de cybersécurité et de cybergouvernance (ce qui serait à terme le rôle du Gabinete de Segurança Institucional da Presidência da República, le Cabinet de la sécurité institutionnelle de la Présidence de la République, déjà mentionné). Une gouvernance centralisée en matière cyber est fortement préconisée (n'oublions pas que le Brésil est un État fédéral) afin de renforcer la coopération des différentes structures dans la cybersécurité nationale avec si possible l'utilisation d'une plateforme SOAR (*Security Orchestration Automation and Response*). Le gouvernement ne s'excluant aucunement des efforts à fournir et être exemplaire avec ses propres agences en relevant le niveau d'exigence. La formation est particulièrement privilégiée pour obtenir à terme de meilleurs spécialistes en intégrant le plus en amont possible le sujet de la cybersécurité dans les programmes éducatifs, et en aval, créer des filières valorisantes.

Point à relever : la cyberstratégie insiste sur l'emploi de procédés cryptographiques au sein des activités sociales pour tout ce qui concerne les sujets sensibles (« *estimular o uso de recursos criptográficos, no âmbito da sociedade em geral, para comunicação de assuntos considerados sensíveis* »). Ce point est notamment réitéré ultérieurement (« *incentivar o desenvolvimento de competências e de soluções em criptografia* »).

Le texte insiste aussi sur l'obligation pour le Brésil d'étendre ses échanges avec l'extérieur et d'améliorer par conséquent sa présence parmi les acteurs qui comptent dans le cyberespace, et de participer plus activement aux travaux internationaux sur sa régulation.

Comme pour certains textes stratégiques russes, il y a une similarité tant dans les objectifs que dans le ton du document : il ne faut y trouver nul satisfecit et certains aspects sont clairement décrits comme sérieusement (voire critiquement) insuffisants, à commencer par la formation de spécialistes cyber et le besoin de renforcer les coopérations stratégiques. La cyberstratégie se permet même d'être assez pointue lorsqu'elle évoque quelques éléments techniques (exemple de l'atteinte à la chaîne logistique, « *Um ataque à cadeia de suprimentos (Supply Chain Attack, em Inglês), ocorre quando há infiltração em um sistema por meio de um fornecedor, de uma empresa parceira ou de um provedor externo com acesso a sistemas e a dados* »).

Ce document officiel comble un réel manque en la matière puisqu'il existait bien des textes législatifs et réglementaires épars ainsi qu'un Livre vert sur la sécurité cybernétique officialisé en 2010 (Livro Verde de Segurança Cibernética no Brasil), mais sans approche stratégique appliquée. Désormais le pays est doté d'une cyberstratégie nationale, et si le cheminement vers une amélioration de son statut sera encore long, il est désormais balisé, assorti de conditions précises et d'objectifs rationnels qui lui offriront une place plus conforme à sa position de première puissance démographique et économique d'Amérique latine. C'est cette volonté de puissance qui permettra d'entendre la voix du Brésil dans le forum des États qui comptent dans le cyberespace.

Et à ce titre, la promulgation en août 2018 de la loi générale sur les données personnelles (Lei Geral de Proteção de Dados Pessoais), calquée sur le Règlement général de la protection des données en vigueur depuis mai 2018 sur le territoire de l'Union européenne, est une autre avancée majeure pour la reconnaissance du pays comme cyberpuissance.

D'autres étapes complémentaires à ce texte central sont tout à fait envisageables, comme par exemple la signature et la ratification de la Convention sur le cybercrime rédigé par le Conseil de l'Europe et agrégeant depuis novembre 2001 nombre d'États européens et extraeuropéens, dont l'Argentine depuis 2018 et le Pérou depuis 2019.

Car il y a dorénavant urgence à la matière puisque la société de cybersécurité brésilienne PSafe a alerté les autorités le 19 janvier 2021 quant à la survenance d'une colossale fuite de données administratives. Celle-ci est provenue de la captation d'un fichier gouvernemental critique, le Cadastro de Pessoas Físicas, dont la révélation pourrait affecter sur la durée la majorité de la population brésilienne au regard des informations contenues (personnelles, fiscales, sociales, entrepreneuriales, etc.).

Fort de cette cyberstratégie, le Brésil est en mesure d'appliquer sa propre devise à l'environnement cyber : de l'ordre et du progrès (*Ordem e Progresso*). ■

SOURCES

- Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, Anina Schwarzenbach, *National Cyber Power Index 2020*, Belfer Center, septembre 2020, https://www.belfercenter.org/publication/national-cyber-power-index-2020
- Secretaria-Geral da Presidência da República, Aprova a Estratégia Nacional de Segurança Cibernética, Diário Oficial da União, https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419
- Raphael Mandarino Junior, Claudia Canongia, Livro Verde de Segurança Cibernética no Brasil, Biblioteca de Segurança, 2010, https://www.bibliotecadeseguranca.com.br/es/livros/livro-verde-seguranca-cibernetica-no-brasil
- Presidência da República, Secretaria-Geral Subchefia para Assuntos Jurídicos, Lei Geral de Proteção de Dados Pessoais, 14 août 2018, http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm

ANALYSE #3

LE BRÉSIL, FUTURE CYBERPUISSANCE ?

PAR YANNICK HARREL / Auteur, conférencier et chercheur en écosystème cyber et mobilités 3.0.

FÉVRIER 2021

PROGRAMME AMÉRIQUE LATINE / CARAÏBE
Sous la direction de Christophe VENTURA, directeur de chercheur à l'IRIS
ventura@iris-france.org

*Cette collection d'articles s'inscrit dans le cadre du programme Amérique latine/Caraïbe de l'IRIS. Elle propose des contributions d'auteurs français ou internationaux dont les analyses éclairent les enjeux géopolitiques latino-américains. Le programme Amérique latine/Caraïbe de l'IRIS entend combiner différents niveaux de production d'analyses destinées à un public divers constitué de professionnels (entreprises, décideurs, journalistes, etc.), **d'**étudiants et de spécialistes de la région (chercheurs, universitaires, institutionnels). Il propose des décryptages de l'actualité géopolitique latino-américaine, des relations entre cette région et le reste du monde, ainsi que la publication d'études thématiques approfondies sur l'ensemble de ces sujets utiles à tous ces publics.*

INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES
2 bis rue Mercoeur
75011 PARIS / France

T. + 33 (0) 1 53 27 60 60
contact@iris-france.org
@InstitutIRIS
www.iris-france.org