

# Quelques éléments d'une géopolitique du Net…

Gaetan GORCE

Passé la ferveur utopiste et militante des fondateurs qui voyaient dans le Net le moyen de permettre à tous d'accéder à la connaissance sans le truchement des États, en enjambant les pouvoirs et les frontières, une autre réalité s'est peu à peu imposée.

Celle d'une formidable concentration économique tout d'abord, et de la constitution de monopoles puissants capables non seulement d'interdire l'accès au marché à toute concurrence potentielle, mais aussi de contrôler la majeure partie de la masse croissante de données circulant sur le Web.

Ce qui ne pouvait manquer de susciter l'intérêt des États tant du point de vue de leur sécurité que de leur indépendance stratégique.

Les États-Unis, s'ils durent partager avec les Européens (notamment au CERN[1]) l'esprit pionnier et d'invention qui fut à l'origine de la révolution numérique, furent les premiers à le comprendre.

Dès la fin des années 1980, sous l'impulsion du sénateur Al Gore, seront mis en place les outils juridiques et de financement qui allaient accompagner le formidable essor de l'industrie et des services numériques. Adopté en 1991, le Bill High Performance Computing Act débloquait déjà 1,7 milliard de dollars au service d'une politique offensive combinant avantages fiscaux et

(1) Organisation européenne pour la recherche nucléaire.

**Gaetan GORCE**

Gaetan Gorce est chercheur associé à l'INHESJ. Il a été membre de la Cnil (2011/2016) et Président de la mission d'information parlementaire sur la gouvernance d'Internet (2015).

commandes publiques. Pour parvenir à assurer cette hégémonie, ne sera négligé par Washington aucun des atouts stratégiques à sa disposition, y compris la monnaie, comme en témoignera la manière dont les États-Unis surent restaurer la suprématie d'IBM et surtout d'Intel en souffrance face à la concurrence japonaise sur le marché des microprocesseurs en contraignant Tokyo à une réévaluation du yen dans le cadre des accords du Plazza en 1985.

Leur suprématie est désormais solidement établie puisque sur les cinquante premières entreprises du secteur, trente-trois sont américaines et aucune européenne, créant une situation d'autant plus préoccupante que les avantages que les États-Unis tirent de cette hégémonie économique sont cumulables et extensibles aux autres domaines stratégiques.

Cette hégémonie s'étend d'abord à tous les étages du système : l'organisation du système de câblage qui permet l'interconnexion mondiale et la répartition (comme la propriété) des *Data-centers* sont telles qu'une très large part des données mondiales transite par une technologie américaine ; les systèmes d'exploitation de nos terminaux sont américains et orientent vers des prestations de services américaines (Google Amazon, Facebook, Apple et Microsoft) traitant ainsi 80 % des données mondiales.

La puissance qui en résulte est déstabilisatrice à plus d'un titre :

– d'abord à travers la force de frappe financière qu'elle confère aux GAFAM dont le chiffre d'affaires respectif, au moins pour deux d'entre eux, tangente le milliard et qui au regard des rendements croissants qu'ils obtiennent (l'essentiel du coût résidant dans l'investissement initial) deviennent de véritables machines à cash, diversifiant de manière foudroyante leur champ d'interventions (cf. la voiture connectée) et absorbant la concurrence émergente (si Facebook a pu racheter What'App pour 18 milliards de dollars, Google a, de son côté, ingéré 150 sociétés depuis sa création !) ;

– ensuite en leur permettant de défier la législation des États (à l'instar du refus de Google d'appliquer la directive sur les droits d'auteur) voire en privant ostensiblement ceux-ci des recettes fiscales que génère leur développement (le conseil du numérique entendu en 2013 par une mission du Sénat a estimé à 1,5 % le taux d'imposition des Gafam rapporté aux bénéfices dégagés par leur activité en France).

Cette position hyper-dominante produit enfin ses effets dans le champ hypersensible de la protection des personnes, de l'intelligence économique et de la cyber-sécurité.

La coopération étroite que l'affaire Snowden a clairement mise à jour entre les grands opérateurs du Net et les services du renseignement américain aboutit à des formes d'espionnage politique et commercial sans précédents.

L'interception s'opère à tous les niveaux.

Celui des infrastructures en se branchant directement sur les réseaux en particulier au point d'atterrissement des câbles de fibre optique (voire directement sur les 448 câbles sous-marins d'une longueur cumulée de 1,2 million de km transportant 99 % du trafic intercontinental).

Celui des réseaux en détournant (ou en profitant des failles, parfois volontairement introduites) des protocoles : le programme Génie de la NSA ne visait-il pas au développement d'implants dans des dizaines de milliers d'ordinateurs ? Par réquisition enfin dans le cadre de coopération officieuse avec les opérateurs (via PRISM) ou officielle via le récent *Cloud Act* qui permet aux autorités américaines d'exiger la communication de toutes les données stockées aux États-Unis ou sur des serveurs à l'étranger mais appartenant à des sociétés américaines !

Cette puissance suscite certes des résistances.

Aux États-Unis aussi comme en témoignent par exemple les enquêtes engagées contre les Gafam par une cinquantaine de procureurs ; ou en Europe.

Mais celle-ci ne dispose aujourd'hui que d'un seul véritable atout : l'avance qu'elle a prise dans le secteur juridique de la protection des données (avec la mise en œuvre l'an passé du règlement général sur la protection des données) susceptible de faire jurisprudence dans le monde occidental (mais qu'affaiblit la faiblesse des garanties obtenues dans le cadre des nouveaux accords régissant le transfert des données des citoyens européens aux États-Unis et ceci malgré la vigilance de la Cour de Justice de l'UE).

Absente des microprocesseurs, bousculée sur les logiciels, totalement dépassée sur les services, l'Europe n'existe encore industriellement que via les fournisseurs d'accès ou Nokia. Le combat qu'elle a engagé, au titre du droit fiscal et de la concurrence, gagnerait par conséquent à être doublé d'une politique active de la commande publique et en matière de *cloud* d'un soutien déterminé à la seule entreprise capable de rivaliser à savoir OvH. Mais les engagements pris à grand renfort de déclarations publiques au cœur des années 2000 sont restés lettre morte.

TOUS LES GRANDS PAYS SE SONT AINSI DOTÉS DE CAPACITÉ DE SURVEILLANCE TOURNANT VITE À L'ESPIONNAGE, VOIRE AUX TENTATIVES DÉLIBÉRÉES DE DÉSTABILISATION POLITIQUE OU ÉCONOMIQUE, DONT LES INTRUSIONS RUSSES DANS L'ÉLECTION PRÉSIDENTIELLE AMÉRICAINE NE SONT QU'UN EXEMPLE PARMI D'AUTRES. SI TOUTES LES ENTREPRISES DU MONDE SONT AUJOURD'HUI SOUMISES À DES MENACES D'INTRUSION TÉLÉCOMMANDÉES OU NON PAR DES ÉTATS, LE PIRATAGE À DES FINS POLITIQUES OU/ET MILITAIRES A PRIS DES PROPORTIONS CONSIDÉRABLES.

Seules au fond la Chine et la Russie, à un degré moindre, se sont donné les moyens de contester cette hégémonie.

Toutes deux en se déconnectant peu ou prou du Web mondial ou, plus précisément, en introduisant un sas entre celui-ci et leurs internautes nationaux. Ainsi, en particulier la Chine, se sont-elles dotées d'un système d'adressage distinct du système mondial. Celui-ci est en effet constitué d'un annuaire mondial des terminaux dont les adresses sont attribuées par une société… de droit américain gérée par la communauté internationale des utilisateurs (opérateurs et citoyens) : l'ICANN. Le sas établit par ces États leur permet en pratique de réorienter les requêtes effectuées par des usagers nationaux vers des sites éventuellement épurés des informations proscrites.

La Chine s'est, par ailleurs, dotée d'un réseau d'acteurs « doublonnant » celui des EU : à chaque entité des Gafam correspond une entreprise chinoise (Baidu, Alibaba, Tencent, Xiaomi) contrôlant le marché domestique, traduisant une capacité industrielle et technologique comparable, et offrant une force de frappe inférieure mais de même nature. Ce dont témoignent d'ailleurs les interrogations répétées sur la fiabilité du matériel proposé par Huawei suspecté d'être infecté par des dispositifs espions, justifiant les réticences de nombreux États a en faire l'opérateur de leur 5 G.

La rivalité s'est, en effet, naturellement déplacée des enjeux industriels à ceux de sécurité dont on a vu qu'ils étaient inévitablement liés.

Sans qu'il soit encore nécessaire de parler de cyberguerre, le Net est devenu le champ clos d'un affrontement multiforme.

Tous les grands pays se sont ainsi dotés de capacité de surveillance tournant vite à l'espionnage, voire aux tentatives délibérées de déstabilisation politique ou économique, dont les intrusions russes dans l'élection présidentielle américaine ne sont qu'un exemple parmi d'autres. Si toutes les entreprises du monde sont aujourd'hui soumises à des menaces d'intrusion télécommandées ou non par des États, le piratage à des fins politiques ou/et militaires a pris des proportions considérables. De l'initiative isolée serbe sur les serveurs de l'OTAN en forme de riposte aux bombardements menés par les États-Unis dans les années 1990 à l'attaque générale dont a fait l'objet l'Estonie dix ans plus tard, on a, à l'évidence, changé d'échelle.

Le sabotage par des logiciels malveillants des infrastructures critiques (eau, énergie, etc.) est désormais un risque possible au point qu'en 2012 le secrétaire américain à la Défense Léon Panetta n'hésitait pas à exprimer ses craintes quant à ce qu'il devait appeler de manière éloquente « *un cyber Pearl Harbor* ».

C'est que chaque pays semble désormais rivaliser d'imagination : le virus américain Stuxnet a ainsi détruit en 2009 plusieurs centrifugeuses de la centrale de Natanz en Iran (provoquant en retour en 2013 l'intrusion de hackers iraniens dans le système informatique d'un barrage près de New York). On ne compte plus les agressions dont la gravité va croissant : le piratage du système de détection aérienne syrien par Israël en 2007 ou celui du système de contrôle des Rafales de la Marine en 2009, cloués au sol ; ou encore celui du NHS en 2017 ; toutes initiatives présentant l'avantage de la précision, de leur caractère asymétrique, bon marché, comme de la discrétion et de la difficulté à en identifier la source.

Dès lors, tous les États, après avoir mis en place des outils de prévention de l'espionnage économique, se dotent progressivement d'unités chargées de conduire le combat numérique (il existe un EU cybercommand depuis 2010 ; la France s'est équipée d'un cyber com en 2016 avec autorité sur toutes les unités opérationnelles spécialisées des trois armes, soit 2 600 hommes et 600 experts de la direction générale de l'Armement (DGA), sans compter 4 400 réservistes).

Le risque d'escalade est désormais sérieux et justifierait un effort de régulation qui en reste malheureusement aux balbutiements, dans cette dimension de la révolution numérique comme d'ailleurs dans les autres.

Certes, on l'a vu, des efforts ont été faits, en particulier à l'initiative de l'UE, pour fixer des règles protégeant les données personnelles et avec elles nos libertés.

La régulation technique du réseau et de ses standards est de son côté bien établie même si elle garde souvent un caractère informel, voire autogéré. En effet, les ingénieurs et techniciens ont imaginé un modèle de gouvernance collégiale indispensable à la définition de standards communs et à l'évolution des réseaux qu'ils ont réussi, envers et contre tout, à préserver… même si l'influence des Gafam y est élevée.

Mais il n'existe toujours pas de cadre politique et juridique partagé internationalement et rappelant les principes fondamentaux de fonctionnement du Net comme les règles applicables aux relations numériques entre États.

Certes, la communauté internationale s'est saisie du sujet.

La perspective d'élaborer un traité international qui définirait et sanctuariserait les règles relatives à Internet est ainsi ouverte depuis que l'ONU a jugé utile de lancer en 2003 le sommet mondial sur la société de l'information qui s'est réuni depuis à de nombreuses reprises encourageant la pratique de forums mondiaux et régionaux associant tous les acteurs du monde numérique.

En 2005, le sommet de Tunis devait même permettre l'adoption à l'unanimité d'une déclaration dite « Agenda de Tunis » importante par les repères qu'elle fixe, mais dénuée de toute force juridique. Du coup, les « quatre grands principes » de gouvernance du Net qu'elle a dégagés restent fragiles qu'il s'agisse de sa neutralité, contestée par les fournisseurs d'accès et abandonnée il y a peu aux États-Unis par la Fédéral communication Commission ; de son unité, fragilisée par les murs de protection élevés par Chinois et Russes ; ou de sa gouvernance multipartite, contestée, on s'en souvient, pour l'influence qu'y exercent en sous-main les Gafam et le gouvernement américain. Seul le principe de protection des données personnelles a semblé progresser sous cette réserve que son caractère juridique n'est pour l'heure pleinement affirmé qu'au sein de l'UE.

L'hypothèse d'un consensus autour d'une sorte de Charte internationale des droits numériques relève par conséquent toujours de l'utopie.

La rivalité entre les puissances se donne en effet libre cours dans les instances de l'ONU (comme lors du débat sur la proposition faite en 2011 par le Brésil et l'Afrique du Sud de créer un comité de l'Onu pour les politiques) ou en dehors (par exemple à travers le projet de « code de bonne conduite intergouvernemental » défendu par le groupe de Shanghai la même année) butant à chaque fois sur le refus des EU, et, à un moindre degré, de l'UE, de placer le Net sous le contrôle même partiel des États les plus restrictifs en matière de liberté numérique, à savoir la Chine et la Russie, sous couvert de l'ONU. Ce qui a eu pour effet de bloquer toute évolution comme l'a illustré l'échec de la Conférence de l'UIT à Dubaï en 2012.

Sans doute faudra-t-il apprendre à se satisfaire d'une évolution progressive comme celle enregistrée par exemple sur les risques de cyberguerre dont chacun s'accorde désormais à penser qu'elle relève du droit international applicable aux conflits armés et dont le *Manuel de Tallinn*, élaboré patiemment par un groupe d'experts internationaux, s'efforce de tirer, de manière seulement indicative, les conséquences.

La prise de conscience des enjeux est, à cet égard, indéniable mais elle n'oblitère pas la préoccupation qu'ont les Puissances de leurs intérêts nationaux : ainsi la Chine s'est-elle engagée auprès du Président Obama voici quelques années à mettre en veilleuse son espionnage industriel et a depuis plutôt tenu cet engagement. Mais c'est qu'elle avait atteint en la matière ces principaux objectifs comme en témoigne le saut technologique accompli par Huawei.

Au final, comment ne pas voir qu'à l'instar des mers et des océans avant-hier, de l'espace aérien puis interstellaire hier, le cyberespace constitue, comme bien commun, un formidable enjeu de régulation ? Et l'on serait en droit d'attendre de la France, dont c'est la vocation, qu'elle soit à la manœuvre pour en favoriser l'émergence.

Mais la contradiction entre un réseau conçu techniquement comme sans frontières ni centre et un système international westphalien restera sans doute indépassable à une époque où la redistribution des cartes entre les puissances bat son plein ■