

Épreuve de Culture générale.

Les progrès de la technologie mise au service des États ont toujours alimenté les craintes de citoyens fantasmant les contours terrifiants d'un Léviathan au mille yeux, sachant tout, et disposant d'un pouvoir absolu. Et, de fait, le Big Brother de 1984 est devenu, du moins en théorie, une réalité puisqu'il est possible de déclencher à distance certains objets connectés, à l'insu de son propriétaire, pour l'écouter et le voir. Or les appareils utilisent la technologie numérique - par opposition à l'analogique; cette distinction technique, néanmoins ~~est~~ effacée par un emploi plus large du terme "numérique", désignant l'ensemble des technologies de l'information et de la communication employant des appareils électroniques connectés les uns aux autres par des réseaux numériques: au centre du numérique, il y a donc Internet. Or face à Internet, les États sont loins d'être aussi à l'aise que Big Brother le laisse croire, car si le numérique peut décupler les capacités de surveillance, il multiplie en proportion bien supérieure l'espace à surveiller. Dès lors, le numérique représente

pour nombre d'États bien plus un problème, une menace
et un défi, qu'un atout.

Les États à l'heure du numérique se voient
en fait contraints à une brutale nécessité de
modernisation et de mise à jour qui peut, à comp-
sûr, en menacer les définitions traditionnelles.

Quel est l'enjeu est, pour les États, de parvenir à
exploiter les richesses nées de ces évolutions techniques.

On verra donc que l'"heure numérique"
a déjà sonné pour les États, qui en font un
outil de modernisation des services. On s'interro-
gera ensuite sur la méfiance que, pourtant, les
États nourrissent vis-à-vis du numérique, avant
de voir dans quelle mesure la question du
numérique est elle, posée sans détour, de
la souveraineté des États et de leur modernisation,
questions cruciales si l'État veut faire du numérique
un atout, et pas un simple outil de gestion.

I Les Etats à l'heure du numérique.

Les technologies liées à la révolution numérique ont conduit les Etats à un mouvement de rationalisation et de modernisation depuis une quinzaine d'années, mais des efforts restent à faire dans la maîtrise de ces outils.

A Mise à jour des services de l'Etat.

Les progrès dans la gestion de données permis par les technologies numériques ont conduit les Etats à rapidement les exploiter pour tirer parti de leur richesse et de leur souplesse d'emploi. Le mouvement est, globalement, celui d'une rationalisation des services de l'Etat, qui peut prendre plusieurs formes : une aide à la surveillance et à la sécurité, par la veille informatique de la gendarmerie, à la surveillance, par la possibilité de consulter immédiatement les dossiers de fichage, mais aussi par l'emploi de bracelets électroniques permettant de trouver une alternative à la prison. En matière de sécurité, la loi renseignement s'appuie largement sur la technologie numérique pour permettre aux agents d'en tirer le meilleur profit. Outre ces aspects de surveillance, renvoyant au Big Brother de Orwell, et qui ont, pour cette raison, agité le débat public, il faut noter que les services comme la télé déclaration de revenus, la possibilité de commander par voie électronique des documents d'état-civil, la simplification des démarches administratives grâce aux technologies numériques, constituent un progrès réel dans l'administration et le service public, et que l'Etat rationalise ses ressources de façon

efficace. Le numérique permet, à coup sûr, aux États d'optimiser le service public et de l'améliorer, et le processus de modernisation est général.

2. Maîtrise technique et formation.

Cet élan de modernisation, cependant, ne va pas sans crispations, et l'émergence d'une nouvelle technologie nécessite de donner à tous les acteurs la formation ~~adéquate~~ adéquate. Le transfert de certaines démarches au numérique n'a pas été immédiat, et les procédures d'admission dans l'enseignement supérieur, jusqu'au milieu des années 2000, devaient passer par le Ministre : le fait indique sans doute une défiance vis-à-vis de la nouveauté, aisément explicable par le manque de familiarité des décideurs actuels avec les nouveaux moyens de communication. Deux exemples récents illustrent la maladresse ^{avec laquelle} ~~avec laquelle~~ les personnels de l'État peuvent ~~aussi~~ considérer l'heure numérique : d'abord, la confusion ~~de~~ grave dont s'est rendue coupable Hillary Clinton en mélangeant ses boîtes de réception électroniques personnelles et professionnelles, alors qu'elle était ministre des Affaires étrangères ; ensuite, la naïveté du juge australien permettant à Kim Dotcom de retransmettre par Twitter son déroulement de son procès, à condition qu'il ne soit pas gardé de copie de ces minutes. Condition irréalisable puisque la duplication de l'information est la condition même du numérique. Les deux exemples, américain et australien, montrent de façon assez frappante à quel point le développement du numérique est tributaire d'un personnel politique, ou juridique, pas toujours très au fait de ses spécificités. Dès lors,

Épreuve de Culture Générale

l'heure numérique, avant d'être un atout ou une menace, et d'abord un défi scientifique, auquel les pays donnent des réponses très variées quoique prévisibles : ainsi les pays du Nord de l'Europe ont-ils promu dans l'enseignement secondaire l'emploi du numérique très précocement, tandis qu'en France, ^{on} ~~se~~ débat entre partisans d'une école sans tablettes, puis que des expérimentations ont été lancées pour équiper de tablettes certains ~~collégiens~~ ^{collégiens}, et les tenants d'une entrée massive des terminaux électroniques connectés à l'école.

Il apparaît donc que les États ont bien intégré le passage à l'heure numérique, et ont pour intention d'exploiter les nombreux avantages que propose ~~ce~~ cette révolution technique en terme de gestion, de statistique. Mais le défi posé par le changement est celui de la formation et de la maîtrise technique, qui seules peuvent garantir une exploitation efficace de l'outil.

II) Etat et Terra incognita : la conquête de l'espace numérique.

Si les Etats se sont plus ou moins ^{min} à l'heure du numérique, ils leur font désormais en maîtrise l'espace, car celui-ci apparaît encore comme largement inexploré, espace pré-juridique pour ainsi dire, et par là même hostile à l'Etat. On verra pourquoi cet espace numérique peut constituer une menace pour l'ordre étatique, et comment ce dernier tente néanmoins de s'y imposer.

A) L'Etat en péril face au numérique.

Il semble que le numérique constitue à certains égards une menace pour l'Etat, dans la mesure où il ouvre un espace nouveau, dans lequel on peut se cacher, et à peu près tout dire. Le tableau horridique du numérique ~~correspond~~ correspond aux dangers que y voient certains pays, qui censurent les contenus, voire ferment les réseaux. Ainsi la Turquie censure-t-elle le logiciel Twitter, la Chine bloque-t-elle un certain nombre d'applications

et l'Iran veut-il mettre en place un "internet iranien", permettant de bloquer les espaces jugés dangereux. Si cette censure fait partie de l'arsenal des régimes autoritaires, elle correspond à un vieux réflexe des États, considérant qu'en certains cas, des ponts doivent être coupés et les communications interdites : c'est d'ailleurs si le numérique peut représenter un danger évident. La réaction du gouvernement égyptien, mis en difficulté en janvier 2011, fut ainsi de couper internet et communications de téléphones portables ; des dispositions similaires existaient dans la loi relative à l'état d'urgence de 1955, ~~donnée~~ si les ^{françaises} technologies numériques, par l'espace de liberté qu'elles créent, constituent un danger pour certains régimes, il n'en demeure pas moins que la criminalité, le terrorisme et une "course des mirades" cybernétique peut se développer en sécurité sur les réseaux, abritée par des logiciels de cryptage sophistiqués et quasi impénétrables. L'actualité récente a montré qu'une application comme "Telegram", conçue pour déjouer la surveillance des services de sécurité russes, a pu être utilisée à la fois par des terroristes annonçant un attentat, et par des hommes politiques français : se rassurer d'être à l'abri jouant le même rôle dans les deux cas. La méfiance que peut inspirer l'espace numérique n'est donc pas que le fait d'une paranoïa de régime autoritaire, car son existence pose de vraies questions de droit.

B. L'irruption de la loi dans une zone de non-droit.
Espace récent, l'espace numérique ~~avant~~ n'acquiesce que petit à petit un cadre juridique, et le législateur se trouve face à une zone particulièrement malaisée à circonscrire sur le plan juridique. La vigueur des débats autour de la loi Hadopi montre à quel point l'espace numérique est rétif à l'irruption du droit, quand bien même il s'agit de mettre un terme au pillage que constitue le téléchargement illégal. La protection sommaire mise en place par Hadopi est donc bien légère face à la réalité des possibilités d'échange de données numériques - et d'autant plus que l'opinion publique souhaite que cet espace conserve l'anonymat qu'il promet, et sa confidentialité. C'est en France la mission de la Commission nationale Informatique et Liberté (CNIL) dont les attributions dépassent les moyens, mais qui vient de se voir "épauler" par le Conseil constitutionnel lorsque celui-ci a censuré un paragraphe de l'article 11 de la loi sur l'Etat d'urgence de 1955, révisée en 2015. Le Conseil constitutionnel a ~~interdit~~ suspendu la possibilité donnée à la police de copier des données informatiques saisies sur un ~~ordinateur~~ terminal, mais aussi sur d'autres machines auquel un réseau permet d'accéder. Le pouvoir que peut donner à l'Etat la technologie numérique est donc limité, justement parce qu'il risquerait d'être illimité. Les efforts de la France, en effet, pour donner des règles à l'espace numérique, restent quasi symboliques tant cet espace apparaît comme supra national. La question du lieu où a été commise une infraction

8/14

Épreuve de Culture générale

débient quasi formelle dans la mesure où les techniques "d'oignon" permettent de dissimuler d'adresse IP en adresse IP, à travers le réseau TOR par exemple. Il devient, dans les conditions, impossible pour un État de faire respecter son droit, puisque l'espace numérique ne relève de sa juridiction que s'il a les moyens de l'y appliquer. Par ailleurs, les lois nationales pouvant être contradictoires les unes avec les autres, ce qui est dit sur l'espace numérique est à la fois interdit et légal. L'irruption de la loi dans le numérique est donc problématique.

L'État face aux technologies numériques se trouve dans une posture inconfortable, puisqu'il lui est difficile de le contrôler, et presque impossible d'y légiférer de façon efficace. L'ampleur des fraudes fiscales dont sont accusés les grands firmes d'Internet illustrent cruellement la détresse des États par rapport à l'économie numérique.

III La redéfinition de l'Etat nation dans le cyberspace.

L'Etat est un acteur du numérique, mais pas l'acteur omnipotent que l'histoire l'a habitué à pouvoir être dans les espaces placés en son pouvoir. Afin de faire du numérique un atout, et non une menace, l'Etat doit donc, en partie, se redéfinir.

A. La souveraineté mise à mal

On l'a vu, les prérogatives de l'Etat dans l'espace numérique sont limitées. Mais le phénomène est accentué et rendu plus aigre encore par l'inégalité totale regnant entre les différents Etats : une hégémonie des Etats Unis est, évidemment, plus écrasante qu'elle ne l'a jamais été politiquement de la gestion des noms de domaine à la situation monopolistique des géants américains Google, Amazon etc, les USA contrôlent absolument tous les aspects de l'internet grand public, ainsi que la conception des logiciels d'exploitation principaux,

Windows et Macintosh. Dès lors, on peut se demander quelle est la réelle fiabilité des systèmes de stockage "Cloud" dont le contenu est, de toute façon, lisible par qui sait ^{comment} y prendre. Face à cette perte de souveraineté de tous les États au profit des USA, se développe donc une guerre numérique, parfois d'origine étatique, menant des campagnes de "hacking" & visant des intérêts nationaux. Malgré les difficultés qu'il y a à établir des preuves solides, il semble que le États russe, chinois ou nord-coréens utilisent cette arme numérique. En fin de compte, cependant, il apparaît, sur le plan international, une réelle "fracture numérique" entre une pays leader, et les autres, plus ou moins équipés pour faire face à cette hégémonie.

B La perpétuelle réinvention de l'État par lui-même.

La situation des États face au numérique illustre le paradoxe sans cesse réactualisé d'un État qui, par définition, doit être stable, presque intangible, et qui cependant est contraint en permanence à évoluer. Cette redéfinition des limites et des frontières est particulièrement nette avec le numérique, et appelle à long sûr un règlement international des enjeux et des questions posées : de même que les avancées au fond des mers et dans l'espace stratosphérique ont conduit les États à cartographier ces nouvelles zones d'influence, sans doute faut-il que l'espace numérique soit envisagé comme un nouveau territoire, que chaque État ne peut utiliser à sa

manière, — et sans en avoir les moyens. Si cet espace numérique acquiert, tel les fonds marins, le statut de "patrimoine commun de l'humanité", alors les États pourraient envisager son existence plutôt comme un atout que comme une menace. L'absence de contrôle, ou la difficulté extrême, tient moins à la faiblesse des États qu'à la structure de l'espace. Imaginer une souveraineté élanique sur cet espace numérique est donc illusoire. Dès lors, l'heure numérique doit être celle de opportunités à saisir et de chantiers à lancer, puisque le numérique constitue un terrain nouveau, dans lequel l'investissement est viable, et les possibilités d'emploi, vastes. Le numérique, secteur à la fois scientifique et économique, porte en lui des atouts évidents de croissance pour les États. L'autre versant, plus politique, de la modernisation, pourrait être le changement de gouvernance qu'impose l'heure numérique. Créant, en effet, un espace de débat, d'information et de révélation particulièrement viable, comme le montrent les affaires Manning, Wikileaks, Assange, l'espace numérique a sans doute pour vocation d'être le lieu d'une citoyenneté renouvelée, et d'une politique plus transparente. À l'atout quantitatif de la maîtrise des flux d'informations, les États pourraient ajouter l'atout qualitatif d'un exercice plus transparent du pouvoir.

Dans les conditions actuelles, l'espace numérique n'est pas celui d'un exercice

12/14

Épreuve de Culture Générale.

classique et équilibre du pouvoir par les États,
mais plutôt celui d'une rédefinition des prérogatives
de l'État.

L'heure numérique constitue pour les
États une réalité technique qu'ils ont prise en
compte en exploitant les ~~avantages~~ bénéfices
en terme de rationalisation et d'optimisation
du service public. Cet atout technique veut,
cependant, représenter une menace dans la
mesure où l'État ne peut pas intervenir
aisément dans le nouvel espace où il n'est
d'ailleurs pas le bienvenu. Le monopole américain,
enfin, peut constituer un danger, que les écarts
à grande échelle ont confirmé. Si, malgré
ces éléments menaçant leur existence même, les
États peuvent faire du numérique un atout,
c'est en en faisant non un objet de contrôle,
mais d'investissement: à un effort de formation
accru doit s'ajouter l'ambition de faire
du numérique un chantier économique et un

chantier moral

14/14

Voir au dos.