Dossier n° 28
« La cybermondialisation : opportunités et risques »

Bien que très présente dans le quotidien, la dimension « cyber » reste difficile à appréhender. Des entreprises où l'essor d'une « iconomie » est possible aux agents de la culture qui découvrent d'autres pratiques, en passant par le domaine stratégique qui doit faire face à une cybercriminalité galopante, les enjeux sont énormes et nécessitent de s'interroger davantage sur les risques mais aussi sur les opportunités de cette « cybermondialisation » en marche. La question de la régulation d'Internet, centrale une fois encore dans l'agenda de la *World Conférence On International Telecommunications* « WCIT-12 » (décembre 2012) se pose dans un contexte de recherche incessante du juste équilibre.[1]

De l'économie à l'iconomie : opportunités et défis de la transition par Michel VOLLE coprésident de l'Institut Xerfi

L'automatisation est source de polémiques. De nombreux auteurs estiment qu'il n'y a plus rien à en attendre. Si Jeremy Rifkin définit la 3ème révolution industrielle comme issue de la seule transition verte, il néglige le fait, lui reproche Michel Volle, que l'informatisation constitue au contraire une arme des plus puissantes pour assurer les économies d'énergie nécessaires.

Il importe de savoir vers quelle économie on se dirige. M. Volle a préféré donner à cet horizon le nom d' « iconomie » plutôt que de se référer au numérique, jugeant que ce substantif, davantage tourné vers la dimension culturelle, ne permet pas de rendre compte au mieux de la « transformation des possibles » à l'œuvre. L'iconomie n'est pas une économie post-industrielle, mais bien plutôt « ultra industrielle » et fortement capitalistique. Elle se définit comme l'automatisation de l'ensemble des tâches répétitives, physiques et mentales. Seuls sont nécessaires dans les usines et dans les bureaux des « superviseurs ». Le produit devient un assemblage de biens et de services, produit par un réseau de partenaires et non plus de « A à Z » dans une seule entité. La colonne vertébrale de la « nouvelle » entreprise s'articule autour d'un système d'information et présente une certaine configuration : un centre de recherche très innovant aux côtés d'une usine qui forme le « noyau dur » de l'organisation, auquel s'ajoutent des usines dispersées un peu partout dans le monde, afin d'être notamment au plus près des clients. L'emploi se concentre dans les activités de recherche (conception et ingénierie) et dans les services. La « main d'œuvre » devient un « cerveau d'œuvre » dont la plus grande vertu réside dans la « débrouillardise », soit la capacité à interpréter des situations inédites et à prendre des décisions nouvelles. La mécanisation au XIXème siècle a eu des conséquences anthropologiques, sociologiques, économiques, majeures: multiplication du salariat, développement de la classe ouvrière, urbanisation, concurrence entre nations industrialisées, jusqu'à l'essor de l'enseignement public obligatoire puisque l'économie mécanisée rendait nécessaire une main d'œuvre plus instruite. M. Volle anticipe des conséquences tout aussi importantes pour l'iconomie, conséquence évidemment différentes, mais qui toucheront tous les secteurs, comme c'est le cas pour chaque révolution industrielle. Déjà on en pressent les signes dans l'informatisation du corps par l'intermédiaire du téléphone mobile, ou dans l'Internet des objets qui fait que la frontière entre virtuel et réel est franchie. M. Volle, juge également que l'écart reste immense entre ce que nous pressentons du potentiel de l'iconomie et la réalité de ce qui nous attend.

L'iconomie n'est pas pour autant un monde idéal, exempt de dangers ou difficultés. Il y aura en effet à court terme une destruction de l'emploi, et donc une transition délicate et pénible vers le plein emploi, résultat (quasi *de facto*) de cette économie à l'équilibre que permettra l'iconomie. Cela implique notamment de modifier le contenu de l'enseignement supérieur et en particulier celui de l'enseignement scientifique qui ne correspond plus aux besoins. Ces perspectives peuvent cependant inquiéter et M. Volle regrette que les entreprises ne s'engagent souvent dans la démarche de l'iconomie qu'à reculons. Elles refusent en effet selon lui au « cerveau d'œuvre » la légitimité qui lui permettrait pourtant d'assurer les responsabilités dont elle le charge. C'est ainsi que tout en demandant à leurs agents de prendre des initiatives, elles écoutent rarement ses derniers quand ils souhaitent faire remonter des informations du terrain, au nom d'une certaine conception du pouvoir. Cette prise en tenaille, sur fond de systèmes d'information mal conçus, ne peut que générer les « épidémies de stress » dénoncées dans nombre de structures.

L'iconomie peut également souffrir de faiblesses intrinsèques. Un logiciel peut provoquer des catastrophes face à des évènements qui n'ont pas été testés *a priori*, en l'absence d'une supervision adaptée. L'iconomie ne protège pas davantage des tentations, comme en

(1) Ce dossier a été rédigé sur la base des analyses présentées lors du 28ème *Rendez-vous de la mondialisation* du 12 décembre 2012, présidé par Kavé Salamatian, professeur des universités à l'université de Savoie. Ce dernier a fait valoir combien Internet était jusqu'à présent un problème de « technologues » alors même que le cyberespace est éminemment politique. Il importe que le politique s'empare toujours davantage du sujet, ce qu'il a commencé à faire, en privilégiant une approche multidisciplinaire. Vincent Chriqui, directeur général du Centre d'analyse stratégique, a prononcé le discours d'ouverture en s'interrogeant en particulier sur les conséquences d'une plus grande utilisation d'Internet pour les grandes entreprises et PME.

témoigne le glissement du système financier, selon M Volle, vers la délinquance de masse, ou le blanchiment d'argent au profit du crime organisé. Dans les deux cas, une structure de pouvoir de type féodal peut apparaître. Ceci constitue un défi à la démocratie et à l'Etat de droit. Certains considèrent, alerte M. Volle, que ces principes n'auront été nécessaires que durant une certaine période, celle d'une économie mécanisée supposant des règles stables, et qu'ils seront remis en cause par l'automatisation. Si nous tenons vraiment à ces principes, il y aura également là un très grand défi à relever.

La cyberculture : quelle appropriation des éléments de culture dans la cybermondialisation ? par Laurent Sorbier, directeur général de l'établissement public du Musée National Picasso

Cernant les conséquences de la cybermondialisation sur la circulation des œuvres et l'évolution des pratiques culturelles, Laurent Sorbier distingue quatre grandes évolutions. En premier lieu, un « réflexe Internet » est désormais incontestable dans les pays industrialisés pour ce qui est des activités culturelles. Choisir un livre, aller au cinéma, se déplacer pour une exposition est maintenant quasi systématiquement précédé d'un recours à Internet avec la consultation de sources très diversifiées, et/ou aux réseaux sociaux pour demander un avis à la communauté d'amis ou de contacts. C'est toute une « économie de la conversation » qui se met en place. Il devient donc central pour tout acteur de la scène culturelle d'assurer sa présence et sa visibilité sur ces réseaux. Si dans le « monde ancien », les œuvres étaient sélectionnées par des professionnels de la culture, des « sachants » selon un modèle « *top down* », le changement qui s'est dessiné à la fin des années 1990 est encore plus prégnant aujourd'hui. Les circuits de circulation des œuvres ont muté, avec à la manœuvre des individus, des blogueurs influents ou « influenceurs » et plus seulement des institutions évoluant selon un processus très organisé. L'« économie de la recommandation » aboutit à un univers beaucoup plus horizontal, induisant une forme de *hiatus* quand ce n'est pas de compétition pure et simple entre les différents intervenants. S'ajoute à cela, à la marge, le phénomène relativement nouveau (au XVIIIème siècle on diffusait déjà des œuvres sous le manteau) des solutions pirates ou illégales complexifiant la donne.

En second lieu, la cybermondialisation a fait muter le format même des œuvres culturelles. Ce sont les formats courts qui prolifèrent désormais et les oeuvres interactives qui se multiplient. L. Sorbier y voit la manifestation même de la culture « Bref » du nom du programme court composé de saynètes qui s'est imposé sur Canal Plus. Ce phénomène n'en est encore qu'à ses débuts et L. Sorbier met en exergue les nouvelles pratiques en train de s'instaurer dans les musées où la réalité augmentée associée à la géolocalisation, permettra d'adresser à l'écran de chaque visiteur, au fil de sa déambulation, des commentaires sur l'œuvre qu'il est en train de regarder. A condition, souligne L. Sorbier, qu'il regarde vraiment l'œuvre en question, puisque le premier réflexe est de photographier l'œuvre pour ensuite la commenter à ces amis. Les institutions vont être tenues de s'adapter et toutes les pratiques seront touchées, jusqu'à celle considérée comme une des plus individuelles, celle de la lecture, quand on voit l'appétence des moins de 25 ans pour le « livre augmenté ».

En troisième lieu, le modèle économique de la culture est très perturbé par la cybermondialisation. L'empilement des contraintes législatives et réglementaires, issues de l'autorégulation s'est construit dans un cadre essentiellement national, au mieux européen. Mais qu'en est-il d'une œuvre immédiatement disponible à l'autre bout du monde ? Il est aujourd'hui facile de se la procurer. On voit toute l'importance de l'harmonisation fiscale et des distorsions de prix (cf. la « *Google Lex* »). C'est pour cette raison que plusieurs univers sont en crise, notamment la presse, l'audiovisuel et le livre.

L. Sorbier entend enfin s'opposer aux Cassandres et souligner que la cybermondialisation peut accroître l'intérêt, via essentiellement le « bouche à oreille » pour des productions culturelles « exotiques » venant des quatre coins du globe, ou des productions qui n'auraient pu être découvertes et appréciées dans le seul monde analogique. Le succès des séries coréennes en a ainsi surpris plus d'un. Certes, les produits qui proviennent jusqu'à nous ont fait l'objet d'une forme d'industrialisation et on ne peut nier que la cybermondialisation peut également enclencher un réflexe de suivisme. Il ne faut pas non plus négliger une possible amplification des dominations existantes au profit des productions très adaptées à la logique d'Internet et très performantes dans cet environnement. La cyberculture se trouve dans une phase intermédiaire, continuant de présenter un « visage à la *Janus* ». La construction d'une régulation adaptée, au niveau mondial, et surtout les initiatives des créateurs eux-mêmes, sont à même de permettre au numérique, qui est quand même ce qui est arrivé de mieux à la culture depuis longtemps selon L. Sorbier, d'exploiter tout son potentiel.

Cybermondialisation : les risques de cybercriminalité et de cyberguerre, par Alix Desforges, chercheur à l'Institut français de géopolitique à l'université Paris 8

Depuis l'apparition des premiers virus à la fin des années 1980, les utilisations malveillantes d'Internet ont connu une croissance exponentielle que viennent renforcer la démocratisation de l'utilisation des réseaux et des technologies IP. La menace a pris une dimension globale, où l'agresseur peut être tout aussi bien votre voisin de palier qu'une entité situé à des milliers de kilomètres se jouant des frontières.

Alix Desforges distingue tout d'abord la cybercriminalité qui se caractérise par une spécialisation très marquée et une vraie division du travail entre ceux qui recherchent les vulnérabilités, ceux qui conçoivent les logiciels malveillants et les commerciaux qui cherchent les clients.

La cybercriminalité dégage désormais des profits supérieurs à ceux générés par le trafic de drogue. Ce sont ainsi 100 000 logiciels malveillants qui sont découverts chaque jour, dont 1% constitue une menace sérieuse pour la sécurité des Etats. C'est dans le domaine de la cybercriminalité qui se développent toutes les techniques utilisées par ailleurs : du *social ingeniering* à l'usage de logiciels espion en passant par les attaques en déni de services visant à saturer les sites. Le couplage de plusieurs techniques peut aboutir à des stratégies beaucoup plus nuisibles. Les conflits et les rivalités trouvant presque toujours une résonance dans le cyberespace, la déstabilisation politique repose ainsi sur une série d'attaques quotidiennes, prenant le plus souvent la forme d'attaques en déni de service ou de défacement de sites pour faire passer des messages.

Deuxième source d'inquiétudes pour les Etats, parfois encore plus redoutée que la première en raison de ses effets majeurs dans la vie quotidienne, le vol d'informations sensibles. L'espionnage vise le secteur industriel, économique, financier, politique ou diplomatique (affaire de Bercy 2011 ou virus *Flame* de mai 2012). Le sabotage concerne des infrastructures critiques tels que les réseaux de distribution d'énergie, le système de santé, la structure financière, à l'image de l'attaque ayant paralysé la compagnie pétrolière saoudienne Aramco (août 2012). Ce type d'attaque est cependant complexe à mettre en place, supposant un savoir-faire qui n'est à la portée de tous.

La cyberguerre est un concept qui ne fait pas consensus. Deux définitions s'affrontent : soit la cyberguerre est considérée comme une guerre engageant des moyens uniquement « cyber », remplaçant la guerre « classique », soit elle renvoie à tout type d'attaque. Savoir par exemple si des lignes de code constituent une arme n'a toujours pas été tranché au niveau international. Entre attaques non détectées et attaques non déclarées pour éviter d'afficher tout signe de faiblesse, il est difficile d'avoir une vision très claire de ce qu'est la cyberguerre. L'utilisation de la dimension « cyber » en cas de conflit armé s'est cependant déjà imposée. Les cybertactiques viennent compléter les opérations « classiques ». Selon Alix Desforges, la cyberguerre ne constitue pas pour autant le cinquième domaine après la mer, la terre, le ciel et l'espace Mais ellle oblige les Etats à redéfinir ce qu'est un ennemi. Derrière une ligne de front, l'ennemi est « à peu près » cerné. L'ordinateur permet l'anonymat, et il devient d'autant plus difficile d'identifier formellement, au-delà du simple faisceau d'indices, un individu isolé, une entité criminelle ou mafieuse, une organisation, un Etat pouvant même être un allié. S'ajoute la discrétion des attaques, qui peuvent n'être détectées que des semaines, voire des mois plus tard, l'attaquant ayant donc eu le temps d'exfiltrer de grandes quantités d'information. De plus, en dépit du perfectionnement des systèmes de défense, l'avantage reste à l'attaquant qui frappe à une vitesse telle qu'il est très difficile de réagir contrairement à la plupart des missiles qui sont détectables à l'avance). Le « brouillard sémantique » dénoncé par A. Desforges (tout devenant « cyber ») complexifie la situation et renforce le sentiment d'insécurité des Etats.

Ces derniers ont réagi de manière différente. La vraie prise de conscience politique dans l'Union européenne et en particulier en France a eu lieu après les cyberattaques en Estonie (2007) et en Géorgie (2009). La cybersécurité est ainsi devenue pour la France un enjeu de souveraineté nationale, aux côtés de la dissuasion nucléaire, des missiles balistiques et des sous-marins nucléaires d'attaque dans le Livre Blanc de la défense et de sécurité nationale. Ceci constitue pour A. Desforges un tournant majeur, qui se traduit par les moyens de plus en plus importants mis à disposition de l'Agence nationale de sécurité des systèmes d'information.

Il n'en reste pas moins impossible d'atteindre un seuil de sécurité absolu en la matière, de nouvelles vulnérabilités étant sans cesse mises au jour, d'où l'inanité de quelque « ligne Maginot » que ce soit. Le concept de « lutte informatique offensive », mis en avant par les Etats Unis ainsi que le discours dissuasif repris par nombre d'Etats restent flous mais génèrent le début d'une course à l'armement. Commence à se développer un marché dans lesquels des entreprises vendent exclusivement à ces derniers ou à des agences de renseignements des dispositifs de surveillance et des failles prêtes à être exploitées. La coopération internationale, avec le partage d'informations sensibles qu'elle suppose, ne paraît pas vraiment une parade car elle repose sur une confiance mutuelle totale des interlocuteurs.

Enfin, tout ceci n'est pas seulement une affaire de machines mais aussi et surtout un problème d'hommes car ce sont eux qui ouvrent les mails contenant le Cheval de Troie, qui appliquent ou non les correctifs de sécurité. La sensibilisation aux enjeux est donc essentielle. Il ne faut pas se focaliser uniquement sur les risques. La cybersécurité présente des opportunités et notamment, pour l'Union européenne et la France, celle de favoriser l'essor d'un secteur industriel à haute valeur ajoutée et à fort potentiel d'emplois. Perspective nullement à négliger dans un contexte de crise conclut A. Desforges.

La cybermondialisation à l'épreuve de la régulation : quelle gouvernance pour Internet ? par Bernard Benhamou, Délégué aux Usages de l'Internet au ministère chargé des PME, de l'Innovation et de l'Economie Numérique

Deux milliards de personnes sont aujourd'hui concernées par Internet et sans doute très bientôt un milliard de plus grâce à l'essor de la technologie mobile. En France son développement a été très spectaculaire en quelques années : 43% des Français utilisent désormais un *smartphone,* 78% des foyers français sont connectés à Internet, le nombre d'heures passées sur l'Internet mobile étant supérieur à celui des heures passées sur un

ordinateur, dans les mêmes proportions qu'aux Etats-Unis. Ces chiffres résument l'ampleur du phénomène sociétal à l'œuvre qui recouvre lui-même un enjeu gouvernemental crucial. Toute rupture du système (cf. les problèmes récents chez Orange) constitue le possible début de déstabilisation d'un pays.

Bernard Benhamou rappelle d'emblée combien « les instruments de souveraineté sont devenus indiscernables des éléments de la puissance technologique». Les Etats-Unis en sont persuadés, affirmant que le développement d'Internet est la clé de leur croissance économique. Ils n'entendent laisser à personne d'autres qu'eux-mêmes le soin de suivre le devenir de ce formidable outil. Qu'un seul pays (même la première puissance mondiale) occupe ici « une place prépondérante » pose problème pour tout diplomate non américain, en raison du principe de souveraineté. Internet, contrairement à un mythe très répandu, est très centralisé dans sa gestion. De par la structure du nommage (procédure d'attribution des noms de domaine) et la fameuse « machine A », dont le rôle a été prépondérant dès le début, cette gestion reste encore sous le contrôle du département du commerce américain. De même, l'ICAN, organisme technique crée à l'origine par les Américains a déjà pris des décisions non plus seulement techniques mais véritablement politiques, devenant de ce fait un objet de tensions majeures. L'objectif du sommet onusien de Tunis (2003/2005) avait déjà été d'organiser un nouveau mode de gouvernance des ressources critiques d'Internet. Les enjeux n'ont pas perdu en importance, bien au contraire, lors de la *World Conférence On International Telecommunications* « WCIT-12 » (NDRL : elle s'est tenu à Dubaï du 3 au 14 décembre 2012, toujours sous l'égide de l'ONU). Toutefois, la position américaine est beaucoup plus délicate à tenir, puisque l'essor d'Internet conditionne de plus en plus la courbe de croissance de tous les pays (cf. la situation du Brésil où le paiement des impôts se fait presque uniquement en ligne).

Une première étape du développement a pris appui sur le réseau des télécommunications. Mais l'avenir se jouera également, souligne B. Benhamou, sur d'autres réseaux, tels les réseaux énergétiques ou de santé, évolution que les experts américains eux-mêmes (Kennedy School of Harvard, MIT) jugent inéluctables. D'autres acteurs, notamment ceux qui construisent les « tuyaux » apparaissent. Il en a résulté, à l'orée du Sommet de Dubaï, deux prises de position antagonistes : d'un côté, celle des Etats-Unis, fervent partisan du *statu quo* et de l'autre une vision nettement plus radicale, portée par la Russie mais aussi par la Chine et les Emirats Arabes Unis, proposant une mise sous tutelle d'une organisation intergouvernementale, les Nations-Unies en l'occurrence.

Ces deux propositions restent l'une et l'autre à risques. Alors que l'« Internet des ordinateurs » ayant prévalu jusqu'à présent est en train de se transformer en « Internet industriel », la première option répond toujours imparfaitement aux défis qui s'annoncent. La deuxième option porte en germe une « balkanisation d'Internet », perspective très inquiétante selon B. Benhamou, s'exprimant à titre personnel. Internet est en effet devenu un « espace commun » (ou *commons*), une plateforme sur laquelle s'appuie un nombre infini de services et d'activités. Faire « passer Internet sous les fourches caudines des Etats » comme certains pays non démocratiques le souhaitent, reviendra à élever une barrière à l'entrée et à freiner, sinon à abolir l'innovation. Rappelons que le web est une invention européenne, qui n'a pu s'épanouir que parce que son tout premier inventeur au CERN n'a pas eu besoin d'autorisation avant de lier entre elles des ressources au moyen de liens hypertexte. Le risque politique est lui aussi majeur. L'Union européenne ne défend pas forcément les mêmes valeurs que d'autres parties du monde, notamment en ce qui concerne la censure. Il est faux de dire qu'Internet peut résister à tout. Une modification bien calibrée de ses protocoles fondamentaux peut durablement le fragiliser.

En 2005 à Tunis, l'Union européenne avait déjà été la seule à imaginer que les Etats se soumettent eux-mêmes à une limitation de leurs pouvoirs en s'adossant aux lois dites fondamentales des réseaux ou « *requests for command* (RFC) », ce qui déboucherait sur une « coopération renforcée » entre Etats. En 2012, il est plus que jamais nécessaire d'élaborer des lignes de protection au bénéfice des citoyens. Ces derniers doivent pouvoir maîtriser les informations qu'ils délivrent à l'extérieur aujourd'hui sans en avoir réellement conscience, alors que la notion de vie privée est, du fait de l'Internet connecté, en train de changer de nature. L'Union européenne, toujours elle, défend un nouveau droit face à ces objets extraordinairement « loquaces », celui du « droit au silence des puces » *via* leur désactivation. B. Benhamou prône sur ce point une alliance transatlantique. Celle-ci pourrait constituer une force d'entrainement alors qu'aucune riposte ne sera efficace au seul plan national.