Jean Rivelois, IRD (Institut de recherche pour le développement)

LE CYBER-PAVILLON NOIR

La piraterie est présentée comme une transgression à des règles commerciales de droit qui concernent l'ensemble des produits protégés par la propriété intellectuelle, qu'il s'agisse d'une propriété intellectuelle et artistique (incluant les droits d'auteurs[1]) ou d'une propriété industrielle couvrant les brevets, les inventions, les secrets commerciaux ou d'affaires[2] , les marques commerciales[3], les dessins et modèles industriels, les bases de données, les appellations d'origine et les noms de domaine (les Indications de provenance Géographique Protégée, IGP). Censée favoriser le progrès technologique et l'émergence d'œuvres nouvelles à travers la recherche-développement, les règles de la propriété intellectuelle ignorent le mode cumulatif des productions humaines, une nouvelle technologie n'étant possible que grâce aux innovations qui l'ont précédée ; de plus, l'effet pervers de cette appropriation des découvertes est qu'elle peut ralentir la recherche et le progrès, en permettant au détenteur d'une découverte d'empêcher un autre de la pousser plus loin. De plus, ces règles commerciales produisent une marchandisation et une privatisation de tout ce que l'homme peut réaliser lui-même, incluant autant le corps humain à travers le séquençage du génome – ce qui ne devrait pas manquer d'opposer les règles commerciales et certaines règles d'éthique car l'instrumentalisation du corps humain va à l'encontre du principe selon lequel le génome humain constitue en un patrimoine commun de l'humanité – que la nature elle-même à travers la brevetabilité des

[1] Le copyright est réglementé par la Convention de Berne (1989) à laquelle ont adhéré 165 pays.

[2] Le brevet est un titre de propriété industrielle qui confère à son titulaire un droit exclusif d'exploitation sur l'invention brevetée, durant une durée limitée et sur un territoire déterminé ; il se distingue du secret industriel par lequel l'inventeur garde le secret absolu de son invention et dispose d'un monopole aussi longtemps qu'un concurrent n'aboutit pas à la même invention. La propriété intellectuelle est reconnue internationalement à travers l'OMPI (Organisation mondiale de la propriété intellectuelle, institution des Nations unies fondée en 1970) ; les brevets sont protégés par le traité de coopération sur les brevets (PCT, Patent Cooperation Treaty), entré en vigueur en 1978 et applicable dans les 142 pays signataires ; en 2005, les plus importants dépôts de brevets ont été effectués par les États-Unis (le tiers des dépôts), le Japon, l'Allemagne, la France et le Royaume Uni, l'ensemble de ces pays produisant les deux tiers du nombre total de dépôts.

[3] Les marques désignent autant des produits commerciaux que des marques dites collectives et de certification, ces dernières étant assujetties à la conformité à des normes (normes de qualité ISO 9000, par exemple). L'enregistrement international des marques dépend du protocole de Madrid (entré en vigueur en 1996) ; la protection d'une marque est de dix ans (monopole absolu d'usage) à compter de la date de dépôt de la demande, et peut être renouvelée indéfiniment. Certains mouvements, notamment altermondialistes, critiquent la propriété des marques ; cf. Klein (Naomi), *No Logo. La tyrannie des marques*, Actes Sud, 2003.

micro-organismes génétiquement modifiés et la brevetabilité du vivant [4] ; elles peuvent ainsi concerner les semences traditionnelles prohibées à la commercialisation ou les semences industrielles interdites de réutilisation car brevetées par des multinationales agro-alimentaires, ou les médicaments non transformables en génériques car brevetés par des groupes pharmaceutiques mondiaux et dont le prix les rend inaccessibles aux populations des pays du Sud. A travers ces règles commerciales et au nom de la protection des petits inventeurs et producteurs de biens consommables, sont défendus les intérêts de grandes multinationales (industries cinématographiques et du disque, clubs de football pour les produits dérivés, fabricants de logiciels, laboratoires pharmaceutiques, groupes agro-alimentaires…) qui commercialisent les produits des premiers ou qui produisent elles-mêmes – ou font produire ou commercialiser par d'autres, lorsqu'il s'agit, par exemple, de marques qui vendent leurs noms – leurs marchandises. De ce fait, la défense de la propriété apparait comme une forme légalisée d'un monopole, et les produits fabriqués comme une rente légale que défendent ces grands groupes mondiaux en installant des barrières contre la concurrence légale (provenant d'acteurs intégrés) ou illégale (provenant d'acteurs de la marge). Dans ce dernier cas, sont visés, non seulement les fabricants qui transgressent les règles de la propriété intellectuelle en pratiquant un capitalisme sauvage, mais également tous les acteurs de la piraterie et de la contrefaçon qui distribuent leurs marchandises dans les marchés informels ainsi que les consommateurs de ces marchandises qui, par exemple, téléchargent gratuitement des films ou de la musique ; il en résulte une criminalisation de l'informalité. La répression de la transgression des règles commerciales, qui vise particulièrement la piraterie et la contrefaçon, s'effectue sans que jamais la question des marges commerciales des groupes monopolistiques ne soit posée, faisant ainsi primer les lois du marché (les lois de la concurrence) sur ce qui pourrait être une éthique du commerce : telle est la raison pour laquelle les acteurs de l'informel revendiqueront une transgression sociale et légitime des lois du commerce.

D'un côté, c'est au nom du droit démocratique à la consommation pour tous (de produits ludiques, de consommation courante ou de médicaments) que les activités de piraterie et de contrebande sont justifiées et légitimées par leurs promoteurs et bénéficiaires, tandis que d'un autre côté, elles sont condamnées au nom du respect de la loi et de la défense de l'emploi par les grands groupes qui en sont victimes – ces mêmes grands groupes n'hésitant

[4] L'internationalisation de la brevetabilité du vivant a été reconnue en 1994 par l'OMC dans le cadre des accords sur les aspects des droits de propriété intellectuelle touchant au commerce (Adpic). Cependant, la Convention sur la diversité biologique (CDB), adoptée en 1992, affirme la prévalence de la souveraineté des États sur leurs ressources biologiques et, notamment, sur l'utilisation des ressources génétiques, ce qui permet aux Etats d'interdire les OGM ; l'industrie américaine des biotechnologies s'oppose à ces principes, et incite les États-Unis à ne pas ratifier la Convention sur la diversité biologique.

pas à transgresser la loi par des pratiques de bio-piraterie[5], d'espionnage industriel, de fraude fiscale ou de non-respect de la législation du travail, ainsi qu'à mettre l'emploi national en péril en délocalisant leurs usines. A l'heure actuelle, les activités de fabrication de produits de contrefaçon ou de commercialisation de marchandises de contrebande répondent à un tel accroissement de la demande qu'elles sont devenues très lucratives ; de ce fait, elles ont tendance à se développer à un niveau industriel et à une échelle mondiale, certaines d'entre elles ayant même été appropriées par des organisations criminelles transnationales qui disposent d'une maîtrise des routes parallèles déjà utilisées pour d'autres trafics[6]. Ici encore, le rôle des Etats est déterminant, selon que les détenteurs du pouvoir officiel choisiront de privilégier le respect de lois nationales protégeant un commerce mondialisé dont les acteurs sont multinationaux, ou un objectif national de pacification des rapports sociaux dont les acteurs sont locaux ; dans ce dernier cas, la répression des transgressions se fera d'une manière sélective, sur la base d'arrangements réciproquement intéressés et favorisant certains acteurs de l'informel alliés du pouvoir, et au détriment des acteurs économiques multinationaux ; les illégalités du secteur informel seront donc tolérées car celui-ci apparaît comme un amortisseur social de la pauvreté, comme pouvant produire des bénéfices

---

[5] Ainsi, dans les années 1990, des substances et plantes en provenance d'Inde et d'Amérique latine ont été brevetées aux Etats-Unis malgré que leurs vertus traditionnelles, notamment médicinales, étaient connues de longue date dans ces pays et régions. Alors que les Etats-Unis et le Japon refusent de modifier le système d'attribution des brevets et que d'autres pays (Norvège, Suisse, Union européenne) plaident pour une sanction administrative et non pour une révocation des brevets, les communautés spoliées réclament la révocation des brevets issus de la bio-piraterie et une protection de leurs savoirs traditionnels au nom du droit des minorités et, notamment, de la reconnaissance des droits des peuples autochtones et de leurs droits coutumiers.

[6] La plupart des analystes s'accordent pour affirmer que les activités informelles auraient représenté, en 2000, 41 % du PNB dans les pays en développement, 38 % dans les pays en transition et 18 % dans les pays de l'OCDE ; sur le territoire de l'UE, les pays les plus touchés sont l'Italie et la Grèce où les activités informelles seraient proches de 30 % du PNB, soit le double de ce qu'elles représentent en France et en Allemagne (cf. *Le Monde de l'économie* du 15 novembre 2011). Il faut noter la criminalisation des activités illégales, telle qu'elle apparaît, par exemple, dans un rapport (Rand Corporation, *Film Piraty, Organized Crime and Terrorism*, mars 2009) qui va jusqu'à assimiler la contrefaçon à une activité qui financerait le terrorisme et qui serait le fait d'organisations criminelles l'ayant ajouté à leurs activités traditionnelles (trafics d'armes et de stupéfiants, prostitution, racket…). Selon ce rapport, le piratage de disques (CD, DVD) produirait des marges bénéficiaires supérieures au trafic de drogue et comporterait peu de risques. La fabrication et la vente de disques piratés serait particulièrement développée en Bolivie, Brésil, Chine, Colombie, Indonésie, Kazakhstan, Koweït, Lituanie, Malaisie, Pakistan, Roumanie, Russie et Ukraine. Selon l'OCDE, le marché des produits contrefaits représentait, en 2005, 200 milliards de dollars et selon la Motion Picture Association (MPA, l'organisme représentant les studios américains), les pertes mondiales de l'industrie du cinéma s'élèveraient à 18 milliards de dollars (sur un chiffre d'affaires de 400 milliards), imputables à 60 % aux DVD pirates et à 40 % au téléchargement en ligne (cf. *Le Monde* du 27 mars 2009). La piraterie concernerait principalement les marchandises suivantes : CD et DVD, accessoires, chaussures, vêtements, programmes informatiques, parfums, jouets, médicaments, cigarettes... En France, la contrefaçon est passible de six mois de prison et de cinq millions d'euros d'amende. Au Mexique, en 2006, fut signé un Accord national contre la piraterie à travers lequel le gouvernement s'engageait à démanteler les organisations criminelles qui contrôleraient la contrefaçon et à diminuer ainsi la vente de produits illégaux ; cet accord était fondé sur la collaboration entre secteurs public et privé ; mais, en 2009, l'Institut pour la protection de la propriété industrielle et du commerce légal (IPPIC) faisait publiquement le constat que cet accord n'avait pas empêché le développement de la piraterie car le gouvernement n'avait pas favorisé la coordination entre Etats fédérés et municipes et ne s'était rapproché ni des gouvernements étrangers, ni des organismes internationaux qui luttent contre la piraterie ; de plus, selon le ministère de la justice mexicain (PGR), seuls 3 % des enquêtes préliminaires portant sur la piraterie se traduiraient par une condamnation à la peine prévue par la loi, soit 3,5 années de prison (cf. *Reforma* du 22 juillet 2009).

politiques électoraux ou comme source d'enrichissement personnel pour des représentants élus ou des fonctionnaires corrompus. C'est ainsi que les règles du clientélisme et celle du « *chacun pour soi* » se trouveront privilégiées par rapport à celles d'un Etat de droit mis au service des lois du marché et à qui ce dernier demande une stricte application de la loi.

Il en résulte que les normes commerciales, à travers les règles de la propriété intellectuelle, aboutissent à reréglementer le commerce mondial auquel les lois du marché avaient imposé une diminution des barrières douanières. Cette rerèglementation bénéficie principalement aux grands groupes multinationaux qui jouent sur les deux tableaux : la libre circulation des marchandises liée à la dérèglementation douanières, et la protection de leurs monopoles à travers des règles de la propriété industrielle qui brident la concurrence et s'opposent aux lois du marché. La réglementation par la propriété intellectuelle consiste donc à substituer des barrières légales mondiales à des barrières physiques nationales ; en se fondant sur un prohibitionnisme excluant toute prise en compte des besoins sociaux de consommation, elle aboutit à une généralisation des transgressions et à une tolérance de ces dernières de la part des Etats qui se retrouvent débordés par des pratiques sociales de transgression légitime et par des trafics qui répondent à une demande sociale. Le prohibitionnisme appliqué au commerce mondial contre la piraterie produira-t-il les mêmes effets que lors de son application à la production et à la consommation de cannabis, c'est-à-dire un échec à empêcher la consommation et une recrudescence des trafics, ou les Etats profiteront-ils de cette prohibition pour se renforcer ?

Toujours est-il qu'aujourd'hui, la piraterie est (à) l'ordre du jour. Le « pavillon noir » des pirates aurait déclaré la guerre au monde entier et les ordres économique, politique et juridique en seraient menacés. Pourtant, certains auteurs soutiennent que les organisations pirates sont inséparables du capitalisme ; en tant que marge du centre, les organisations pirates seraient donc indissociables du centre[7]. Considérées sous un autre angle, certaines organisations pirates, structures souples indépendantes, fédérées en réseaux et situées à la marge du système, peuvent également apparaître comme des organisations de contre-pouvoir ; de plus, en occupant une zone grise, elles seraient en mesure de contester ce que les Etats décrètent comme légitime (la loi, les réglementations, la propriété, les monopoles des multinationales, les secrets d'Etat, les profits non partagés) et de contribuer à l'invention de nouvelles normes ; ce faisant elles apparaîtraient comme les véritables défenseurs de la liberté et de la concurrence, profitant du fait que cette dernière opère sur un marché ouvert ; ainsi en serait-il, par exemple, des cyber-pirates. Pour lutter contre les organisations pirates, les organisations légales vont avoir tendance soit à conclure des pactes avec elles (la France

[7] Cf. Rediker (Marcus) & Linebaugh (Peter), *L'Hydre aux mille visages. L'Histoire cachée de l'Atlantique révolutionnaire*, Paris, éd. Amsterdam, 2008. Cf. également Durand (Rodolphe) & Vergne (Jean-Philippe), *L'organisation pirate*, Paris, Editions Le Bord de l'Eau, 2010.

utilisant les corsaires pour s'opposer au commerce maritime des Anglais, la Hollande armant des navires corsaires pour s'opposer à l'Espagne qui les considérait comme des navires pirates, le Pentagone traquant les hackers pour les embaucher ensuite, les multinationales du textile écoulant leurs produits sur les marchés informels du Mexique pour se défaire de leur stocks ou pour éliminer les produits locaux en cassant les prix), soit à les criminaliser en les faisant passer pour des bandits qu'il faut réprimer (les cyber-pirates qui divulguent les télégrammes diplomatiques américains, les producteurs de disques pirates, les pirates maritimes). Entre les pirates et les représentants de la loi, le jeu continue donc, chacun se référant à ses propres normes pour justifier son action. Qui sont les acteurs de ce nouveau mode de piratage ? Quelles sont leurs stratégies de légitimation et de pénétration des systèmes de pouvoir ? Quelles sont les interactions qui les relient entre eux ? Quelles sont les normes auxquelles ils se réfèrent de part et d'autre de la loi ? Et que révèlent-ils quant à la structure des systèmes politiques vis-à-vis desquels ils se situent et quant à l'avenir de nos sociétés ? Telles sont les principales questions abordées dans ce texte.

1. Des acteurs qui contribuent à l'établissement d'un Etat sécuritaire

La notion de cyberespace correspond à une vision idéale du futur : celle d'un monde libertaire pacifié (le « village global » de McLuhan), où les connaissances et le savoir seraient partagés et qui serait libéré de toute contrainte financière et de toute censure étatique ; on assisterait donc à une redistribution vers les individus des pouvoirs détenus naguère par les Etats et les institutions : pouvoirs de communiquer, de savoir, d'informer, de comparer, de décider... Mais avec l'abolition de l'espace, les acteurs de ce nouveau monde virtuel ont tendance à s'affranchir des règles du monde réel, ce dernier étant traditionnellement fondé sur la distinction privé-public ainsi que sur la notion de territoire ; le territoire qui se conçoit comme un espace à conquérir, à contrôler et sur lequel les Etats exercent leur puissance et leur souveraineté, est aujourd'hui mondialisé et connecté, ce qui implique qu'il se trouve partagé entre les Etats, les individus et les opérateurs de réseaux (fournisseurs de services), ces derniers l'investissant afin d'assurer leur domination commerciale en direction des usagers-consommateurs de services. Ce territoire qui était l'enjeu des guerres traditionnelles de conquête ou d'influence exercées par les Etats ou des groupes révolutionnaires peut-il être aujourd'hui l'enjeu d'une nouvelle guerre numérique qui reviendrait à une démocratisation du pouvoir de faire la guerre ?

Perturbant l'organisation traditionnelle des pouvoirs, le monde du cyberespace s'est complexifié et se trouve maintenant aux mains de quatre acteurs principaux : 1) la majorité des utilisateurs qui réclament son affranchissement en dehors de toute censure, 2) les Etats qui s'efforcent de réglementer pour conserver le monopole de l'information, protéger les données d'attaques susceptibles de déboucher sur de l'espionnage informatique contre les

administrations ou les entreprises nationales ou sur des pratiques de cyber-terrorisme et de cybercriminalité, 3) les entreprises privées légales (détentrices de brevets, de savoir-faire ou de données pouvant intéresser des assaillants et, donc, vulnérables au vol de propriété intellectuelle ou au cyber-espionnage) ou illégales (distribuant des marchandises de contrefaçon, par exemple) qui profitent du cyberespace pour stocker leurs données, créer de nouvelles valeurs basées sur le commerce informatique ou commercialiser des supports informatiques de plus en plus sophistiqués, certaines de ces activités étant régies par le secret, 4) les rebelles (des hackeurs) qui l'utilisent pour s'attaquer à l'autorité des Etats et de leurs représentants ainsi qu'aux entreprises, ces dernières reconnaissant difficilement qu'elles ont fait l'objet de cyberattaques pour ne pas afficher leur vulnérabilité [8]. Face à ces rebelles, les entreprises commerciales sont en demande de régulation protégeant leurs intérêts et les Etats sont amenés à réglementer, à se protéger ou à contre-attaquer par la mise en place d'un cyber-armement, sorte de quatrième armée recrutant des cyber-détectives, professionnels du chiffrement, qui travaillent à détecter les attaques, à perpétrer eux-mêmes des attaques pour le compte des Etats qu'ils représentent ou à alerter les cibles potentielles dont les données informatiques stockées ne sont pas bien verrouillées et qui risquent d'être touchées par l'espionnage industriel informatique ; les Etats agissent directement, soit en réglementant, soit

[8]. Les hackeurs, qui pratiquent le piratage informatique, étaient à l'origine des programmateurs avides de manipuler les machines pour mieux les comprendre et les améliorer. La culture du hacking s'est ensuite progressivement transformée pour favoriser l'ouverture, le partage, l'accès libre à l'information et la défiance envers les autorités, notamment celles qui imposent des obstacles physiques et édictent des lois tendant à limiter ou à réprimer les libertés en général et la liberté de pirater en particulier. Quant aux autorités, elles ont tendance à considérer les hackeurs comme des cyber-délinquants difficiles à réprimer car la plupart de leurs actions collectives en réseau sont dénuées d'organisation et de direction centralisée. Trois grandes périodes ont marqué l'histoire du hacking : 1) les années 1950-1960 au cours desquelles l'information libre est érigée en idéal absolu ; les années 1960 qui ont connu la miniaturisation et la démocratisation de l'accès à l'ordinateur ; les années 1980 qui ont vu certains hackeurs entrer dans le monde de l'entreprise (notamment les fondateurs d'Apple et de Facebook) (cf. Steven Levy, L'Ethique des Hackeurs, Paris, Editions Globe, 2013). L'une des actions les plus spectaculaires de piratage informatique aura été celle de Wikileaks, association à but non lucratif créée en 2006 comme un lanceur d'alerte et dédié à la publication, par son site Web, de documents et d'analyses politiques et sociétales à partir de fuites et de piratages d'informations gouvernementales secrètes, tout en protégeant ses sources et en référence à la liberté d'expression et de diffusion par les médias ; sa justification est d'œuvrer à l'amélioration de l'histoire commune et au respect du droit de chaque personne de créer l'histoire, principe contenu dans l'article 19 de la Déclaration universelle des droits de l'homme ; sur ces bases, en 2010, WikiLeaks a publié une vidéo de l'armée américaine montrant deux photographes de Reuters, tués par un hélicoptère Apache, lors du raid aérien du 12 juillet 2007 à Bagdad ; cette publication a marqué le début de la célébrité mondiale du site ; en 2010, utilisant cinq journaux de grande audience comme relais, WikiLeaks commence la révélation de plus de 250 000 télégrammes de la diplomatie américaine ; selon le New York Times, ces notes * offrent un panorama inédit des négociations d'arrière-salle telles que les pratiquent les ambassades à travers le monde +, alors que d'autres acteurs (gouvernements, institutions internationales) condamnent cet acte, notamment parce que le fait divulguer au public les informations que contiennent les documents serait dangereux pour les relations internationales entre les Etats, la diplomatie ne pouvant fonctionner qu'à partir du secret ; en 2011, WikiLeaks a mis en ligne 391 832 documents secrets sur la guerre en Irak, portant sur une période du 1er janvier 2004 au 31 décembre 2009, et révélant, notamment, que la guerre avait fait environ 110 000 morts pour cette période, dont 66 000 civils, et indiquant que les troupes américaines auraient livré plusieurs milliers d'Irakiens à des centres de détention pratiquant la torture. Toutes ces actions et d'autres encore ont conduit les autorités des Etats-Unis et leurs alliés à présenter le fondateur de Wikileaks (Julien Assange) comme un ennemi de la nation américaine et à le neutraliser arbitrairement.

en profitant de l'absence d'encadrement légal[9], ou indirectement, en sous-traitant leurs activités d'espionnage informatique à des prestataires privés (des sociétés de services en ingénierie informatique, SSII, ou des fournisseurs de services informatiques comme Dell, par exemple) qui mettent leurs capacités en matière d'intelligence économique au service de la sécurité nationale et des agences de renseignements. Les frontières terrestres et légales ont donc été remplacées par des cyber-frontières à l'intérieur desquelles l'objectif de la cyber-défense est d'assurer la sécurité informatique, le risque étant que des hackeurs (individuels, étatiques ou salariés de sociétés privés) soient capables de violer les réseaux informatiques non seulement des particuliers (atteintes à la vie privée), mais également des administrations (et, notamment, les plus sensibles comme la défense nationale ou les services de renseignement), des entreprises travaillant pour des secteurs stratégiques (armement, pétrole, électricité, téléphonie, banque, médias), ou qu'ils puissent perturber les réseaux électriques, affectant ainsi l'ensemble des infrastructures d'une ville, d'une région ou d'une nation.

C'est ce qui justifierait que, depuis le 11 septembre 2001, dans de nombreux pays, même démocratiques, au nom de la lutte contre une supposée menace terroriste internationale (terrorisme islamiste, trafiquants de drogue, cyber-terroristes), a tendance à s'imposer un renforcement des politiques nationales de sécurité publique et une limitation des libertés individuelles et publiques allant de pair avec une criminalisation des mouvements sociaux pacifiques d'opposition aux gouvernements et avec la mise en place de ce qu'on pourrait appeler un Etat sécuritaire. C'est ainsi que les démocraties d'Europe et d'Amérique en arrivent à porter atteinte à l'un des fondements de leur identité politique : la défense des libertés individuelles[10] ; cette évolution se produit lorsque, au nom de la lutte contre le terrorisme, elles adoptent des dispositifs préventifs et répressifs qui seront ensuite étendus à la criminalité de droit commun (la guerre contre la drogue au Mexique, par exemple) puis à l'ensemble de la société civile. Une telle évolution apparaît également comme une réponse à un objectif de société sans risque, et donc sans crime, qui serait, en fait, la transposition du principe de précaution du droit de l'environnement au droit pénal[11]. Il s'agirait bien d'un

---

[9] Ainsi en est-il des services secrets français, placés sous la coupe du ministère de la Défense, dont les fonctionnaires affectés à l'étranger, au nom de la lutte contre le terrorisme, espionnent les flux de trafic internet entre la France et l'étranger, en dehors de tout contrôle administratif et de tout ciblage thématique, interceptant ainsi des informations relevant de la vie privée ; ces informations sont transmises à d'autres services de l'Etat. Parce que les centres d'hébergement des sites qui espionnent sont basés à l'étranger, ils ne relèvent pas de la loi française, ce qui confère à cet espionnage perpétré par des agents de l'Etat un caractère d'illégalisme (cf. *Le Monde* du 12 juin 2013).

[10] Selon l'Observatoire pour la protection des défenseurs des droits de l'homme (création conjointe de la Fédération internationale des droits de l'homme et de l'Organisation mondiale contre la torture), en 2006, on a assisté au renforcement de la tendance des Etats à avoir recours à l'arsenal législatif, notamment antiterroriste, pour restreindre les libertés d'association, d'expression et de rassemblement pacifique (cf. *Le Monde* du 16 mars 2007).

[11] Cf. Delmas-Marty (Mireille), *Liberté et sûreté dans un monde dangereux*, Paris, Le Seuil, 2010. L'auteur décrit deux mécanismes récents qui limitent les libertés publiques : 1) la déshumanisation du droit pénal qui se manifeste par la mise sous surveillance ou l'internement-emprisonnement (à travers l'accroissement du nombre de gardes à vue, par

changement de régime et de paradigme qui avait été décrit par Gilles Deleuze en 1990, remarquant que l'on était de train de passer des sociétés disciplinaires des XVIII^{e}, XIX^{e} et début du XX^{e} siècles dominées par le modèle des lieux d'enfermement (école, prison, famille...) aux sociétés de contrôle, plus libres, ouvertes et fluides, mais où les individus et les groupes sont transcrits et réduits au langage numérique[12]. Une telle méthode de mise sous surveillance, de mise en norme et de mise en fiche des populations et des individus est elle-même récupérée par le marqueting qui va établir un profilage des individus et une anticipation de leurs comportements en évaluant, stockant et croisant leurs goûts, leurs habitudes de consommation et leurs situations (à partir de leurs comptes bancaires, de leurs dossiers médicaux, de leurs dossiers scolaires, de leurs connexions internet à des moteurs de recherche...). Les bases de données qui seront ainsi constituées, stockées, échangées et commercialisées constitueraient le cœur de la nouvelle société de surveillance[13]. Cette société de contrôle ou de surveillance contrevenant au *principe de libre-arbitre* apparaît comme la contrepartie d'une nouvelle forme d'Etat : l'Etat sécuritaire.

Dans l'Etat sécuritaire, l'objectif d'ordre public prend le pas sur celui d'intégration sociale. Le social constituerait en effet la principale menace susceptible de remettre en cause l'ordre socio-politique établi. Cette menace est individualisée et généralisée dans la mesure où chaque individu est potentiellement coupable de remettre en cause l'ordre établi. La surveillance doit donc être totale et, pour cela, s'appuyer non seulement sur des méthodes traditionnelles de fabrication d'ennemis, de stigmatisation-amalgame de groupes sociaux (l'ultra gauche anarchisante assimilée à des terroristes, les musulmans assimilés à des islamistes, les lanceurs d'alerte catalogués comme des traîtres à la patrie, les étrangers assimilés à des envahisseurs ou à des trafiquants de drogue, les cultivateurs et consommateurs de drogue assimilés à des trafiquants de drogue, les trafiquants de drogues assimilés à des terroristes transnationaux, les délinquants de quartier assimilés à des criminels internationaux...) et de mesures arbitraires collectives et préventives (la systématisation des gardes à vue pour outrage et rébellion vis-à-vis des forces de l'ordre, les contrôles policiers au faciès, les fouilles répétées et systématiques dans les quartiers sensibles de banlieue, dans les aéroports), mais également sur des techniques nouvelles : la génétique, la biométrie, la surveillance par satellites, la vidéosurveillance, les fichages (par exemple, ceux effectués par les compagnies aériennes sur leurs clients, sans leur consentement), le traçage des individus

---

exemple) d'individus ou de groupes au seul motif de leur dangerosité potentielle, et 2) la radicalisation des mesures de contrôle social perceptible B travers la généralisation des fichiers et des bases de données personnelles ainsi que leur interconnexion.

[12] Cf. Deuleuze (Gilles), *Post-scriptum sur les sociétés de contrôle*, in L'autre journal, n°1, mai 1990.

[13] Cf. Sadin (Eric), *Surveillance globale*, Paris, Climats, 2009. Cf. également la revue Multitude, *Big Brother n'existe pas, il est partout*, Paris, éd. Amsterdam, 1990.

grâce aux télécommunications, l'espionnage informatique. L'Etat moderne atteint ainsi son apogée lorsque l'objectif de sécurité est à la fois centralisé, individualisé, diffus, généralisé et banalisé.

De plus, dans l'Etat sécuritaire, les objectifs de maintien de l'ordre public et de protection des personnes et des pouvoirs se substituent à celui de respect du droit des personnes. En effet, l'Etat sécuritaire défait la sécurité juridique qui découlait d'un contrat social primitif ayant fondé les rapports politiques modernes sur la décision communautaire de vivre ensemble selon des règles et des lois communes ; ce contrat social, fondé sur un peuple déléguant à une autorité politique gouvernementale la mission de garantir aux hommes d'être libres, égaux, solidaires et que soit respectée leur propriété, fruit de leur travail, s'opposait à un état de nature (la loi du plus fort) se caractérisant par une égalité passive face au malheur, à la persécution et à la menace. C'est sur la base de ce contrat social que pourrait se développer une « gouvernementalité sécurisante » alternative fondée sur des lois publiques applicables à tous, sur une justice indépendante et sur un Etat garantissant le respect de la liberté, de l'égalité, de la laïcité, de la protection des droits sociaux... Au lieu de cela, c'est une « gouvernementalité sécuritaire » qui a tendance à s'imposer, fondée sur la surveillance policière, l'exception devenue règle (état d'urgence, couvre-feu pour les jeunes), la remise en cause des droits fondamentaux des individus (à travers les contrôles d'identité systématiques au faciès, les entraves à la liberté de circulation et au droit à l'intimité...) et qui a pour objectif, d'assurer un ordre public limité à la sécurisation des biens, des territoires et des personnes[14]. C'est ainsi que, de minoritaire, la menace contre l'ordre public (re)devient sociale, aboutissant à une socialisation et à une collectivisation-individualisation de la menace. L'espionnage électronique pratiqué par les Etats est révélateur de cette évolution vers un Etat sécuritaire.

2. L'espionnage électronique comme pratique de pouvoir

Comme exemple de réglementation, il est possible de citer le Patriot Act, sorte de loi d'exception votée par le Congrès des Etats-Unis au lendemain des attentats du 11 septembre 2001 et qui permet au FBI, à la CIA et au NSA (National Security Agency) d'accéder aux données personnelles stockées sur les serveurs de tous les organismes publics ou privés de nationalité américaine, comme les fournisseurs d'accès à internet (Microsoft, Google), mais également les fabricants d'ordinateurs ou de logiciels (Microsoft, Apple [15]), les opérateurs

[14] Cette distinction entre différents types de gouvernementalité est reprise de l'analyse foucalienne opérée par Gros (Frédéric) in *Le dernier âge de la sécurité*, Paris, Gallimard, 2011.

[15]. En septembre 2012, Antisec, l'un des groupes appartenant à la mouvance Anonymous, a mis en ligne un fichier de plus de 12 millions de dossiers individuels d'utilisateurs d'iPhone et d'iPad qu'il affirmait avoir volé au FBI ; ces dossiers contenaient le numéro d'identification de l'appareil, la clé permettant de lui transmettre des messages de service, le nom choisi par son possesseur ainsi que les coordonnées physiques de ce dernier (identité, adresse, numéro

téléphoniques (Verizon) ainsi que les fournisseurs de commerce en ligne (Amazon) ou de réseaux sociaux (Facebook, Twitter)[16], et cela sans aucun contrôle judiciaire, sans en référer aux personnes visées et en ciblant des personnes dans le monde entier (extra-territorialité)[17]. Les Etats sont de plus en plus nombreux (Allemagne, Grèce, Grande-Bretagne, Russie, Irlande, Singapour, Norvège) à vouloir se prémunir de la super-puissance américaine en matière de transferts de données informatiques en mettant en place des serveurs nationaux qui permettent de tracer des frontières nationales dans les nuages ; tel est l'objectif du *cloud computing* qui consiste, pour des entreprises (publiques ou privées, mais en majorité anglo-saxonnes) à louer à des clients (particuliers, administrations, entreprises) des espaces protégés de stockage d'informations numériques ; mais ces espaces protégés sont toujours susceptibles d'être confrontés à des intrusions externes visant à l'exploitation de leurs données (*data mining*) à des fins d'espionnage militaire ou industriel[18].

Dans les temps de l'après guerre froide, les services d'espionnage sont de plus en plus en quête d'informations qui relèvent moins du militaire ou de l'opérationnel que du politique, de la finance internationale, du commerce, de l'industrie et de la haute technologie. En accordant une place déterminante à l'action secrète, l'espionnage se pose comme l'une des clefs de l'Histoire, ce qui conduit à interpréter les événements en termes de complot et à considérer que les hommes de l'ombre peuvent changer le cours de l'Histoire ; l'idéologie qui guide ces pratiques s'applique autant aux relations internationales (dans les domaines géopolitiques et commerciaux[19]) qu'aux interactions entre le centre et la marge des systèmes

---

de téléphone), autant d'éléments qui permettraient à un expert informatique d'intercepter les historiques de communication et de messageries de l'appareil ou à un Etat disposant d'importants moyens logistiques de mettre en place un système de surveillance de masse de millions d'utilisateurs (cf. *Le Monde* du 9-10 septembre 2012).

[16] En 2010, un procureur fédéral américain enquêtant sur la publication par Wikileaks de documents secrets du gouvernement américain, a exigé de plusieurs prestataires internet américains qu'ils lui livrent secrètement les données de connexion de certains collaborateurs de Wikileaks ; la société Twitter qui avait refusé d'obéir à cette injonction a été contrainte de s'incliner en 2011, suite à la décision, faisant jurisprudence, d'une juge fédérale américaine affirmant que toutes les données personnelles collectées par un service internet américain étaient placées sous la juridiction des Etats-Unis, même si l'utilisateur est étranger et se connecte depuis un autre pays. En 2012, un tiers des serveurs informatiques dans le monde étaient localisés aux Etats-Unis (cf. *Le Monde Economie* du 23 octobre 2012).

[17] Dans le but de légaliser la surveillance secrète des réseaux dans et hors des Etats-Unis, décidée en 2001, une nouvelle législation extraordinaire à portée extraterritoriale a été votée par le Congrès américain en 2008 (le Foreign Intelligence Surveillance Act Amendment Act, Fisaaa) qui autorise la surveillance des communications civiles et militaires des citoyens, entreprises et administrations non américains pour les cas non seulement de terrorisme ou de grande criminalité, mais également, à des fins d'espionnage politique, économique et personnel. Quant aux communications téléphoniques des Américains sur leur territoire, le Patriot Act de 2001 avait imposé aux opérateurs téléphoniques de transmettre au FBI et à la NSA les relevés détaillés d'appel de leurs abonnés sur tous les appels téléphoniques émis depuis les Etats-Unis ou passés aux Etats-Unis depuis l'étranger.

[18] La loi américaine Fisaaa de 2008 a autorisé l'extension de la surveillance électronique à toutes les données présentes sur le *cloud* dont les fournisseurs américains (Coogle, Microsoft, Amazon, Apple...) sont tenus d'installer des systèmes permanents destinés à scanner toutes leurs données et à les dériver vers la NSA (cf. *Le Monde* du 2 juillet 2013).

[19] Il est très difficile de distinguer ce qui relève de l'ordre de la puissance géopolitique et ce qui concerne la domination économique, d'abord parce que la seconde contribue au renforcement de la première et, ensuite parce que, maintenant, les moyens des services secrets sont mis au service de la conquête de marchés. C'est ce qui a été révélé

politiques, le trafic de stupéfiants et la lutte contre le terrorisme étant maintenant devenus les principaux enjeux des relations internationales qui légitiment la mise en œuvre de moyens d'espionnage informatique à l'échelle planétaire ; ce type d'espionnage, lorsqu'il est détourné à des fins de puissance, s'avère attentatoire aux libertés publiques et à la protection des données privées, et délégitime les démocraties en les faisant apparaître comme des systèmes politiques usant de méthodes totalitaires de surveillance des populations ainsi que des gouvernements et des institutions étrangers[20].

La fiction littéraire et le goût partagé de l'aventure entretiennent la légitimité de ces affrontements en coulisse et permettent de masquer leur idéologie sous-jacente, leurs fréquents débordements ou implications sur les populations civiles ainsi que la tricherie et la duplicité qui constituent leur fondement et peut contribuer à les rendre contre-productifs pour les entreprises ou les Etats qui en sont victimes. Cette menace contre la société a tendance à s'accroître du fait qu'aujourd'hui, l'espionnage clandestin s'est recentré sur l'acquisition de gains de savoir, à des fins civiles ou militaires, par le vol de documents, l'interception de communications ou la corruption d'agents publics ou privés, en faisant l'économie des études, des recherches, du temps et des financements (en hommes, en compétence et en matériels) qui sont à la base des progrès technologiques ; il en résulte que le renseignement technique, du fait des enjeux financiers et technologiques qui lui sont liés, est devenu maintenant un risque

---

lors de la découverte (en 2000) du réseau d'espionnage Echelon, système d'écoute planétaire conçu pendant la guerre froide et contrôlé quasi exclusivement par la National Security Agency (NSA) américaine et qui comprend des stations aux Etats-Unis, en Grande-Bretagne, au Canada, en Nouvelle-Zélande et en Australie ; servant à l'origine pour un usage militaire, ce réseau a été reconverti dans l'interception et l'exploitation des communications de toute nature, y compris privées, au profit d'entreprises anglo-saxones ; basé sur l'imbrication, de longue date, entre les services de renseignement américains et de Grande-Bretagne, il ne va pas sans poser des problèmes d'alliances puisque la Grande-Bretagne aide à ce que soient espionnés les grands groupes industriels de l'UE au profit de ceux des Etats-Unis alors qu'elle appartient à l'UE ; en effet, selon Le Monde du 10 mars 2000, il existerait au secrétariat au commerce américain un Office of Intelligence Liaison (OIL) qui reçoit les dossiers de la NSA et communique les analyses qu'ils contiennent à de grands groupes industriels américains (Boeing, Lockheed, Loral, TRW, Raytheon...) ; alors que les Européens (sauf la Grande-Bretagne) considèrent ces écoutes à caractère économique comme un danger en matière de libertés publiques et individuelles, les Américains les justifient en arguant qu'elles servent à lutter contre les entreprises qui rompent les embargos internationaux, qui développent des technologies duales (militaro-civiles) ou qui versent des commissions indues à leurs clients. En 2006, l'affaire Swift (du nom d'une entreprise basée dans la banlieue de Bruxelles), a montré que les Américains (la CIA et le Trésor), sous prétexte cette fois de lutte contre le terrorisme avaient espionné pendant des années les transactions bancaires mondiales en violation des règles sur la protection des données. Pour ce qui concerne la surveillance des réseaux téléphoniques et électroniques, les Etats-Unis classent les pays en deux grandes catégories : les *Five Eyes*, c'est-à-dire eux-mêmes et les "pays très proches" (Royaume Uni, Nouvelle Zélande, Australie, Canada) qui bénéficient d'un accès à un système sécurisé d'échange et de réception d'informations, et le reste du monde, composé des "pays cibles" de leur espionnage.

[20] Cf. le programme électronique américain Prism, développé par l'Agence nationale de sécurité (NSA) américaine, avec un objectif de lutte contre le terrorisme et qui avait pris pour cibles (installation de micros, infiltration du réseau informatique) non seulement les données informatiques des particuliers dans le monde entier, mais également les ambassades à Washington et les représentations à l'ONU des pays alliés des Etats-Unis, parmi lesquels la France, l'Italie, l'Allemagne, la Grèce, le Japon, le Mexique, la Corée du Sud, l'Inde, la Turquie... (révélations du *Guardian* du 30 juin 2013) ainsi que les bureaux de l'Union européenne à Bruxelles et de la mission diplomatique de l'UE à Washington (révélations de *Der Spiegel* du 29 juin 2013). Ces révélations furent fondées sur des documents obtenus par l'intermédiaire d'Edward Snowden, un lanceur d'alerte qui était employé par la NSA, considéré comme un traître par les Etats-Unis pour avoir dévoilé les pratiques illégales et anti-démocratiques de son gouvernement. Au moment de ces révélations, le président américain était en visite en Afrique du Sud et faisait l'éloge du combat politique de Mandela au service de la démocratie.

informatique pour l'ensemble de la société, ce qui est rendu évident par le fait que les services de renseignement peuvent disposer aujourd'hui des moyens techniques pour stocker massivement et mutualiser (au profit d'autres administrations ou services) les données techniques (les *métadonnées*) qu'ils ont collectées[21], ce stockage et cette mutualisation s'opérant clandestinement et sur la base d'un flou juridique qui autorise des pratiques en marge de la légalité et hors de tout contrôle[22]. Il en résulte une redéfinition des règles du droit pénal ; en effet, en matière pénale, il existe un principe fondamental qui est celui de *la présomption d'innocence*, c'est-à-dire le fait qu'*une personne est présumée innocente tant qu'elle n'a pas été reconnue coupable à travers une décision de justice* ; ce principe s'oppose au renversement de la charge de la preuve qui oblige l'accusé à prouver son innocence. Dans les Etats sécuritaires contemporains, le principe de la présomption d'innocence – de même que *le principe démocratique de l'intégrité inviolable de l'individu* qui fonde la liberté sur la distinction entre vie privée et vie publique – est légalement transgressé à travers la surveillance électronique des masses qui implique de traiter chaque citoyen comme un suspect potentiel ; cette surveillance qui tend à s'institutionnaliser à travers une collaboration entre les services de l'Etat et les sociétés privées d'internet, repose sur une dissymétrie de traitement par le fait qu'elle impose *la règle de la transparence* aux individus – piratage et stockage indéfini des communications et des données personnelles (feuilles d'impôts, itinéraires de vol, géolocalisation téléphonique) et, donc, négation de la vie privée, celle-ci étant portée à la connaissance de tous soit d'une manière consentie (facebook, par exemple), soit d'une manière automatique ou malveillante, chaque individu étant, à tout moment, potentiellement tenu de rendre compte de son passé qui ne lui appartient plus – tandis que les Etats et les entreprises continuent à fonctionner selon *la règle du secret*. Les services secrets, par nature coercitifs, ont donc accru leurs fonctions traditionnelles (la liquidation ou le retournement d'agents étrangers, la protection des secteurs de la défense et des ventes d'armes, l'espionnage des membres de gouvernements amis, alliés et ennemis, le retournement d'employés d'entreprises civiles étrangères concurrentes afin qu'ils livrent des secrets industriels et commerciaux), en se mettant au service de la guerre économique et des grands groupes exportateurs de leurs pays dans des secteurs stratégiques (aéronautique, informatique, biotechnologies...). Différentes affaires ont montré comment la guerre économique repose sur le développement

[21] Les métadonnées concernent non pas le contenu des messages (ce qui se dit, relevant de l'espionnage ciblé), mais leur contenant (qui parle, à qui, à quelle heure, combien de temps) qui est traité sous forme d'immenses graphes de liaisons entre personnes.

[22] Dans ce cas, la légalité supposerait, du moins en France, un contrôle exercé par une commission, que chaque demande d'interception soit justifiée, ciblée et limitée dans le temps, ce qui exclut toute interception massive. Mais, de toutes façons, toujours dans le cas français, cette commission n'aurait pas accès aux fichiers des services de renseignement. Ces données qui n'existent donc pas officiellement, car obtenues illégalement, pourraient même entrer dans une procédure judiciaire, à condition d'être présentées en tant que renseignements anonymes.

de certains illégalismes en impliquant des acteurs dont le recours à des pratiques illégales est toléré[23] ; dans ce dispositif, les services de renseignement sont un acteur intermédiaire pivot : le renseignement recouvre à la fois les services officiels d'intelligence économique et des officines privées qui pratiquent des actes illégaux pour détourner des informations et sont souvent dirigées par d'anciens policiers ou militaires disposant d'un réseau de relations leur permettant d'être protéger par leurs amis institutionnels ou politiques et de recruter dans les services de l'Etat afin de profiter du savoir-faire de ses agents[24].

Il en résulte une privatisation du renseignement, une banalisation des illégalismes d'Etat par la sous-traitance au privé ainsi que la formation de réseaux d'influence : les lobbies industriels financent les campagnes électorales des dirigeants politiques, et, en échange, ces derniers, une fois élus, "prêtent" les services secrets aux industriels, avec tous les risques de dérapage et que la guerre économique ne se transforme finalement en guerre militaire.

---

[23] La notion *« d'illégalismes »* permet à Foucault d'éviter le mot *« délinquance »*, trop couramment usité et faisant référence à une nature prédélinquante reconnaissable. Foucault utilisait le concept opératoire *d'illégalisme de droit* afin de qualifier les comportements transgressifs de la bourgeoisie dirigeante du XIX[e] siècle qui se donnait ainsi *« la possibilité de tourner ses propres règlements et ses propres lois… »* afin d'assurer une circulation économique dans les marges de la législation, marges prévues par ses silences, ou libérées par une tolérance de fait (fraudes fiscales par exemple). Selon Foucault, les illégalismes de droit sont distincts des *illégalismes de biens* qui font référence aux illégalismes commis par les classes populaires (rapines, vols, braconnage, etc.), tolérées durant plusieurs siècles par des autorités bienveillantes pour s'assurer l'allégeance de leurs serviteurs mis dans une situation d'obligés ; cette situation perdura en Europe occidentale jusqu'à la fin du XIX[e] siècle et l'avènement de la société bourgeoise capitaliste, période au cours de laquelle fut engagée une répression stricte de ces illégalismes. Toujours selon Foucault, cette distinction a entraîné une différenciation des circuits judiciaires : « *pour les illégalismes de biens, pour le vol, les tribunaux ordinaires ; pour les illégalismes de droit (fraudes, évasions fiscales, opérations commerciales irrégulières) des juridictions spécialisées avec transactions, accommodements, amendes atténuées, etc.* ». Cf. Foucault (Michel), *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, 1975. Comme illustration de la transposition des illégalismes foucaldiens au monde du Net, on peut prendre le cas français de l'espionnage de Greenpeace par EDF qui avait utilisé pour cela une société privée dirigée par un ex-agent des services de renseignement français, celle-ci ayant avait elle-même eu recours à un hackeur autodidacte afin d'effectuer un piratage informatique consistant en des intrusions illégales dans le système informatique de la victime (cf. Le Monde 18 octobre 2011). Les services secrets peuvent également avoir recours à des pratiques illégales directes en imposant aux opérateurs téléphoniques qu'ils leur fournissent des relevés de communication sans l'accord d'un juge, ce qui est également une pratique illégale (cf. en 2011, l'affaire des fadettes en France ayant consisté au détournement des relevés téléphoniques d'un journaliste du journal Le Monde pour découvrir son informateur ministériel). L'instrumentalisation politique des services secrets à des fins d'intimidation, de corruption ou de répression des opposants politiques en ayant recours à des méthodes illégales tolérées par le pouvoir politique est une pratique courante, même de la part de gouvernants issus d'élections pluralistes ; cf. les cas de l'Argentine de Menem, de la Colombie d'Uribe, du Pérou de Fujimori, de la Russie, du Pakistan...

[24] Ces agences privées de renseignement sont spécialisées autant dans les recherches internationales en matière de lutte contre la criminalité économique que dans la recherche d'actifs ; elles peuvent autant faire ou défaire une réputation qu'évaluer la fortune d'un riche mari volage. Elles emploient autant de jeunes cyber-informaticiens hackers et polyglottes que d'anciens policiers reconvertis ou des magistrats à la retraite. Le cabinet américain Kroll est parmi ceux qui sont les plus réputés. En Europe, Genève (lieu du négoce de nombreuses matières premières, siège de nombreuses multinationales et lieu de résidence de nombreuses grandes fortunes mondiales) est le siège de multiples sociétés d'investigation. En France, ces agences privées sont souvent noyautées et instrumentalisées par les services publics de renseignement (cf. *Le Monde* du 22-23 janvier 2012).

3. Les guerres des ondes

Les guerres du cyberespace sont donc aujourd'hui déclenchées ; l'Estonie a subi des cyberattaques en 2007, la Géorgie en 2008 et, en 2012, ce sont les centrales nucléaires iraniennes qui avaient été touchées par une offensive américaine ainsi que 30 000 ordinateurs de la compagnie pétrolière saoudienne Aramco, infectés par des virus venus d'Iran (selon les Américains) ; en 2013, des hackeurs chinois auraient pénétré les systèmes informatiques du Pentagone dans lesquels étaient stockés les plans de dizaines d'armements militaires cruciaux, dont des avions et des missiles. Il faut cependant distinguer divers acteurs pratiquant différentes formes d'illégalismes liés à l'utilisation des réseaux électroniques de communication : 1) les pirates qui utilisent le réseau mondial pour effectuer des échanges désintéressés et fausser les stratégies commerciales des grands groupes privés (exemple du téléchargement gratuit de musiques ou de films) et qui sont amenés à s'organiser autant en réseaux sociaux mondiaux (les Anonymous, le site Wikileaks) qu'en partis politiques (partis pirates représentés en Allemagne, Suède, Islande[25], République tchèque, Suisse...)[26], 2) les hackeurs individuels qui développent des stratégies "de résistance" face aux institutions étatiques ou entrepreneuriales (déverrouillage des protections, vol et diffusion de données confidentielles par des lanceurs d'alerte) ou face au système global de communication par internet (par injection de virus informatiques), mais qui peuvent également poursuivre des fins commerciales, par exemple en injectant des virus informatiques dans le réseau afin de vendre des antivirus (similitude avec le racket : "paye-moi pour te protéger de moi-même") ou en pénétrant dans les courriers électroniques pour les contaminer par de la publicité forcée (cookies), 3) les organisations criminelles informatiques transnationales qui emploient des hackeurs professionnels pour perpétrer des braquages de banques à l'aide d'ordinateurs et d'internet (au lieu d'armes et de masques) en pénétrant le système informatique de groupes bancaires et en piratant les numéros et les codes secrets de cartes magnétiques recodées[27] ou

[25] Fin 2009, l'Islande est assommée par la crise financière qui vient de ruiner le pays ; alors que la population cherche à comprendre, des journalistes locaux reçoivent un courriel leur conseillant de se connecter au site Wikileaks sur lequel ils découvrent des informations confidentielles, sûrement envoyées par un lanceur d'alerte employé d'une banque, prouvant que la crise financière a été provoquée par l'incompétence, la cupidité et la corruption des dirigeants des banques nationales ; malgré que ces derniers aient obtenu qu'un juge interdise aux médias locaux de diffuser les documents, tout le pays s'est néanmoins retrouvé au courant en quelques heures car internet, une fois lancé, échappe à tout contrôle. Ce fait a constitué une démonstration de la puissance potentiellement démocratique du réseau mondial ; par la suite, les gouvernements et les multinationales n'auront de cesse de museler ce réseau en le réglementant et en l'espionnant.

[26] Ces partis pirates ont en commun la défense de l'internet libre, ouvert et non surveillé ; leur programme politique, soutenu par une frange de la jeune génération internet qui renoue ainsi avec la politique, comprend : la libre circulation intégrale des données sur le Net, la réforme complète de la propriété intellectuelle, l'anonymat des connexions Web et l'utilisation des nouvelles technologies pour créer un système politique fondé sur la transparence de l'action publique et la démocratie participative.

[27] Cf. l'affaire, révélée le 9 mai 2013 par le bureau de la procureure de New York, concernant des pirates informatiques qui, quelques mois auparavant, avaient dérobé, en deux opérations, près de 45 millions de dollars à des

qui utilisent internet soit pour blanchir de l'argent provenant d'activités criminelles[28] ou pour financer des réseaux terroristes, 4) les Etats qui développent non seulement des pratiques de collecte de renseignement (espionnage), mais également des stratégies agressives visant à mieux contrôler le cyberespace afin d'asseoir leur puissance sur d'autres nations ou d'assurer leur domination sur leur propres populations par l'usage du hacking cyber-sécurité et cyber-opérations actives). Face à ces acteurs, on trouve les lanceurs d'alerte (les *whistleblowers*), des individus, employés ou fonctionnaires anonymes ou autodésignés qui, au nom de la transparence, décident d'alerter le public en dénonçant, preuves à l'appui, des actions illégales ou immorales commises par leur administration ou leur entreprise, s'exposant au risque de se retrouver accusés d'espionnage ou de haute-trahison (*felony*) par celles-ci et d'être sévèrement condamnés par les tribunaux, la sanction tombant alors sur celui qui dénonce les illégalismes et non sur celui qui les commet [29] ; leur action de contre-pouvoir ne peut être efficace que s'ils sont relayés par une presse ou des cyber-réseaux indépendants (comme le site Web WikiLeaks).

Le contrôle du cyberespace et de ses réseaux est donc devenu un enjeu dans les rivalités de pouvoir qui se superposent aux conflits géopolitiques traditionnels sur des territoires réels. Les conflits cyber-spatiaux, comme les conflits territoriaux, engagent des forces politiques, des Etats, des groupes d'intérêt économiques et des groupes sociaux

---

banques de différents pays, en s'appuyant sur un réseau de correspondants locaux répartis dans 26 pays ; en quelques heures, ces correspondants avaient retiré l'argent des distributeurs automatiques, ce qui suppose une organisation en cellules, secrète, efficace et rapide, afin de coordonner les opérations de terrain.

[28] Cf. l'affaire, révélée le 29 mai 2013, de la mise en accusation par la justice new-yorkaise de l'émetteur de monnaie numérique Liberty Reserve et de sept de ses responsables (arrêtés en Espagne, au Costa Rica et aux Etats-Unis), accusés d'avoir blanchi six milliards de dollars en sept ans pour plus d'un million de clients. Créée en 2006, et installée au Costa Rica, Liberty Reserve, premier réseau mondial de blanchiment d'argent sur le net, était une plate-forme de paiement électronique permettant à tout internaute d'envoyer de l'argent à n'importe qui ou d'en recevoir, n'importe où dans le monde, en dehors de toute réglementation ; ses services étaient utilisés dans 17 pays, dont le Vietnam, le Nigeria, la Chine, Chypre et les Etats-Unis ; la société prélevait 1 % d'honoraires sur chaque transfert effectué. Selon l'acte d'accusation, « *Liberty Reserve était devenue la plaque tournante financière de la cybercriminalité, facilitant un grand nombre d'activités criminelles en ligne, dont les fraudes à la carte bancaire, les vols d'identité, les investissements frauduleux, le piratage informatique, la pornographie infantile et les trafic de drogue* ». Les sociétés de transferts de fonds sur internet, en fort développement, utilisent des monnaies cybernétiques virtuelles qui alimentent des systèmes de paiement anonymes, décentralisés, réduisant les coûts des transaction et échappant au contrôle des banques ainsi qu'à toute forme de régulation ; leur anonymat favorise les transactions illégales.

[29] La référence des lanceurs d'alerte demeure Daniel Ellsberg qui, en 1971, alors qu'il appartenait aux services secrets américains, a provoqué une controverse politique nationale aux Etats-Unis quand il a fourni au New York Times les Pentagon Papers, soit 7 000 pages de documentation top-secrète appartenant au Pentagone, portant sur le processus décisionnel du gouvernement pendant la guerre du Vietnam et dénonçant les mensonges systématiques des différentes administrations destinés à justifier l'engagement américain ; son action a contribué à retourner l'opinion publique jusque là favorable à la guerre du Vietnam ; il a été poursuivi pour vol, conspiration et espionnage. Plus proche, il faut citer le cas de Bradley Manning qui, alors qu'il était analyste militaire de l'armée américaine, fut accusé d'avoir transmis à Wikileaks, en 2010, différents documents militaires classés secret défense afin de dénoncer les pratiques guerrières de l'armée américaine et de provoquer un débat public sur les guerres en Irak et Afghanistan ; ou encore le cas d'Edward Snowden, ancien agent de la CIA et ex-collaborateur de la NSA, qui, en 2013, transmit au Guardian et au Washington Post des documents montrant l'étendue planétaire de la surveillance et de l'espionnage exercés par la NSA à partir du piratage des structures de l'internet qui lui donnait accès à des centaines de milliers d'ordinateurs sans avoir à les pirater individuellement.

criminels ou de contre-pouvoir. Pour affirmer leur emprise, les Etats vont d'abord essayer d'imposer des régulations destinées à sécuriser leur territoire (établissement de frontières virtuelles par la censure ; repérage des groupes qui contestent le pouvoir ou les institutions) et à protéger leurs populations (contre, par exemple, les messages pornographiques intempestifs ou les sites pédophiles). Ces lois et ces réglementations vont à l'encontre des thèses que défendent les partisans de l'indépendance du cyberespace réunis au sein de l'association Electronic Frontier Foundation (EFF) ; cette association défend notamment l'ouverture, la neutralité et l'interopérabilité des réseaux. De ce point de vue, le cas de la Chine est exemplaire puisque ce régime a su anticiper les risques de la croissance d'internet, non en procédant à son interdiction complète, mais par le filtrage des informations à la source, par l'encadrement réglementaire et législatif des fournisseurs, par la surveillance des contenus des sites et la répression policière des internautes ne pratiquant pas l'autocensure et ne respectant pas la législation, les réglementations et les interdictions. De plus, le gouvernement chinois a su tirer parti d'internet pour diffuser sa propre propagande. L'ordre numérique est également pratiqué par d'autres Etats autoritaires comme les monarchies du Golfe qui, au nom de la sécurité nationale face au terrorisme islamiste, mais en réalité pour brider toute velléité de changement politique et particulièrement de contestation démocratique de régimes pratiquant l'arbitraire politique et la prédation économique des ressources au profit d'un clan au pouvoir, se sont dotées d'une capacité répressive exorbitante en adoptant des législations qui musellent toute liberté d'expression réfractaire susceptible de se manifester à travers les réseaux sociaux ; ainsi en est-il à Abou Dhabi, pays où les partis politiques sont interdits, où un décret de novembre 2012 permet aux services de sécurité d'infliger une forte amende pour quiconque critiquera l'émir, ses proches, les institutions et les symboles du pays ainsi que pour quiconque organisera un groupe via internet ou appellera à manifester sans solliciter l'autorisation du pouvoir ; le Qatar, le Koweït, le sultanat d'Oman et l'Arabie saoudite ont adopté des législations similaires. Encore sous prétexte de lutte contre le terrorisme, les services secrets de gouvernements dictatoriaux ou autoritaires, comme ceux de la Libye de Kadhafi, de la Syrie d'Assad ou de Bahreïn, ont acheté à des sociétés occidentales mercenaires qui le leur ont installé et en ont assuré la maintenance, des matériels d'écoute et d'interception de communications ainsi que des systèmes de surveillance du trafic internet qui leur ont permis d'appréhender, de torturer et d'emprisonner ou de faire disparaître des opposants politiques (journalistes, dissidents ou net-citoyens) défendant des idéaux démocratiques et de restreindre l'expression des libertés individuelles et collectives [30].

[30] Cf. Les ennemis d'internet, rapport de l'association Reporters sans frontières (RSF), mars 2013. Selon ce rapport, les pays qui appliquent le plus strictement une surveillance généralisée de leurs citoyens sont Bahreïn, la Chine, l'Iran, la Syrie et le Vietnam. Ces pays utilisent des moyens de surveillance variés comme des logiciels espions, le vol de compte sur les services internet, la surveillance ciblée et le piratage de connexions. Ils sont aidés en cela par des sociétés privées domiciliées en France, aux Etats-Unis, au Royaume-Uni, en Italie et en Allemagne. Grâce aux

Rivalisant avec les hackeurs professionnels ou embauchant certains de ces derniers en leur reconnaissant une qualité d'innovation, les secteurs public et privé se sont également "hackeurisés". Certains gouvernements utilisent les services de hackeurs, soit pour mener des campagnes dissuasives de défense (cas de l'Allemagne), soit pour mener des cyberattaques (cas des Etats-Unis et d'Israël qui, en 2010, ont envoyé des virus dans les serveurs d'une centrale iranienne d'enrichissement d'uranium). Aux Etats-Unis, le gouvernement (ministère de la Défense, agences comme la CIA ou la NSA) utilise les services de fabricants d'armes ayant ouvert des départements de sécurité informatique offensive capables de pénétrer les ordinateurs ou les serveurs des administrations, des organes de défense ou d'entreprises stratégiques de pays ennemis pour leur piller ou leur détruire leurs stocks de données ; quant à la NSA (le service de renseignement américain chargé de l'espionnage des télécommunications), avec la complicité des fabricants de logiciels (Microsoft, par exemple), elle a exigé que tous les logiciels exportés soient munis de *backdoors*, des portes dérobées qui lui permettent de pénétrer au cœur des systèmes utilisant ces produits américains [31]. Des sociétés privées de sécurité offensive ont également été créées qui, comme des trafiquants d'armes, vendent leur savoir-faire intrusif aux plus offrants (entreprises privées à la recherche d'un avantage comparatif concurrentiel, mais également organismes officiels comme la police, l'armée ou les services secrets accroissant ainsi leurs moyens de lutte contre la criminalité nationale ou internationale) pour pratiquer de l'espionnage économique ou porter des cyber-attaques militaires [32]. Mais, à travers les cyberattaques, le risque le plus important, davantage que l'espionnage, est celui du sabotage d'infrastructures (réseaux de distribution électrique, approvisionnement en eau) ou de la prise de contrôle de systèmes opérationnels. C'est ainsi que, au nom de la défense contre le cyber-terrorisme, les techniques de surveillance sont susceptibles de pervertir la démocratie et de remettre en question la vie privée à l'échelle de populations entières ; à l'idéal de libération de l'individu et de communication décentralisée prôné par les pionniers d'internet se substitue donc une centralisation de la surveillance et du pouvoir d'Etat[33].

---

logiciels espions que ces sociétés fournissent, il est possible d'espionner le contenu de disques durs, de récupérer des mots de passe, d'accéder au contenu de messageries électroniques ou d'espionner des communications téléphoniques par internet (VOIP). Ces matériels d'espionnage sont tellement efficaces que les Etats-Unis ont interdit leur exportation vers la Syrie et l'Iran.

[31] Cf. Analyse de la valeur du projet de contrat avec la société Microsoft, rapport d'expert concernant le contrat passé entre Microsoft le ministère français de la défense (15 février 2008).

[32] Cf. *Le Monde* du 20 février 2013.

[33] Le 6 juin 2013, le Washington Post et The Guardian ont rapporté que les services de surveillance des communications américains et britanniques (la NSA et le GCHQ) utilisaient deux programmes secrets : l'un permettant la récolte, depuis 2006, des données d'appels téléphoniques aux Etats-Unis via les opérateurs ; l'autre, nommé Prism (dont la version britannique s'appelle Tempora, mis en place en 2008), visant à intercepter les communications d'internautes étrangers se situant hors des Etats-Unis sur neuf grands réseaux sociaux, dont Facebook. Ces données,

Egalement sur le plan économique, les sites de commerce en ligne sont vulnérables car exposés à la contrefaçon. C'est ainsi qu'existent nombre de plates-formes de vente en ligne qui ressemblent à des sites de marque sauf que les produits proposés sont des contrefaçons. Ces pratiques illégales peuvent s'effectuer soit par le détournement du trafic légal (le parasitisme), soit par le vol d'identité numérique avec l'objectif d'usurpation de marque (le *cybersquatting*) ou de plagiat de contenus. Pour lutter contre ces illégalismes, des sociétés privées ont été créées qui vendent leurs services aux grandes entreprises pour traquer les sites de commerce en ligne pratiquant le parasitisme ou le *cybersquatting*.

Sur le plan géopolitique, les réseaux informatiques sont essentiellement contrôlés par des opérateurs privés, mais l'adressage des domaines est géré par un organisme américain à but non lucratif : l'Internet Corporation for Assigned Names and Numbers (ICANN), lui-même contrôlé par le ministère du commerce américain. Ainsi sur les treize serveurs racines existants, dix sont situés aux Etats-Unis. Telle est la raison pour laquelle se profile un conflit entre Américains et Européens, ces derniers revendiquant une gouvernance partagée pour l'accès aux réseaux. Le commerce international est également exposé à une différence d'approche entre Américains et Européens pour ce qui concerne l'exploitation des *Big Data*, ces données électroniques qui constituent la matière brute de l'économie numérique et recèlent quantité d'informations pouvant être traitées, recyclées et revendues. Ce sont quatre grandes entreprises américaines qui dominent ce marché : Google, Facebook, Apple et Amazon ; l'exploitation de leurs données échappe à la fois aux individus (qui fournissent involontairement les données de base en utilisant internet) et aux Etats (sur les territoires desquels sont collectées ces données). Face à une telle situation, les Américains défendent une liberté maximale (le libre marché, la dérégulation de commerce) pour l'extraction, l'exploitation et la rentabilisation des données afin de favoriser l'expansion mondiale et l'accroissement des bénéfices de leurs entreprises numériques ; quant aux Européens, ils souhaitent réglementer l'exploitation de ces données afin que soit respectée la vie privée et le libre choix des individus face aux grands groupes commerciaux et que puisse être taxé le commerce qui découle de la revente des *Big Data*.

Par ailleurs, Internet n'est plus seulement un réseau physique mais aussi et surtout un ensemble de services commerciaux fournis non seulement par des entreprises numériques (magasins en ligne comme Amazon, ou réseaux sociaux comme Facebook, par exemple), mais également par les opérateurs et les moteurs de recherche (Google, Yahoo, par exemple) ; or ces acteurs ont tendance, pour favoriser leurs propres intérêts, à enfreindre le principe de neutralité des réseaux, censé garantir l'accès universel aux contenus en ligne. Ce principe implique que tout utilisateur devrait pouvoir accéder à tout contenu, sans discrimination, et

---

ainsi que celles récoltées sur Yahoo, Microsoft, Google et les autres géants américains d'internet sont évidemment transmises aux services de renseignements des deux pays.

que les opérateurs, fournisseurs d'accès à internet (FAI), en tant que "tuyaux" par lesquels passent les données, devraient se contenter de transmettre ces dernières, sans les identifier ou les classer. Ce principe se heurte au besoin des opérateurs de garantir la qualité du réseau, ce qui les conduit notamment à donner priorité à un flux (vidéo, courriels...) par rapport à un autre, selon les besoins des usagers, les intérêts partagés (entre opérateurs, propriétaires de moteur de recherche, créateurs de sites, entreprises numériques) et l'état des réglementations imposées par un régulateur. Or, lorsque les opérateurs et les moteurs de recherche fournissent eux-mêmes des services, dans le cadre d'un abonnement, par exemple, ou en commercialisant des applications ou des préférences pour certains sites, le principe de neutralité est faussé par ce conflit d'intérêts, ce qui va à l'encontre de l'intérêt des usagers car ces derniers sont dirigés prioritairement vers les services gérés par les opérateurs, les moteurs de recherche ou les réseaux sociaux. Cette sélection anticoncurrentielle contrarie donc le second principe qui fonde les réseaux en ligne : le principe d'égalité, assurant l'accès à l'information pour l'ensemble des usagers et qui implique que les services d'accès et de communication devraient garantir aux usagers la liberté d'accès à tous les services (par exemple ceux qui sont spécialisés dans la comparaison des prix) ainsi que les libertés d'expression, d'innovation et de création. Encore faudrait-il pour cela que les régulateurs prévoient des sanctions dissuasives contre les opérateurs qui restreignent les communications en ligne.

Il résulte de cette évolution que les valeurs boursières de certains opérateurs, moteurs de recherche et réseaux sociaux ont maintenant dépassé celles des acteurs de l'industrie et du secteur financier en faisant en sorte que tous les utilisateurs qui apparaissent dans leurs fichiers clientèles sont ensuite classés et décomposés en listings revendus à des entreprises commerciales privées. Leur seconde source de revenus est la publicité qui envahit leurs sites. Alors qu'ils ne devraient générer par eux-mêmes aucun contenu et rester neutres, les moteurs de recherche, par exemple, trafiquent leurs mises à jour et falsifient leurs recommandations d'achat, aboutissant ainsi à une instrumentalisation commerciale des consommateurs-utilisateurs, basée sur la tromperie ou le vol de données qui sont, en fait, des illégalismes tolérés. L'instrumentalisation des utilisateurs, cette fois d'origine politico-policière, est rendue encore plus évidente par le fait qu'existe une collusion entre les grands groupes américains mondialisés de l'internet (Google, Facebook, Yahoo…) et les services secrets (notamment la NSA, mais également la DGSE française ou le BND allemand), fondée sur l'intérêt commun d'avoir besoin de toute l'information disponible pour servir l'objectif de contrôle (commercial ou policier) des populations. C'est ainsi qu'a été mise en place une sphère politique parallèle, les services étatiques s'émancipant de tout contrôle démocratique, aboutissant à la négation de la sphère privée des citoyens.

Finalement, la guerre des ondes a été remportée par les Etats-Unis, grâce à une alliance stratégique avec la Grande-Bretagne, la Nouvelle-Zélande, l'Australie et le Canada

(les *Five Eyes*)[34] en matière de cyber-sécurité et de cyber-opérations actives (le *hacking* d'Etat) visant à la surveillance et à l'espionnage des réseaux téléphoniques et électroniques à l'échelle mondiale.

CONCLUSION

Contrairement à ce que prétendaient les défenseurs d'internet dans les années 1990, qui voyaient dans le réseau le moyen de populariser à l'échelle mondiale une véritable démocratie égalitaire qui transcenderait et permettrait de réduire les conflits sociaux, ou géopolitiques et de lutter contre les dictatures, ni la géographie, ni les conflits territoriaux, ni les régimes autoritaires n'ont disparu[35]. La guerre se poursuit simplement à un autre niveau.

Elle se développe d'abord à travers un affrontement entre l'Etat national et les sociétés du Net, et a pour enjeu l'exercice des lois nationales dont le but de protéger la liberté individuelle de confidentialité des citoyens consommateurs du Net et de sanctionner leur transgression par les entreprises de ce secteur dont les acteurs sont mus par la liberté individuelle d'entreprendre. La loi se trouve donc au carrefour entre deux libertés individuelles, prise dans un rapport de force qui avantage les entrepreneurs collectifs du Net au détriment, apparent, des acteurs individuels qui consomment le Net. En effet, les multinationales du Net enregistrent et monnayent, en les revendant à des annonceurs publicitaires, les données personnelles et les traces laissées sur le réseau par les internautes, en contravention des lois, et sans autre possibilité, pour les consommateurs, que de ne plus pouvoir utiliser les réseaux s'ils ne sont pas d'accord avec les règles illégales d'utilisation que leur imposent les sociétés du Net comme condition pour pouvoir accéder à leurs services. En effet, en se connectant à Google, Facebook ou Twitter, l'utilisateur accorde une licence mondiale illimitée et gratuite aux réseaux qui peuvent ainsi disposer à leur guise des données

---

[34]**.** La base de cette alliance est un traité américano-britannique signé en 1946 ; son pivot exécutif et opérationnel est la National Security Agency (NSA) américaine. Suite aux attentats anti-américains de 2001 et au nom de l'antiterrorisme, cette alliance a été renforcée en moyens humains, matériels et financiers – avec 35 000 employés et un budget annuel de plus de 10 milliards de dollars, la NSA est l'agence la mieux dotée de la planète –, la NSA s'autorisant une surveillance électronique à l'échelle mondiale, au mépris des libertés individuelles et publiques. En 2013, la révélation, par le lanceur d'alerte Edward Snowden, du caractère universel de cette surveillance qui ne se limitait pas à renforcer la sécurité des Etats-Unis face aux menaces criminelles ou terroristes (par la mise sur écoute de millions de citoyens ordinaires), mais était étendue aux domaines politique (écoute des ambassades étrangères, des bureaux de ministres, de chefs d'Etat ou de gouvernement) et économique (espionnage industriel afin d'aider les entreprises américaines à devancer les entreprises étrangères concurrentes pour l'obtention de marchés), a permis de montrer l'opérationnalité de la distinction entre partenaires amis (les *Five Eyes* anglo-saxons et Israël) et partenaires alliés, ces derniers (notamment les pays européens et le Japon) étant exposés à la même surveillance que les pays concurrents (Brésil, Russie, Chine…) et ennemis (Syrie, Venezuela, Cuba…). Ici encore, c'est la *real politik* qui s'est imposée, aucune mesure de rétorsion, comme la remise en cause des accords de coopération, n'étant décidée par les gouvernements alliés des Etats-Unis à l'encontre de Washington car non seulement les agences de renseignements des pays visés opèrent de la même manière, en marge de la légalité, mais ces pays ont besoin du renseignement américain, par exemple lorsque la France lance une opération militaire en Libye (en 2011) ou au Mali (en 2013).

[35] Concernant les guerres du cyberespace, cf. l'entretien avec Frédérick Douzet de l'Institut français de géopolitique in *Le Monde* du 5-6 octobre 2008.

personnelles transmises ou déposées (textes, photos, dessins, mails, mots clés sur les moteurs de recherches…)[36]. Une nouvelle norme mondiale imposée par les marchés s'impose donc face aux lois nationales, et en transgressant ces dernières. On se trouve donc ici dans un cas, non de tolérance de la transgression, mais d'imposition d'une transgression à travers un coup de force contre la loi et contre les réglementations nationales, duquel résulte une *mise devant le fait accompli* des Etats nationaux par des multinationales privées et mondialisées qui sont un acteur stratégique et puissant des marchés, disposant d'énormes ressources financières lui permettant de payer des amendes aux Etats pour avoir transgressé les règles de confidentialité, et de continuer à transgresser ces règles comme si de rien n'était[37]. Apparaît ainsi une nouvelle forme d'illégalisme qui ne s'opère plus avec la complicité des représentants de l'Etat, mais contre la légalité que ces derniers défendent, et avec la complicité des acteurs sociaux consommateurs qui privilégient les libertés individuelles de consommer et de communiquer en toute transparence – qu'ils assimilent à la liberté d'expression – par rapport à la liberté individuelle de confidentialité de la vie privée, et qui, donc, cautionnent les transgressions des multinationales du Net – et la perpétuation de ces transgressions – que ces dernières présentent comme la condition d'exercice de la liberté d'expression. Tel est le schéma corruptif : l'Etat, qui délègue son pouvoir de communiquer au Sociétés du Net, est trahi par ces dernières associées aux consommateurs pour défendre un intérêt particulier (les profits commerciaux pour les sociétés, la volonté de communiquer pour les consommateurs) ; accessoirement, on se retrouve face à une division du peuple entre peuple gouvernant que défend l'Etat au nom de l'intérêt général et des principes universels de l'Etat de droit, et peuple gouverné que défend les sociétés du Net au nom d'intérêts particuliers différents et convergents, liés aux lois du marché (la liberté d'entreprendre et la liberté d'expression). A travers ce renversement corruptif, l'Etat apparaît comme l'ennemi des marchés qui défendent la liberté de communication au nom de la liberté d'expression, cette dernière étant présentée par les multinationales du Net comme contraire et supérieure au respect de la vie privée. Par voie de conséquence, et afin de ne pas se couper de la base sociale qui leur assure leur légitimité, les représentants des Etats libéraux sont forcés de laisser-faire et d'institutionnaliser cette transgression ; impuissants à réglementer, ils sont amenés à la normaliser de fait, ce qui revient à la régulariser informellement. Il en résulte non seulement que les libertés

---

[36] Cf. *Le Canard enchaîné* du 2 avril 2014.

[37] En France, c'est la Commission nationale de l'informatique et des libertés (CNIL), autorité administrative indépendante, qui, conformément aux lois "Informatique et Libertés" de 1978 et 2004 ainsi qu'à la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) de 2011, est chargée de contrôler les applications en matière informatique et de veiller au respect des droits en matière de protection des informations personnelles par les acteurs du Net ou ceux des télécommunications qui pratiquent la vidéo-surveillance ; elle a infligé en janvier 2014, une amende de 15 000 euros à Google pour non respect des règles de confidentialité alors que cette société réalise un bénéfice annuel de plus de 12 milliards de dollars. L'amende n'étant pas dissuasive, Google s'en est acquitté et a continué à transgresser la loi sur le territoire français.

individuelles d'expression, de communication, d'entreprendre et de consommer peuvent être contradictoires avec à la liberté individuelle de protection de la vie privée, les premières transgressant la seconde, mais également que, dans un Etat libéral, les premières sont d'une valeur supérieure à la seconde et au droit des Etats.

La guerre est également déclenchée à une échelle mondiale, polarisée autour de l'affrontement post-guerre froide entre les Etats-Unis (adeptes du marché et de la libre concurrence, pour qui les Etats traditionnels interventionnistes sont l'ennemi) et l'Europe (défendant les libertés individuelles par la mise en place de réglementations d'Etats, face à la menace représentée par les grands groupes privés, tout en adoptant simultanément le crédo libéral de la croissance par les marchés), l'enjeu étant le contrôle du marché des services fournis à travers internet ainsi que la surveillance, par le contrôle des réseaux, des usagers d'internet et des puissances rivales. Sans oublier la montée en puissance numérique de l'acteur chinois qui troublera de plus en plus le jeu, tirant sa richesse de l'endettement du monde et sa force d'un socialisme libéral qui laisse faire les marchés sous le strict contrôle de l'Etat.

Ainsi, internet n'est pas simplement un outil ; c'est un moyen de domination et de puissance qui utilise le contrôle ou l'appropriation des communications comme une ressource du *soft power* [38] et qui révèle l'emprise croissante des Etats-Unis sur ce nouveau pouvoir se développant dans le cadre d'une mondialisation qui risque de leur échapper (ouverture des frontières profitant aux migrations illégales, à la fraude fiscale et au blanchiment des bénéfices des trafics, multiplication des opérateurs et des réseaux de communication, extension géographique de la capacité de nuisance de groupes subversifs politico-religieux ou socio-économiques comme les trafiquants de drogue, multiplication des risques liés au réchauffement climatique ou aux épidémies...), avec l'objectif d'apporter une réponse globale à ces nouveaux problèmes transnationaux. Le soft power, prôné par les Etats-Unis dans les

[38] Le *soft power* peut être défini comme la capacité d'un acteur politique (un État, une firme multinationale, une ONG, des institutions internationales telles que l'ONU ou le FMI, ou des réseaux de citoyens, comme le mouvement altermondialiste ou les cyber-réseaux) d'influencer indirectement le comportement d'un autre acteur ou la définition par cet autre acteur de ses propres intérêts, en utilisant des moyens non coercitifs (technologiques, culturels ou idéologiques) relevant de politiques d'influence (sur les médias, les groupes d'opposition, les relais associatifs ou communautaires). Son théoricien est Joseph Nye, qui le désigne comme la capacité de séduire et de persuader les autres États sans avoir à user de la force ou de la menace ; il s'agirait d'une nouvelle forme de pouvoir dans la vie politique internationale contemporaine, qui ne fonctionne pas sur le mode de la coercition mais sur celui de la persuasion, c'est-à-dire la capacité de faire en sorte que l'autre (adversaire ou concurrent) veuille la même chose que soi. Selon Joseph Nye, le soft power ou la puissance de persuasion reposent sur des ressources intangibles telles que : l'image ou la réputation positive d'un État, son prestige (souvent ses performances économiques ou militaires), ses capacités de communication, le degré d'ouverture de sa société, l'exemplarité de son comportement (de ses politiques intérieures mais aussi de la substance et du style de sa politique étrangère), l'attractivité de sa culture, de ses idées (religieuses, politiques, économiques, philosophiques...), son rayonnement scientifique et technologique, mais aussi de sa place au sein des institutions internationales lui permettant de contrôler l'ordre du jour de ses débats (et donc de décider de ce qui est légitime de discuter) et de figer des rapports de puissance au moment où ils lui sont le plus favorables ; cf. Nye Joseph, *Bound to Lead : The Changing Nature of American Power*, New York, Basic Books, 1990.

années 1990, s'exercerait donc en privilégiant le pouvoir de cooptation sur les pratiques de coercition, c'est-à-dire en s'appuyant sur la séduction ou sur la possibilité de définir la hiérarchie des problèmes politiques du moment ; mais, en fait, il vise à imposer une politique fondée sur la contrainte (définition d'ennemis terroristes infiltrés qui a tendance à assimiler toute opposition politique à du terrorisme et qui justifierait une surveillance générale dans le cadre d'un Etat sécuritaire, présenté comme incontournable, pour assurer la sécurité des populations) et à empêcher l'expression de points de vue et de pratiques alternatifs. Ce pouvoir qui s'exerce en répliquant les qualités de son ennemi désigné, c'est-à-dire les acteurs en réseaux non régulés usant des technologies de communication d'une manière diffuse et non hiérarchisée, et qui compléterait les pouvoirs traditionnels (militaire et économique), est en fait un élément fondamental dans la manifestation de la puissance des Etats et, notamment celle des Etats-Unis qui l'utilisent pour fonder leur super-puissance mondiale. Et l'exemple des dérives étatiques d'internet montre bien comment ce soft power est une construction idéologique visant à occulter une coercition réelle qui s'exerce contre la démocratie à travers l'utilisation de techniques de surveillance à l'échelle de l'humanité. Transgressant lois et traités par l'utilisation de règles informelles, les Etats sont donc devenus aujourd'hui les pirates les plus puissants, mixant influence et violence légales et illégales pour essayer d'atteindre leur objectif de monopole de la piraterie.