Thèmes & Commentaires

Régulations

INTERNET, ESPACE D'INTERRÉGULATION

Sous la direction de
Marie-Anne Frison Roche

the Journal of Regulation

DALLOZ

L'intervention régulatrice de l'État sur les flux transfrontières circulant *via* Internet : un système de contraintes

Régis Bismuth
Professeur agrégé de droit public
à l'Université de Poitiers

L'État serait-il un échelon d'intervention périmé ou dépassé pour ce qui concerne la régulation des activités prenant appui sur Internet ? Une première intuition commande une réponse résolument positive, et ce, pour deux raisons. La première tient à la dimension transfrontière de ces activités qui font intervenir des acteurs, infrastructures et flux localisés et/ou diffusés sur des territoires différents, ce qui rend d'autant plus délicate l'intervention unilatérale de l'État. Internet constituerait ainsi un espace où la régulation ne pourrait être pensée qu'à l'échelle globale. Dès lors, la seule intervention étatique serait vouée à une inéluctable inefficacité ou une blâmable extraterritorialité. La seconde tient à la nature immatérielle de ces flux qui pénètrent sournoisement le territoire de l'État sans en traverser physiquement les frontières[1]. Ce dernier serait dès lors désarmé pour réguler des flux qui, quoique se propageant sur son territoire constituant l'assise spatiale de sa souveraineté, échapperaient *de facto* à toute possibilité de contrôle. De plus, à l'impuissance de l'État face à Internet se juxtaposait la volonté de certains de disqualifier toute velléité d'intervention du souverain sur ce réseau prétendument déterritorialisé. Elle se dégage en particulier de la Déclaration d'indépendance du Cyberespace de 1996 qui, s'adressant aux États, proclamait : « *You have no sovereignty where we gather*. […] *Cyberspace does not lie within your borders*[2]. » Cette position radicale de cyber-libertariens-utopistes concernait d'ailleurs aussi bien l'éventualité d'une intervention unilatérale que collective des

1. H. Ruiz Fabri, « Immatériel, territorialité et État », *Archives Phil. dr.* 1999, t. 43, p. 189-190.
2. J. P. Barlow, *A Declaration of the Independence of Cyberspace*, Davos, 8 févr. 1996, <https://projects.eff.org/~barlow/Declaration-Final.html>

États[3]. Tant sa technologie que ses usagers rendaient ainsi Internet rebelle à toute idée de régulation étatique[4].

Cette préconception que l'État en est réduit à un rôle de figuration dans la régulation d'Internet mérite toutefois d'être battue en brèche. Il ne s'agit pas nécessairement de l'échelon idoine d'intervention en tout point mais, entre une autorégulation largement réduite aux aspects techniques et une régulation mondiale encore balbutiante, il reste un acteur essentiel, en particulier dans les cas où ses intérêts propres sont en jeu. L'objet de cette contribution est justement de faire le bilan critique du rôle de l'État en la matière en se focalisant sur ses interventions régulatrices se rapportant à des situations transfrontières. Celles-ci désignent l'hypothèse où l'émetteur du flux circulant sur Internet se situe dans un État différent de celui à l'origine de l'intervention régulatrice et où se localise le récepteur. Il en est ainsi de la situation où une personne ou entité propose un service (par exemple, jeux et paris, services financiers, etc.) à une personne ou entité située dans un autre État. La question est donc de savoir si ce dernier a la possibilité d'exercer son contrôle sur une telle relation, étant entendu qu'une telle analyse présente un intérêt dès lors que les réglementations applicables à ces services dans le pays d'origine diffèrent de celles en vigueur dans l'État de destination.

Le contrôle des flux transfrontières soulève des problèmes juridiques et techniques. Les seconds ne seront pas traités ici tant ils ne relèvent pas de notre champ de compétence. Il faut toutefois souligner que des difficultés techniques sont régulièrement invoquées par les acteurs afin d'expliquer pourquoi ils ne peuvent se conformer à leurs obligations. C'est par exemple le cas de Google qui a allégué de certaines contraintes techniques pour se mettre en conformité avec ses obligations au titre du « droit de référencement » tel qu'il résulte de l'arrêt de la CJUE du 13 mai 2014[5]. L'entreprise a en effet indiqué qu'elle respectait ces exigences pour les extensions européennes de ses moteurs de recherche (par exemple google.fr ou .de, .co, .uk, etc.) mais qu'il lui était impossible de les mettre en œuvre pour les versions non européennes (par exemple google.com ou .us), et ce, alors qu'un référencement dont on peut demander le retrait serait toujours accessible dans l'espace européen *via* les versions non européennes du moteur de recherche. Elle soulignait de plus qu'étendre ainsi cette exigence consistait à donner une portée extraterritoriale au droit au déréférencement[6], argument puissamment relayé outre-Atlantique[7] alors qu'il ne correspond en rien à ce qu'a prescrit la Cour de l'Union européenne

3. P. Mounier, « Internet Governance and the Question of Legitimacy », *in* E. Brousseau, M. Marzouki et C. Méadel (ed.), *Governance, Regulations and Powers on the Internet*, Cambridge, Cambridge University Press, 2012, p. 170-171.

4. J. Boyle, « Foucault in Cyberspace : Surveillance, Sovereignty, and Hardwired Censors », *University of Cincinnati Law Review* 1997, vol. 66, p. 178 s.

5. CJUE 13 mai 2014, *Google Spain SL, Google Inc. c/ Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, aff. C-131/12.

6. « Google ne veut pas appliquer le "droit à l'oubli" dans le monde entier », *Le Monde (Économie et Entreprise)*, 1er août 2015, p. 11.

7. « "Right to Be Forgotten" Could Spread », *New York Times*, 6 août 2015, p. B1.

pour qui prime le critère de l'accessibilité sur le territoire européen du référencement litigieux[8].

L'étude des aspects juridiques des problèmes résultant des flux transfrontières requiert préalablement de revenir de façon plus générale sur la régulation d'Internet pour laquelle trois échelons d'intervention, qui peuvent opérer individuellement ou conjointement, sont identifiables : l'échelon privé, l'échelon étatique et l'échelon interétatique. Une distinction mérite également d'être réalisée dans ce cadre entre Internet en tant qu'infrastructure et Internet pour ce qui concerne les contenus qu'il permet de véhiculer.

Internet est à l'origine une infrastructure privée, gérée et régulée par des intérêts privés, impliquant une myriade d'institutions prenant la forme d'organismes de droit privé à but non lucratif. Ceux-ci ont un rôle particulier dans « la gestion des ressources critiques » et « des services de base [permettant] la circulation des contenus[9] ». S'il est impossible de toutes les mentionner dans le cadre de cette étude, une attention particulière doit être portée à l'*Internet Corporation for Assigned Names and Numbers* (ICANN) qui a notamment pour rôle la coordination technique du système de noms de domaine (DNS ou *domain name system*[10]). Les acteurs privés ne jouent par ailleurs qu'un rôle secondaire en ce qui concerne la régulation des contenus. Cela se manifeste en particulier dans les domaines de la standardisation des contrats de commerce électronique et dans celui désigné « Netiquette » qui se manifeste par des chartes de bonne conduite destinées aux utilisateurs professionnels ou particuliers[11].

Il n'existe pas encore de véritable régulation interétatique à vocation universelle d'Internet. Le réseau s'étant développé en dehors de la tutelle des pouvoirs publics, il a été délicat pour les États de s'imposer conjointement afin d'exercer leurs compétences sur ce qui avait déjà été construit et régulé par des acteurs privés. Un « mouvement d'interétatisation[12] » d'Internet est toutefois perceptible quoique timide, lequel peut d'ailleurs être comparé à celui qu'a connu la standardisation internationale des normes comptables qui a longtemps été le fait d'acteurs

8. C'est ce que souligne notamment la CNIL dans le cadre de son rejet du recours gracieux formé par Google : « Les extensions géographiques ne sont qu'un chemin d'accès au traitement. Dès lors que le déréférencement est accepté par le moteur de recherche, il doit s'opérer sur toutes les extensions conformément à l'arrêt de la CJUE. Si le droit au déréférencement était limité à certaines extensions, il pourrait être facilement contourné. […] Contrairement à ce qui a pu être indiqué par la société Google, cette décision ne traduit pas une volonté d'application extraterritoriale du droit français par la CNIL. Elle se borne à demander le plein respect du droit européen par des acteurs non européens offrant leurs services en Europe » (CNIL, *Droit au déréférencement : Rejet du recours gracieux formé par Google à l'encontre de la mise en demeure*, 21 sept. 2015, <www.cnil.fr>).

9. E. Lagrange, « Panorama des institutions impliquées dans la "gouvernance de l'Internet" », *in* SFDI, *Internet et le droit international*, Paris, Pedone, 2014, p. 206 s.

10. E. Lagrange, « L'Internet Corporation for Assigned Names and Numbers : un essai d'identification », *RGDIP* 2004. 305 s.

11. F. Latty, « La diversité des sources du droit de l'Internet », *in* SFDI, *Internet et le droit international*, *op. cit.*, p. 58-59.

12. A.-T. Norodom, « Internet et le droit international : Défi ou opportunité ? », *in* SFDI, *Internet et le droit international*, *op. cit.*, p. 31.

privés avant de voir les États tenter d'influencer ce processus qui leur a longtemps échappé[13]. L'Union internationale des télécommunications (UIT) joue un rôle prépondérant dans ce mouvement visant à « faire basculer entre les mains des États le pouvoir de contrôle du réseau et de ses usages [et] récupérer la fonction de coordination et de régulation[14] ». Certains États militent en ce sens (Chine, Russie, Émirats arabes unis, etc.) alors que d'autres cherchent justement à le limiter afin d'éviter qu'il n'affecte la neutralité d'Internet. C'est en particulier le cas des États-Unis, du Canada et du Royaume-Uni qui ont refusé de signer l'acte final de la Conférence mondiale sur les télécommunications internationales tenue à Dubaï en 2012 qui avait pour ambition d'assurer un transfert de certaines compétences techniques de l'ICANN vers l'UIT[15]. Une remarque similaire peut également être faite en ce qui concerne certaines compétences non techniques de l'ICANN en matière d'attribution des noms de domaine de premier niveau (TLD), activité pour laquelle un objecteur indépendant a été nommé afin de déterminer si une demande d'attribution ne viole pas l'ordre public ou les intérêts d'une communauté[16]. Ici encore, la question se pose de savoir si les États sont les mieux placés afin de statuer sur ces questions[17].

Ces quelques éléments montrent qu'il existe un système de vases communicants ayant vocation à distribuer les compétences intéressant la régulation globale d'Internet entre l'échelon interétatique (par exemple IUT) et l'échelon privé transnational (par exemple ICANN). Du point de vue du droit international, la question de l'intervention unilatérale de l'État pour ce qui concerne le contrôle de certains contenus sur Internet se place à un niveau différent et n'a pas vocation à interférer avec ce qui pourrait constituer une régulation universelle (publique ou privée) d'Internet. Le contrôle des flux transfrontières sur le réseau par un État a en effet pour fonction de permettre à celui-ci de protéger ses intérêts propres. Toutefois, cette intervention régulatrice peut affecter les intérêts des États sur le territoire desquels cette activité trouve son origine. Plus qu'une question de régulation universelle, il s'agit donc de déterminer dans quelle mesure le droit international,

13. M. De Bellis, « Control by Public Regulators over a Private Standard-Setter : The IFAC and the Establishment of the PIOB within the Auditing Sector », *in* S. Cassese et al. (eds.), *Global Administrative Law – Cases, Materials, Issues*, 2e éd., Rome/New York, IRPA/IILJ, 2008, p. 19 s. V. aussi, T. Perroud, « Standardisation internationale privée et *Global Administrative Law* », *in* R. Bismuth (dir.), *Standardisation internationale privée – Aspects juridiques*, Bruxelles, Larcier, 2014, p. 185 s.

14. E. Lagrange, *op. cit.*, note 9, p. 214.

15. UIT, *Conférence mondiale sur les télécommunications internationales*, Dubaï, 2012.

16. Par ex., l'attribution du TLD amazon à l'entreprise Amazon, ce qui serait susceptible d'affecter les intérêts des communautés de l'Amazonie. V., A. Pellet, « Une gestion privée de l'ordre public d'Internet ? », *in* SFDI, *Internet et le droit international*, *op. cit.*, p. 239 s.

17. Le Pr Alain Pellet, objecteur indépendant de l'ICANN, relevait à ce propos : « Je dois dire qu'après une année de pratique de ce mécanisme […] et ayant eu l'occasion de réfléchir à ce système, j'en suis venu à me dire qu'entre deux maux, il faut choisir le moindre ; et qu'entre une institution interétatique qui conduirait tout droit soit à un blocage aux conséquences catastrophiques, soit à l'étouffement de la liberté d'Internet sous la pression d'une coalition d'États philanthropiques comme la Chine, l'Arabie Saoudite ou la Fédération de Russie, et le système libéral, bizarrement organisé et largement auto-régulé mis en place par l'ICANN, j'opte sans guère d'hésitation pour ce dernier » (A. Pellet, *op. cit.*, note 16, p. 246).

en particulier pour ce qui concerne la théorie des compétences de l'État, permet à celui-ci de réguler des flux transfrontières (I). Il faut ensuite déterminer dans quelle mesure l'État doit repenser son intervention régulatrice et l'adapter aux nouvelles réalités sociales résultant de cette technologie (II). En dernier lieu, il est possible de constater que si le droit international général ne s'oppose pas à ce qu'un État régule des flux transfrontières, le droit international économique et le droit de l'UE imposent de nouvelles disciplines aux États qui permettent de contrôler la substance des interventions régulatrices de l'État, générant ainsi de nouvelles contraintes dont il doit tenir compte (III).

I. LA POSSIBILITÉ D'UNE INTERVENTION RÉGULATRICE DU POINT DE VUE DES COMPÉTENCES DE L'ÉTAT

Permettre à un État de réguler des flux transfrontières se diffusant par le biais d'Internet n'implique nullement de transformer, voire de déformer, les règles de droit international relatives à l'exercice des compétences de l'État[18]. En effet, les États tiennent globalement compte de celles-ci lorsqu'il s'agit de réguler de tels flux et cela se vérifie aussi bien du point de vue de l'exercice par eux de leur compétence exécutive (A) que juridictionnelle (B). Ces règles nécessitent seulement d'être appliquées d'une façon adaptée aux nouvelles relations sociales résultant de cette technologie.

A. Du point de vue de l'exercice par l'État de sa compétence exécutive

Les principes relatifs à l'exercice par l'État de sa compétence exécutive ont été fixés en 1927 par la Cour permanente de justice internationale (CPJI) dans son arrêt rendu dans l'affaire du *Lotus*. Elle y indiqua que « la limitation primordiale qu'impose le droit international à l'État est celle d'exclure – sauf l'existence d'une règle permissive contraire – tout exercice de sa puissance sur le territoire d'un autre État[19] ». Les États ont pleinement conscience de ces limites et contraintes posées par le droit international lorsqu'ils concluent des conventions relatives à la coordination de leurs compétences pour ce qui concerne les activités sur Internet. La Convention de Budapest sur la cybercriminalité du 23 novembre 2001 et adoptée

18. Pour une réflexion générale de la compétence des États dans le contexte d'Internet, v., U. Kohl, *Jurisdiction and the Internet – Regulatory Competence over Online Activity*, Cambridge, Cambridge University Press, 2007. V. aussi, J. Kulesza, *International Internet Law*, Abingdon, Routledge, 2012, p. 1-29.

19. CPJI 7 sept. 1927, *Lotus*, série A, n° 10, p. 18.

sous l'égide du Conseil de l'Europe constitue à cet égard un exemple pertinent[20]. Elle montre en effet que certains principes de droit international qui ont émergé à une époque où Internet n'existait pas peuvent néanmoins s'appliquer à ces nouvelles activités. Toute la question dans le cadre de la Convention de Budapest est de déterminer en quoi la dimension immatérielle et transfrontalière d'Internet permet ou non de caractériser une situation où un État exerce sa puissance sur le territoire d'un autre État.

Cette convention traite notamment de la question de l'accès transfrontière par les États aux données, c'est-à-dire de la situation qui consiste à « accéder unilatéralement aux données informatiques stockées sur le territoire d'une autre Partie[21] ». L'article 32 de la Convention envisage deux situations. En premier lieu, un État peut « accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données[22] ». En second lieu, un État peut « accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, s'il] obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique[23] ».

Ces deux dispositions peuvent être appréhendées de deux façons différentes mais, dans les deux cas, elles restent conformes à l'esprit des principes généraux du droit international en matière d'exercice de compétence exécutive. Pour ce qui concerne l'accès à des données informatiques stockées accessibles au public, il est possible de considérer que la libre accessibilité signifie qu'il n'y a pas d'exercice de puissance sur le territoire d'un autre État. Elle peut être aussi envisagée en tant que règle permissive du droit international. Il en est de même pour des données non librement accessibles qui nécessitent le consentement de la personne légalement autorisée à divulguer ces données. Il est possible d'envisager cette disposition comme une règle permissive ou comme témoignant d'une absence de l'exercice de compétence exécutive sur le territoire d'un autre État car, dans cette situation, on peut considérer que c'est la donnée qui est librement communiquée depuis l'étranger à l'État la sollicitant.

L'exemple de la Convention de Budapest sur la cybercriminalité montre ainsi que des doutes subsistent quant à l'identification précise de ce que constitue l'exercice d'une compétence exécutive dans le cadre d'activités transfrontières et immatérielles. Les États ont toutefois justement à l'esprit les contraintes résultant du droit international en la matière et cherchent à clarifier le régime relatif à ces

20. Sur ces aspects, v., J. Bourguignon, « La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'État », *in* SFDI, *Internet et le droit international*, *op. cit.*, p. 366 s.

21. Conseil de l'Europe, *Rapport explicatif de la Convention sur la cybercriminalité*, 23 nov. 2001, § 293.

Comité de la Convention Cybercriminalité (T-CY), *Note d'orientation du n° 3 – Accès transfrontalier aux données (article 32)*, adoptée par la 12e Réunion plénière du T-CY, T-CY (2013) 7 F rev, 2-3 déc. 2014.

22. Art. 32(a).

23. Art. 32(b).

opérations et notamment les prérogatives des États dans le domaine de l'accès transfrontière aux données. On peut également déduire de ces deux dispositions de la Convention de Budapest que l'intrusion unilatérale d'un État sur un système informatique fermé situé à l'étranger constituerait l'exercice d'une compétence exécutive qui ne serait pas légale du point de vue du droit international. Cette approche est également confirmée dans le domaine du droit international appliqué à la cyberguerre[24]. Ainsi, dès lors qu'il entend mettre en œuvre sa compétence exécutive dans le domaine d'Internet, l'État reste soumis aux principes du droit international qui lui permettent d'avoir recours à tout acte de puissance sur son territoire et, en cas de règle permissive, sur le territoire d'un autre État.

B. Du point de vue de l'exercice par les États de leur compétence juridictionnelle

L'exercice par les États de leur compétence juridictionnelle s'inscrit dans un cadre différent. Comme l'a souligné la CPJI dans la même affaire du *Lotus*, « loin de défendre d'une manière générale aux États d'étendre leurs lois et leur juridiction à des personnes, des biens et des actes hors du territoire, il leur laisse, à cet égard, une large liberté, qui n'est limitée que dans quelques cas par des règles prohibitives » et « pour les autres cas, chaque État reste libre d'adopter les principes qu'il juge les meilleurs et les plus convenables[25] ». C'est ainsi qu'un élément de rattachement est en général exigé par le forum susceptible d'exercer sa compétence afin de se limiter à des situations qui présentent pour lui un intérêt ou une proximité suffisante. Celui-ci est principalement territorial (la situation se déroule sur le territoire de l'État) ou fondé sur la nationalité (la situation implique un ressortissant de l'État). Il peut également résulter d'autres hypothèses (atteinte aux intérêts fondamentaux de l'État, cas de compétence universelle) qui ne méritent pas ici de développements additionnels[26]. Le lien de rattachement territorial présente quant à lui un intérêt particulier pour ce qui concerne l'exercice par les États de leur compétence juridictionnelle à l'égard d'activités se déroulant sur Internet. Il s'agit notamment de déterminer si l'on doit s'en tenir à une approche restrictive du lien de territorialité ou si celui-ci mérite d'être appréhendé selon ses objectifs dans une logique plus fonctionnelle. Dans la première hypothèse, la compétence se limiterait à des situations qui se déroulent essentiellement sur le territoire du forum saisi, ce qui ne permettrait pas d'appréhender dans leur ensemble des flux transfrontières circulant sur Internet et donc de contrôler les agissements de l'émetteur lorsqu'il se trouve sur le territoire d'un autre État. Dans la seconde hypothèse, la compétence de l'État

24. M. N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare (Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence)*, Cambridge, Cambridge University Press, 2013, p. 15 s.

25. CPJI 7 sept. 1927, *Lotus*, préc., p. 19.

26. De façon générale, v., J. Crawford, *Brownlie's Principles of Public International Law*, 8e éd., Oxford, Oxford University Press, 2012, p. 466 s. ; C. Staker, « Jurisdiction », *in* M. Evans (ed.), *International Law*, 4e éd., Oxford, Oxford University Press, 2014, p. 309 s.

pourrait s'étendre à des situations permettant de contrôler l'émetteur du flux transfrontière dans la mesure où, quoique se trouvant sur le territoire d'un autre État, il cherche à cibler spécifiquement des personnes se situant sur son territoire. Cette appréhension fonctionnelle de la compétence territoriale se retrouve dans la théorie dite « des effets » qui a pour fonction d'étendre la compétence (notamment d'une juridiction) à des conduites qui, quoique se réalisant à l'étranger, produisent des effets directs, substantiels et prévisibles sur le territoire de l'État concerné[27]. La Cour de Luxembourg l'a déjà appliqué dans le domaine du droit de la concurrence en soulignant à propos des ententes la distinction nécessaire entre leur formation et leur mise en œuvre car « faire dépendre l'applicabilité des interdictions édictées par le droit de la concurrence du lieu de la formation de l'entente aboutirait à l'évidence à fournir aux entreprises un moyen facile de se soustraire auxdites interdictions. Ce qui est déterminant est donc le lieu où l'entente est mise en œuvre[28] ». La Cour a même souligné que la compétence de la Communauté dans ce cadre était « couverte par le principe de territorialité qui est universellement reconnu en droit international public[29] ». C'est cette même logique fonctionnelle qui est à l'œuvre dans le domaine d'Internet où l'on parle davantage de la théorie de la « focalisation » (ou du *targeting*) que de celle des « effets[30] ».

Dans le domaine d'Internet, la seule accessibilité d'un contenu litigieux ne saurait constituer un critère permettant de fonder dans tous les cas la compétence d'une juridiction nationale à l'égard d'un émetteur de contenu situé à l'étranger. En effet, comme l'a souligné la cour d'appel de Paris, « compte tenu de l'universalité de ce réseau, appliquer le critère de la simple accessibilité aurait nécessairement pour conséquence d'institutionnaliser la pratique du *forum shopping*[31] ». Ce critère, s'il peut être retenu dans des circonstances bien précises pour certaines infractions ou certains types de dommage[32], aurait également pour effet de favoriser les situations de conflit positif. C'est pourquoi il revient en règle générale selon cette même juridiction « de rechercher et de caractériser, dans chaque cas particulier, un lien suffisant, substantiel ou significatif, entre ces faits ou actes et le dommage allégué[33] ».

Il serait délicat de procéder ici à une analyse de l'ensemble de la jurisprudence exploitant la théorie de la focalisation, car l'examen de la compétence repose sur des instruments qui peuvent être distincts en fonction de la demande (concurrence

27. M. N. Shaw, *International Law*, 6e éd., Cambridge, Cambridge University Press, 2008, p. 688 s. ; K. Hixson, « Extraterritorial Jurisdiction Under the Third Restatement of Foreign Relations Law of the United States », *Fordham International Law Journal* 1988, vol. 12, p. 127 s.

28. CJCE 27 sept. 1988, *A. Ahlström Osakeyhtiö et al. c/ Commission*, aff. 89, 104, 114, 116, 117 et 125 à 129/85, § 16.

29. *Ibid.*, § 18. Pour une critique de cette confusion entre théorie des effets et compétence territoriale, v., B. Stern, « L'extraterritorialité revisitée – Où il est question des affaires *Alvarez-Machain*, *Pâte de bois* et de quelques autres », *AFDI* 1992. 239 s., spéc. p. 288 s.

30. F. Jault-Seseke, « Internet, vecteur d'affinement des règles de compétence juridictionnelle », *in* SFDI, *Internet et le droit international*, *op. cit.*, p. 167 s.

31. Paris, 6 juin 2007, RG n° 06/14890, *Google*, *JCP* 2007. II. 10151, note M.-E. Ancel ; *LPA* 2007, n° 224, note A. Mendoza-Caminade.

32. F. Jault-Seseke, *op. cit.*, note 30, p. 174 s.

33. Paris, 6 juin 2007, préc., note 31.

déloyale, contrefaçon, etc.[34]). Il est néanmoins possible de préciser quels sont les principaux indices dont la juridiction peut tenir compte afin de déterminer si l'émetteur ciblait par le biais de son activité un public déterminé[35]. La CJUE en a dressé une liste indicative à destination du juge national dans le cadre de l'arrêt sur les affaires jointes *Pammer* et *Alpenhof* qui concernait la protection des consommateurs dans le cadre d'achats réalisés sur Internet. Selon la cour, certains éléments constituent des indices explicites que le commerçant manifeste sa volonté de cibler un marché donné. Il en est ainsi de « la mention selon laquelle ce dernier offre ses services ou ses biens dans un ou plusieurs États membres nommément désignés[36] » ou de l'engagement de dépenses pour un service de référencement auprès de l'exploitant d'un moteur de recherche afin d'améliorer la visibilité du site auprès de certains consommateurs[37]. L'examen ne doit pas pour autant se limiter à « des indices aussi patents[38] » et la Cour rappelle à ce propos que d'autres éléments, en particulier lorsqu'ils sont combinés les uns aux autres, sont susceptibles de démontrer qu'une activité est dirigée vers l'État membre du consommateur. Il en est ainsi de l'utilisation de noms de domaine de premier niveau (.fr, .de, etc.) autres que celui où le commerçant est établi, de la référence à divers éléments suggérant l'existence d'une clientèle dans cet État (témoignages de clients[39]…), ainsi que de la possibilité d'utiliser la langue et la devise de l'État ciblé si elles sont différentes de celles de l'État d'origine du commerçant[40].

Les règles de compétence juridictionnelle montrent bien qu'elles ont su s'adapter afin de s'appliquer aux flux transfrontières qui circulent *via* Internet. Il en est d'ailleurs de même pour ce qui concerne la compétence législative[41]. On peut ainsi, à l'instar de certains, relever que la théorie de la focalisation traduit davantage une forme de *continuum* qu'une différence de nature entre compétence territoriale et théorie des effets[42]. L'innovation technologique que constitue Internet n'a donc pas pour conséquence de désarmer l'État dès lors qu'il entend exercer sa compétence sur de tels flux. D'ailleurs, loin de limiter une telle compétence, celle-ci peut se voir étendue quasiment à l'infini dès lors qu'est établi un lien, même ténu, avec le forum qui entend l'exercer. On pourrait d'ailleurs parler pour les États-Unis, sur le territoire desquels transitent de nombreux flux, d'une forme de compétence universelle

34. F. Jault-Seseke, *op. cit.*, note 30, p. 171 s.

35. CJUE 7 déc. 2010, *Peter Pammer c/ Reederei Karl Schlüter GmbH & Co. KG* et *Hotel Alpenhof GesmbH c/ Oliver Heller*, aff. C-585/08 et C-144/09, *Rev. crit. DIP* 2011. 414, note O. Cachard.

36. *Ibid.*, § 81.

37. *Ibid.*

38. *Ibid.*, § 82.

39. *Ibid.*, § 83.

40. *Ibid.*, § 84.

41. M.-E. Ancel, « La compétence législative à la croisée de deux logiques », *in* SFDI, *Internet et le droit international*, *op. cit.*, p. 181 s.

42. M. Ayashi, « Objective Territorial Principle or Effects Doctrine ? Jurisdiction and Cyberspace », *in* C. Focarelli (ed.), *Le nuove frontiere del diritoo internazionale : Attori non statalui, spazio virtuale, valori fondamentali e governo multinazionale di territori*, Pérouse, Morlacchi, 2008, p. 97 s., spéc. p. 113 s.

de facto[43]. Cette innovation technologique constitue néanmoins un défi pour ce qui concerne la forme que peut épouser son intervention régulatrice.

II. LA NÉCESSITÉ POUR L'ÉTAT DE REPENSER SON INTERVENTION RÉGULATRICE

Une fois que l'État considère qu'il est susceptible d'exercer sa compétence sur des flux transfrontières circulant *via* Internet, encore faut-il que son intervention permette de réguler efficacement des activités. La mutation technologique générée par Internet est toutefois à l'origine de nouvelles contraintes pour les États et ceux-ci doivent adapter aussi bien le contenu (A) que les modalités (B) de leurs interventions.

A. Une intervention régulatrice contrainte par la compartimentation de la régulation

La question qui se pose dorénavant est de déterminer si Internet constitue une innovation telle qu'elle est de nature à rendre obsolètes les mécanismes sur lesquels repose la régulation de l'État. En d'autres termes, les instruments actuellement en vigueur sont-ils susceptibles ou non de s'appliquer *mutadis mutandis* aux activités prenant appui sur ce réseau ? La question n'appelle pas de réponse d'ensemble positive ou négative, car les situations varient en fonction des activités et des branches du droit concernées. À titre d'illustration, le domaine du droit pénal se prête mal à la possibilité d'une seule exploitation des infractions existantes en les transposant aux activités virtuelles dans la mesure où le principe de légalité des délits est susceptible de limiter les possibilités d'application du texte pénal par analogie à de nouvelles relations sociales. C'est ainsi que certaines infractions doivent être amendées afin de préciser qu'elles s'appliquent aux activités

43. Il en est ainsi de l'établissement de la compétence personnelle dans le cadre d'affaires relevant du FCPA aux États-Unis dès lors que les activités litigieuses des personnes visées se manifestaient par le biais d'emails qui transitaient *via* des serveurs localisés aux États-Unis. Comme l'a relevé à cet égard une cour de district : « *The emails were "routed through and/or stored on network servers located within the United States". The mere fact that Defendants may not have had personal knowledge that their emails would be routed through or stored in the United States does not mean that they did not, in fact, use an instrument of interstate commerce sufficient for purposes of conferring jurisdiction. Second, the Court rejects Defendants' argument that it was not foreseeable that emails sent over the Internet in a foreign country would touch servers located elsewhere. The Court does not disagree with Defendants that "[t]he [I]nternet is a huge, complex, gossamer web", but that is all the more reason why it should be foreseeable to a defendant that Internet traffic will not necessarily be entirely local in nature* » ; *Securities and Exchange Commission c/ Straub*, 921 F. Supp. 2d 244 (SDNY, 2013).

en ligne[44], de même que de nouvelles doivent être instituées afin de réprimer de nouveaux types de comportements[45]. Internet requiert dès lors d'adapter le droit pénal afin de forger un nouveau droit de la cybercriminalité[46].

S'il existe de nombreuses activités prenant appui sur Internet pour lesquelles les États ont été contraints d'adapter leur réglementation, il en est une qui perturbe significativement et de manière transversale la logique régulatrice de l'État, celle des monnaies virtuelles, aussi appelées « crypto-monnaies[47] ». Il s'agit de monnaies d'origine privée conservées sur des supports numériques qui peuvent être adossées à une entreprise privée et fonctionnent dès lors dans le cadre d'un système fermé et centralisé (comme les *Amazon Coins* émises par l'entreprise Amazon) ou constituer un système de paiement ouvert et utilisable par tous (tel que Bitcoin[48]). Des positions divergentes se manifestent quant à la question de savoir si le terme de « monnaie » peut être adossé à ce type d'instruments[49]. Certains, selon ce qui est communément désigné comme la théorie étatique de la monnaie, estiment que seul le souverain est susceptible de battre monnaie et de lui conférer un cours légal et, ainsi, son pouvoir libératoire[50]. Dans cette perspective, le bitcoin ne peut être qualifié juridiquement de monnaie[51]. D'autres, selon la théorie dite « sociologique » de la monnaie[52], considèrent que celle-ci n'est pas réductible à la seule qualité souveraine de son émetteur mais que c'est son utilisateur qui constitue son centre de gravité, car la monnaie existe avant tout par l'usage qui en est fait par une communauté[53]. C'est ici qu'Internet, faisant fi des frontières nationales autour desquelles s'articulent des espaces monétaires administrés unilatéralement ou conjointement par les États, permet la constitution de communautés transnationales propices à développer des instruments monétaires communs. Le processus de constitution de ces communautés diffère selon que l'on se place dans le cadre

44. C'est le cas par exemple du harcèlement qui est dorénavant punissable lorsque les faits « ont été commis par l'utilisation d'un service de communication au public en ligne » (C. pén., art. 222-33-2-2(4)).

45. Il en est ainsi des délits relatifs aux atteintes aux systèmes de traitement automatisés de données (C. pén., art. 323-1 s.)

46. P. Guillot, « De la répression des infractions cybernétiques à la protection des droits des internautes », *in* SFDI, *Internet et le droit international*, *op. cit.*, p. 325 s.

47. European Central Bank, *Virtual Currency Schemes*, oct. 2012, p. 13 (définissant une *virtual currency* comme « *a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community* »).

48. Pour plus de détails, v. *ibid.*, p. 13 s. V. aussi, C. Breton, « Les enjeux de la dématérialisation des moyens de paiement pour l'État », *in* SFDI, *Internet et le droit international*, *op. cit.*, p. 463 s.

49. Pour une vue d'ensemble des différentes théories relatives à la monnaie, v., R. Bismuth, « Monnaie (droit) », *in* F. Hervouët, P. Mbongo et C. Santulli (dir.), *Dictionnaire encyclopédique de l'État*, Paris, Berger-Levrault, 2014, p. 636 s.

50. Cette théorie étatique de la monnaie a été notamment diffusée par G. F. Knapp, *The State Theory of Money*, Londres, Macmillan, 1924.

51. H. de Vauplane et S. Cazaillet, « *Bitcoin : money, money, money?* », *Lexbase* 17 avr. 2014, n° N1872BUU.

52. Théorie notamment diffusée par A. Nussbaum, *Money in the Law National and International – A Comparative Study in the Borderline of Law and Economics*, Brooklyn, The Foundation Press, 1950.

53. R. Bismuth, *op. cit.*, note 49, p. 639.

d'une monnaie virtuelle s'intégrant dans un système de paiement fermé ou un système ouvert. Dans le premier cas, c'est le pouvoir de marché de l'entreprise qui émet la monnaie qui permet de garantir son utilisation effective et ainsi son acceptation par la communauté, c'est-à-dire les clients de l'entreprise (par exemple les *Amazon Coins* ou les anciens *Facebook Credits*). Dans le second cas, c'est l'adhésion progressive d'une communauté à un système de paiement donné considéré comme fiable qui confère à celui-ci une attractivité (par exemple Bitcoin).

Ces monnaies d'un nouveau genre qui se diffusent *via* Internet sont ainsi en contact avec l'économie réelle, en particulier celles s'intégrant dans un système de paiement ouvert, tout en restant à l'écart du système bancaire qui constitue une interface essentielle de régulation et de contrôle des flux financiers. C'est ainsi que l'opacité dans laquelle les monnaies virtuelles évoluent est à l'origine de nombreux risques pour ceux qui les utilisent et les États : risque d'opérations frauduleuses pour les utilisateurs, risque de non-convertibilité, risque de volatilité et de dépréciation de leur valeur, risque de contournement des obligations fiscales et des réglementations relatives au blanchiment de capitaux et au financement du terrorisme[54].

Les monnaies virtuelles remplissant des fonctions analogues aux monnaies ayant cours légal, mais ne s'intégrant pas dans les catégories définies de la régulation financière, leur encadrement se heurte donc à l'incapacité des autorités de régulation dont les compétences sont limitées et compartimentées. Cette idée a été très bien exprimée par Janet Yellen, gouverneur de la *Federal Reserve*, lorsqu'elle indiqua que « [*i*]*t's important to understand that this is a payment innovation that's happening outside the banking industry* » et que par conséquent « [*t*]*he Federal Reserve simply does not have the authority to regulate bitcoin in any way*[55] ». C'est pourquoi, dans l'incapacité d'exercer leurs compétences réglementaires, les autorités de régulation financière et banques centrales se sont principalement limitées à émettre des avertissements (*warnings*) visant à sensibiliser les acteurs aux risques associés aux monnaies virtuelles[56].

Ainsi, par les innovations qu'il permet de voir émerger, Internet est susceptible de bousculer des logiques de régulation fondées sur une approche sectorielle qui a pour effet de compartimenter l'intervention de l'État. Il est d'ailleurs intéressant de constater que c'est dans le domaine du droit fiscal que la nature du bitcoin a été appréciée de la façon la plus réaliste sans tenir compte de cette compartimentation. Le réalisme du droit fiscal conduit en effet à appréhender une situation indépendamment des qualifications juridiques qu'elle est susceptible de se voir assigner par différentes branches du droit. Le fait que le bitcoin et ceux qui l'échangent ne peuvent être respectivement considérés comme un instrument financier ou des

54. Pour un panorama de ces risques, v., European Banking Authority, *EBA Opinion on Virtual Currencies*, EBA/Op/2014/08, 4 juill. 2014, p. 21 s. V. aussi le rapport du GAFI, Financial Action Task Force, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, juin 2014.

55. « Janet Yellen : Fed Will Steer Clear of Bitcoin », *Fortune* 27 févr. 2014.

56. V. par ex., Banque de France, *Les dangers liés au développement des monnaies virtuelles : L'exemple du Bitcoin*, *Focus* 5 déc. 2013, n° 10. Pour davantage d'exemples, v. European Central Bank, *Virtual Currency Schemes – A Further Analysis*, févr. 2015, p. 30.

prestataires de services d'investissement n'a pas constitué un obstacle à ce que la CJUE reconnaisse que « la devise virtuelle bitcoin n'a pas d'autres finalités que celle de moyen de paiement et qu'elle est acceptée à cet effet par certains opérateurs[57] », conduisant ainsi la Cour à considérer que les échanges euros/bitcoins bénéficiaient de l'exonération applicable aux moyens de paiement légaux.

B. Adapter les modalités et les objectifs de la régulation

Comme cela vient d'être évoqué, la compartimentation des régulations a abouti à une fragmentation matérielle des fonctions de l'État rendant plus complexe la régulation de nouvelles relations sociales rendues possibles par Internet et chevauchant les différents espaces de régulation qui sont définis à l'échelon national. Mais Internet implique aussi pour l'État de réévaluer et de réadapter les objectifs et les modalités mêmes de la régulation car sa compétence exécutive est limitée en principe à son territoire et, par conséquent, son emprise sur les flux transfrontières est limitée plus aux effets qu'ils produisent sur celui-ci qu'aux acteurs qui en sont à l'origine mais qui se situent à l'étranger. Comprendre la nouvelle logique régulatoire qu'Internet rend nécessaire requiert en premier lieu de revenir sur les spécificités de ce réseau.

L'architecture décentralisée d'Internet implique l'intervention d'un ensemble d'intermédiaires permettant la mise en relation de l'émetteur et du récepteur d'un flux circulant sur le réseau. Ces intermédiaires peuvent avoir pour fonction de stocker le contenu (les hébergeurs), de permettre un accès au réseau (les fournisseurs d'accès) ou de permettre d'identifier les contenus pertinents et d'y accéder (les moteurs de recherche). Ces multiples intervenants constituent des « passages obligés qui, territorialisés, sont autant d'occasions pour les États d'exercer, ou de faire exercer, un contrôle sur les contenus qui y transitent[58] ». Ces acteurs privés se voient ainsi confier par les États une mission de régulation de l'Internet, un peu similaire à celle de certains acteurs privés dans le cadre de la régulation des marchés financiers tels que les commissaires aux comptes. On peut d'ailleurs relever que, dans les deux domaines, l'expression de *gatekeepers* (ou « gardiens ») est employée pour les désigner[59].

Cette logique se retrouve particulièrement dans le domaine du droit d'auteur. Ces différents intermédiaires peuvent en effet voir leur responsabilité engagée non parce qu'ils ont permis la réalisation d'une violation du droit d'auteur par leur biais, mais parce qu'ils ont omis d'agir promptement pour la faire cesser dès lors qu'ils

57. CJUE 22 oct. 2015, *Skatteverket c/ David Hedqvist*, aff. C-264-14, § 52.

58. P. Jacob, « Les moyens de faire respecter le droit d'auteur dans l'environnement numérique », *in* SFDI, *Internet et le droit international*, *op. cit.*, p. 421-422.

59. J. Zittrain, « A History of Online Gatekeeping », *Harvard Journal of Law & Technology* 2006, vol. 19, n° 2, p. 253 s. ; J. C. Coffee Jr., *Gatekeepers : The Professions and Corporate Governance*, Oxford, Oxford University Press, 2006.

en ont eu connaissance[60]. C'est ainsi qu'ils ont dû développer des procédures de notification et de retrait de contenu illicite (aussi désignés *notice and take down*) susceptibles d'être sollicités par les ayants droit, dans un premier temps de façon non contentieuse[61]. Les autorités judiciaires ou administratives sont ensuite susceptibles d'intervenir en cas d'inaction ou de refus face à la demande de retrait afin de contraindre ces intermédiaires à s'y conformer. Dans cette perspective, « l'enjeu de la réponse étatique glisse […] de l'identification des auteurs de l'infraction vers celle de ceux qui sont en mesure d'y mettre un terme[62] ».

Dès lors qu'elles disposent des instruments nécessaires, les autorités de régulation peuvent participer à la mise en œuvre effective de ces mécanismes et demander, à l'instar des ayants droit dans le contexte de violations relevant du droit d'auteur, la neutralisation de l'accessibilité sur le territoire français de contenus contraires à la réglementation. Une affaire récente opposant l'Autorité des marchés financiers (AMF) à certains hébergeurs et fournisseurs d'accès constitue de ce point de vue une illustration intéressante. L'AMF avait constaté que deux sociétés respectivement domiciliées au Royaume-Uni et en Suisse (AxaTrades et FXBTrade) proposaient par le biais d'Internet des services d'investissement en ligne à destination de la France alors qu'elles ne disposaient pas de l'agrément requis par la réglementation. À l'aune de ces faits, l'AMF a assigné en référé les hébergeurs de ces sites situés à l'étranger et les fournisseurs d'accès internet localisés en France afin d'exiger que soit bloqué l'accès aux sites litigieux depuis la France. La saisine du TGI de Paris est organisée par l'article L. 621-14 (II) du Code monétaire et financier qui autorise le président de l'AMF à demander en justice qu'il soit ordonné au responsable de toute pratique contraire aux règlements d'y « mettre fin ou d'en supprimer les effets ». L'action se fondait sur les dispositions de l'article 6-1.8 de la loi du 21 juin 2004 *pour la confiance dans l'économie numérique* aux termes desquelles « l]'autorité judiciaire peut prescrire [aux prestataires d'hébergement] ou à défaut aux [fournisseurs d'accès] toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne ». C'est ainsi que le TGI de Paris a ordonné aux hébergeurs, et aux fournisseurs d'accès en cas d'inexécution des premiers, « de mettre en œuvre ou faire mettre en œuvre, toute mesure propre à empêcher l'accès, à partir du territoire français », des deux sites litigieux[63]. On peut identifier ici une certaine logique de subsidiarité : il s'agit de cibler, autant que faire se peut, le mal à la racine en s'adressant à ceux qui hébergent le contenu litigieux et, si les premières mesures ordonnées venaient à ne pas être respectées par leurs destinataires (notamment pour les hébergeurs qui ne sont pas situés en France), de cibler dans un second temps les relais par lesquels ces sites demeurent accessibles sur le territoire de l'État.

60. Pour des illustrations, v., P. Jacob, *op. cit.*, note 58, p. 422 s.
61. *Ibid.*
62. *Ibid.*, p. 423.
63. TGI Paris, ord. réf., 22 sept. 2014, *Le président de l'Autorité des marchés financiers c/ S.A. NC Numericable, S.A. Orange et autres*, disponible sur <www.legalis.net>.

En se reposant sur ces nouveaux relais que sont les *gatekeepers*, l'État ne fait pas qu'adapter les modalités de la régulation de l'Internet, il en fait aussi évoluer les objectifs. Conscientes qu'elles ne peuvent parfois pas obtenir une cessation absolue de la diffusion de contenus illicites, les autorités étatiques en ciblent les relais essentiels afin de limiter l'accessibilité aux contenus illicites. Cela se vérifie notamment dans le cas où l'on exige d'un moteur de recherche le retrait d'un référencement conduisant à un contenu illicite : celui-ci sera toujours en théorie atteignable par l'internaute mais ce dernier, en l'absence de référencement, aura plus de difficulté à identifier l'adresse permettant d'y accéder[64]. Dans le domaine du droit d'auteur, il y a également une logique économique qui est à l'œuvre afin de restreindre l'accessibilité des contenus illicites. En effet, comme le soulignait le rapport Lescure, « [l]'objectif est moins d'éradiquer totalement la contrefaçon en ligne, ambition probablement illusoire, que de contrarier au maximum le fonctionnement des sites contrefaisants, afin de décourager ceux qui les gèrent[65] », ajoutant « [qu'il] s'agit aussi de rendre l'accès aux contenus illicites plus compliqué, moins aisé, de sorte qu'il soit moins attractif que l'offre légale[66] ». Dans le cadre de la régulation de l'Internet, l'État en est donc parfois conduit à devoir « se contenter de mesures globalement efficaces[67] ».

III. UNE INTERVENTION RÉGULATRICE SOUMISE AUX CONTRAINTES DES OBLIGATIONS INTERNATIONALES ET EUROPÉENNES DE L'ÉTAT

L'État est ainsi soumis à deux catégories de contraintes lorsqu'il entend exercer son contrôle sur des flux transfrontières circulant *via* Internet : d'une part, des contraintes résultant du droit international général qui fixe des limites pour l'exercice par les États de leurs compétences exécutives et, plus subsidiairement, juridictionnelle et, d'autre part, la nécessité pour l'État d'adapter ses interventions régulatrices en ajustant la réglementation lorsque celle-ci n'est pas adaptée aux réalités d'Internet ou en se fixant des objectifs plus modestes, notamment de restreindre la circulation de flux illicites plutôt que d'envisager leur suppression. D'autres contraintes viennent toutefois limiter davantage ses marges de manœuvre en la matière, notamment celles résultant des engagements internationaux de libéralisation économique (et notamment des relations commerciales) pris par l'État[68].

64. V. les ex. cités par P. Jacob, *op. cit.*, note 58, p. 425-426.
65. P. Lescure, *Contribution aux politiques culturelles à l'ère numérique*, mai 2013, p. 385.
66. *Ibid.*
67. P. Jacob, *op. cit.*, note 58, p. 426.
68. Il existe évidemment d'autres obligations internationales souscrites par les États au regard desquelles peuvent être évaluées les mesures prises par les États pour encadrer les flux transfrontières circulant par Internet. Il en est ainsi de la CEDH dans la mesure où les limitations d'accès à Internet

À cet égard, il apparaît utile de se pencher sur les solutions prescrites au regard du droit de l'OMC lorsqu'un État entend exercer son pouvoir réglementaire pour ce qui concerne une activité de nature transfrontière sur Internet (A). Ces solutions pourront être confrontées avec celles résultant du droit de l'UE dans le même domaine car elles tendent à mettre en perspective l'importance que peuvent avoir les processus d'harmonisation sur l'appréciation de la liberté réglementaire des États dans le contexte d'une intégration économique (B). Pour ces deux modèles, nous aurons recours au problème particulier que pose la réglementation des jeux en ligne dont on sait qu'ils constituent un commerce spécifique faisant l'objet d'un encadrement strict par les États[69].

A. Des contraintes de rationalité et de non-discrimination en droit de l'OMC

En 2004 et 2005, un groupe spécial et l'Organe d'appel de l'OMC ont rendu chacun un rapport particulièrement instructif dans le cadre de l'affaire opposant les États-Unis à Antigua-et-Barbuda à propos de certaines mesures adoptées par les États-Unis visant la fourniture transfrontière de services de jeux et paris[70]. Antigua-et-Barbuda contestait devant l'Organe de règlement des différends de l'OMC la réglementation américaine prohibant les services de jeux en ligne dès lors que ceux-ci étaient proposés par un prestataire étranger alors que cette prohibition n'affectait pas les prestataires américains. En ce sens, Antigua-et-Barbuda considérait que la réglementation américaine constituait une violation de plusieurs dispositions de l'Accord général sur le commerce des services (AGCS, plus connu sous l'acronyme anglais de GATS), et plus particulièrement son article XVI relatif à l'accès aux marchés.

Le premier élément méritant d'être mentionné à propos de ce différend se rapporte au débat concernant l'applicabilité du GATS, lequel illustre bien les difficultés résultant de l'application à des activités se déroulant sur Internet de textes qui n'avaient pas été conçus au moment où le réseau permettait de les envisager.

---

peuvent constituer des restrictions à la liberté d'expression. À titre d'illustration, la CEDH a récemment considéré que le blocage total du site YouTube prononcé par un tribunal turc du fait de la présence de vidéos constituant un outrage à la mémoire d'Atatürk violait l'article 10 de la Convention car « les autorités auraient dû notamment tenir compte du fait que pareille mesure, qui rendait inaccessibles une grande quantité d'informations, ne pouvait qu'affecter considérablement les droits des internautes et avoir un effet collatéral important » (CEDH 1er déc. 2015, *Cengiz et autres c/ Turquie*, req. n° 48226/10 et 14027/11, § 64).

69. On peut à cet égard rappeler l'art. 1er de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne (dont on peut discuter de la portée normative) et qui dispose que « l]es jeux d'argent et de hasard ne sont ni un commerce ordinaire, ni un service ordinaire ; dans le respect du principe de subsidiarité, ils font l'objet d'un encadrement strict au regard des enjeux d'ordre public, de sécurité publique et de protection de la santé et des mineurs ».

70. OMC, *États-Unis – Mesures visant la fourniture transfrontière de services de jeux et paris*, WT/DS285/R, Rapp. du groupe spécial du 10 nov. 2004 ; WT/DS285/AB/R, Rapp. de l'Organe d'appel du 7 avr. 2005.

Plus précisément, il s'agissait de déterminer si les États-Unis avaient pris des engagements de libéralisation qui intégraient les jeux et paris en ligne. En effet, dans le domaine du commerce des services, les États membres de l'OMC dressent des listes d'engagements par lesquelles ils réalisent des concessions de libéralisation pour des secteurs de service donnés et où ils précisent dans quelle mesure les secteurs envisagés sont libéralisés selon les quatre différents modes de prestation de services prévus par le GATS[71] : prestation transfrontière (Mode 1), consommation à l'étranger (Mode 2), présence commerciale (Mode 3) et présence de personnes physiques (Mode 4). Les États-Unis avaient pris des engagements de libéralisation dans le domaine des « services récréatifs » dans le cadre du Mode 1, ce qui a conduit le groupe spécial à considérer que cet engagement couvrait le domaine des jeux et paris[72] mais aussi que le Mode 1 s'appliquait à la fourniture de services par le biais d'Internet, précisant notamment qu'il ne convenait pas de faire de distinction entre les différents modes de livraison des services compte tenu d'un principe de neutralité technologique[73]. Si cela n'a pas été abordé frontalement par le groupe spécial, la question de l'adéquation du Mode 1 pour caractériser les services en ligne mérite d'être posée. En effet, ce mode avait été envisagé au moment de sa conception comme reflétant la situation où le service est produit à l'étranger puis transféré par divers moyens sur le territoire de l'État où se situe le consommateur (par exemple, la prestation d'un architecte ou d'un avocat[74]). C'est pourquoi il était tout aussi concevable d'envisager que l'activité de jeux en ligne s'inscrive dans le cadre du Mode 2 dans la mesure où c'est le consommateur qui se déplace à l'étranger, plus précisément sur le territoire de l'État où le site est hébergé[75]. Ces zones grises entre les Modes 1 et 2 suggèrent dans tous les cas que les États membres de l'OMC n'avaient pas pleinement conscience de l'éventuelle portée dans le futur de leurs concessions réalisées dans le cadre des listes d'engagements.

Au-delà de ces aspects, le principal enseignement de ce contentieux réside dans l'examen par l'Organe d'appel de la question de savoir si la restriction résultant de la réglementation américaine et constituant une violation de l'article XVI relatif à l'accès aux marchés était susceptible de se justifier sur le fondement de

71. GATS, art. I(2).

72. WT/DS285/R, *op. cit.*, note 70, § 6.135.

73. WT/DS285/R, *op. cit.*, note 70, § 6.285 (soulignant « qu'au titre de l'AGCS, le mode 1 englobe tous les moyens possibles de fournir des services depuis le territoire d'un Membre de l'OMC vers le territoire d'un autre Membre de l'OMC. Par conséquent, un engagement concernant l'accès aux marchés pour le mode 1 implique le droit pour les fournisseurs des autres Membres de fournir un service par tous les moyens de livraison possibles, que ce soit par courrier, téléphone, Internet, etc., à moins qu'il ne soit spécifié autrement dans la Liste d'engagements d'un Membre. Nous notons que cela est conforme au principe de "neutralité technologique" qui semble être largement partagé parmi les Membres de l'OMC »).

74. S. Wunsch-Vincent, « The Internet, Cross-Border Trade in Services, and the GATS : Lessons From US – Gambling », *World Trade Review* 2006, vol. 5, n° 3, p. 324 s.

75. *Ibid.* Il était difficile dans ce cadre d'envisager l'éventualité du Mode 3. S'il est vrai qu'il peut être établi que le site se focalisait sur le territoire des États-Unis, la présence commerciale visée par le Mode 3 s'entend strictement au sens du GATS comme l'établissement d'une filiale ou d'une succursale ou d'un bureau de représentation sur le territoire de l'État d'accueil (GATS, art. XXVIII(d)).

l'exception de moralité publique ou du maintien de l'ordre public prévue par l'article XIV du GATS. L'analyse à ce point de vue s'effectue principalement à deux niveaux. Il s'agit en premier lieu pour les juridictions de l'OMC de déterminer si les mesures en question sont « nécessaires à la protection de la moralité publique ou au maintien de l'ordre public[76] » puis, en second lieu, d'évaluer si, comme le prescrit le texte introductif de l'article XIV, elles ne sont pas « appliquées de façon à constituer soit un moyen de discrimination arbitraire ou injustifiable (…), soit une restriction déguisée au commerce des services ». Sur le premier point, l'Organe d'appel n'a pas eu de difficulté à reconnaître le lien de nécessité existant entre les réglementations américaines et la protection de la moralité publique ou le maintien de l'ordre public[77]. Il rappela à cet égard que les États-Unis avaient exposé de manière détaillée devant le groupe spécial des éléments qui établissaient un lien entre fourniture à distance de services de jeux et blanchiment d'argent, fraude, jeu compulsif et pratique du jeu par les mineurs[78]. Cependant, sur le second point, l'Organe d'appel a confirmé l'une des constatations du groupe spécial selon laquelle les États-Unis n'avaient pas appliqué la prohibition de la fourniture transfrontière de services de jeux et paris (notamment dans le domaine des courses de chevaux) à certaines entreprises américaines de la même façon qu'aux fournisseurs étrangers pour lesquelles les procédures ont été menées à leur terme[79] et, qu'en conséquence, cette pratique constituait une discrimination arbitraire et injustifiable ou une restriction déguisée au commerce[80].

Ainsi, dans le cadre de l'OMC, il est reconnu aux États le droit de réglementer des flux transfrontières transitant par Internet dès lors que cette réglementation est nécessaire à la protection de la moralité publique ou au maintien de l'ordre public, de même que d'autres exceptions sont envisagées dans l'article XIV du GATS, par exemple pour ce qui concerne la lutte contre les pratiques frauduleuses et la protection des données personnelles[81]. Cependant, dès lors qu'une réglementation est envisagée, celle-ci ne saurait être conçue ou appliquée de manière à générer une rupture de traitement injustifiée entre fournisseurs étrangers et nationaux. Sur ce point, il est important de préciser que la position des États-Unis devant les juridictions de l'OMC consistait à contester l'existence d'un traitement discriminatoire entre fournisseurs nationaux et étrangers et qu'ils n'ont pas cherché à justifier – ce qui aurait été délicat, mais éventuellement possible – les raisons d'un traitement préférentiel donné aux fournisseurs nationaux. Cet aspect a été justement abordé dans le contexte du droit de l'UE et, sans ambitionner de vouloir transposer les solutions de la CJUE à la jurisprudence de l'OMC, celles-ci apportent d'utiles réflexions en la matière.

76. GATS, art. XIV(a).
77. WT/DS285/AB/R, *op. cit.*, note 70, § 327.
78. WT/DS285/AB/R, *op. cit.*, note 70, § 313.
79. WT/DS285/R, *op. cit.*, note 70, § 6.588-589.
80. WT/DS285/AB/R, *op. cit.*, note 70, § 372.
81. GATS, art. XIV (c) (i) et (ii).

B. Des contraintes dépendant du niveau d'harmonisation en droit de l'UE

La réglementation des services de jeux d'argent et de hasard en ligne ne fait pas l'objet d'une harmonisation à l'échelon du droit de l'UE et ces activités sont d'ailleurs exclues du champ d'application de la directive CE « Commerce électronique » n° 2000/31[82] ainsi que de celui de la directive CE « Services » n° 2006/123[83]. Pour cette dernière législation, il était d'ailleurs précisé que l'exclusion se justifiait dans la mesure où ces activités « entraînent de la part des États membres la mise en œuvre de politiques touchant à l'ordre public et visant à protéger les consommateurs[84] ». Quoiqu'elles ne fassent pas l'objet d'une discipline en droit de l'UE, ces activités n'en demeurent pas moins soumises aux règles générales de l'article 56 du TFUE proscrivant « les restrictions à la libre prestation des services à l'intérieur de l'Union (…) à l'égard des ressortissants des États membres établis dans un État membre autre que celui du destinataire de la prestation ».

La question de la liberté réglementaire dont bénéficient les États membres de l'UE pour encadrer les activités transfrontières transitant *via* Internet s'est justement posée en 2009 dans le cadre d'un différend concernant les restrictions dont était l'objet l'entreprise de jeux en ligne Bwin International au Portugal. Cette société qui ne disposait d'aucun établissement au Portugal offrait *via* Internet des services de jeux en ligne par le biais de ses serveurs localisés à Gibraltar et en Autriche. Le site Bwin avait noué un partenariat avec la ligue portugaise de football en espérant que celui-ci profite à son activité de paris sportifs dans ce pays. C'est dans ce contexte que l'établissement portugais Santa Casa auquel a été confié par la loi un monopole de l'exploitation des jeux et paris sportifs au Portugal a infligé des amendes à la ligue et à Bwin. Ceux-ci ont contesté ces décisions en soutenant que l'exclusivité dont bénéficie Santa Casa, notamment en matière de jeux en ligne, constitue une restriction injustifiée à la libre prestation des services dans l'UE au regard de l'article 56 TFUE, question sur laquelle la CJUE s'est prononcée dans le cadre d'un renvoi préjudiciel[85]. La CJUE a admis que de telles restrictions peuvent être envisagées dès lors qu'elles se fondent sur « des raisons impérieuses d'intérêt général, telles que les objectifs de protection des consommateurs, de prévention de la fraude et de l'incitation des citoyens à une dépense excessive liée au jeu[86] ». En l'absence d'harmonisation européenne sur ces activités,

82. Art. 1er (5) (d) de la dir. CE n° 2000/31 du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *JOCE* 17 juill. 2000, n° L 178/1 (excluant « les activités de jeux d'argent impliquant des mises ayant une valeur monétaire dans des jeux de hasard »).

83. Art. 2 (2) (h) de la dir. CE n° 2006/123 du 12 déc. 2006 relative aux services dans le marché intérieur, *JOCE* 27 déc. 2006, n° L 376/36 (excluant « les activités de jeux d'argent impliquant des mises ayant une valeur monétaire dans les jeux de hasard, y compris les loteries, les casinos et les transactions portant sur des paris »).

84. Dir. CE n° 2006/123, *op. cit.*, note 83, Préambule, § 25.

85. CJUE 8 sept. 2009, *Liga Portuguesa de Futebol Profissional et Bwin International Ltd. c/ Departamento de Jogos da Santa Casa da Misericórdia de Lisboa*, aff. C-42/07.

86. *Ibid.*, § 56.

les États membres sont libres de fixer le niveau de protection recherché, dès lors que les mesures qui sont adoptées sont nécessaires et proportionnées par rapport aux objectifs visés, et appliquées de manière non discriminatoire[87].

La question centrale traitée par la Cour était donc de déterminer si le Portugal était fondé à octroyer des droits exclusifs à un seul établissement en matière de jeux en ligne afin d'assurer la réalisation des objectifs de lutte contre la criminalité et de protection des consommateurs des jeux de hasard. À ce point de vue, la Cour a reconnu que l'exclusivité dont bénéficie Santa Casa se justifie dans la mesure où cet établissement se plaçait sous le strict contrôle de l'État et offrait dès lors des garanties suffisantes à celui-ci pour ce qui concerne le respect des règles relatives à ces objectifs[88]. La CJUE a tenu à mettre en relief la spécificité de ces activités transfrontières sur Internet en soulignant que l'État membre ne dispose pas des mêmes possibilités de contrôle des opérateurs qui sont établis en dehors du territoire national et que l'absence d'une harmonisation européenne sur cette matière (ou du moins encore dans les limbes[89]) pouvait dès lors légitimement conduire l'État à considérer qu'un prestataire étranger n'est pas soumis à une réglementation appropriée permettant de constituer une garantie suffisante contre les risques de fraude et de criminalité[90]. La confiance qu'implique une reconnaissance mutuelle des prestataires étrangers ne saurait dès lors être décrétée pour des services tels que les jeux de hasard en ligne qui comportent des risques bien différents de ceux d'autres services plus traditionnels. Toutefois, comme l'a souligné la jurisprudence postérieure à cette affaire, l'État se doit d'être cohérent avec les objectifs qu'il s'assigne et les droits exclusifs accordés à des établissements nationaux ne pourraient être considérés compatibles avec le droit de l'UE si les établissements nationaux qui en bénéficient se lancent dans une politique commerciale agressive visant à encourager de manière déraisonnable la participation du public à ces activités afin de maximiser leurs profits[91].

* *
*

Loin de constituer un échelon d'intervention périmé et d'être désarmé pour réguler les flux transfrontières qui transitent par le biais d'Internet, l'État doit néanmoins composer dans un tel contexte avec un ensemble de contraintes qui dépendent essentiellement des activités concernées. Du point de vue du droit international général, ce sont surtout les limites relatives à la compétence exécutive de

87. *Ibid.*, § 57-60.

88. *Ibid.*, § 65.

89. V., *Vers un cadre européen global pour les jeux de hasard en ligne*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, COM (2012) 596 final, 23 oct. 2012.

90. *Ibid.*, § 68-69.

91. CJUE 8 sept. 2010, *Markus Sto• e.a. c/ Wetteraukreis*, *Kulpa Automatenservice Asperg GmbH e.a. c/ Land Baden-Württemberg*, aff. C-316/07, C-359/07 à C-360/07, C-409/07 et C-410/07, § 106 ; CJUE 8 sept. 2010, *Carmen Media Group Ltd c/ Land Schleswig-Holstein e.a*, aff. C-46/08, § 68.

l'État prohibant toute mesure coercitive à l'étranger[92] qui restreignent son champ d'action. Il dispose toutefois d'une palette d'instruments afin d'encadrer des contenus disponibles, en particulier ceux provenant de l'étranger et qui ciblent spécifiquement l'État souhaitant exercer sa compétence. Compte tenu de l'architecture du réseau, la régulation de flux transfrontières ne pourra pas en toutes occasions cibler ceux qui en sont à l'origine. C'est pourquoi l'État est conduit à réévaluer sa stratégie de régulation en se reposant sur divers acteurs qui participent à la circulation et à la diffusion de ces contenus (hébergeurs, fournisseurs d'accès et plus subsidiairement les moteurs de recherche). L'action de l'État se doit également de respecter certains principes relevant de ses engagements internationaux ou de ses obligations relevant du droit de l'UE. Si le droit de l'OMC lui reconnaît une liberté réglementaire, celle-ci ne doit pas être exercée de façon à générer une discrimination injustifiée entre fournisseurs de services étrangers et nationaux. À l'instar de ce que prescrit le droit de l'UE, l'intervention de l'État doit également se révéler cohérente, nécessaire et proportionnée par rapport aux objectifs d'intérêt général qui sont poursuivis. Dans le contexte spécifique de l'UE, l'État membre conserve une certaine marge de manœuvre dès lors que son intervention porte sur une matière qui n'a pas fait l'objet d'un processus d'harmonisation. L'idée qui se dégage de la jurisprudence de la CJUE en matière de jeux en ligne est que, dans certains domaines sensibles, il ne peut y avoir d'obligation de reconnaissance mutuelle dès lors que les droits nationaux ne convergent pas vers des règles communes. La question risque de se reposer dans le cadre de l'accord de partenariat actuellement en négociation entre l'UE et les États-Unis (TTIP) ou dans celui du *Trade in Services Agreement* (TiSA), mais il n'est pas certain que les solutions prescrites par les futurs tribunaux d'arbitrage établis dans ce cadre rejoignent les positions que l'on peut qualifier de raisonnables de la Cour de Luxembourg. Les arrêts rendus par celle-ci dans l'affaire visant Google pour le droit au déréférencement[93] ou plus récemment dans celle relative au mécanisme *Safe Harbor* qui permet un transfert de données à caractère personnel vers un pays tiers à l'UE[94] ont été vivement critiqués outre-Atlantique. Certains estiment en effet qu'ils imposaient aux entreprises américaines telles que Google et Facebook des contraintes déraisonnables méritant d'être contestées[95]. Si ces futurs accords sont fondés sur un principe de reconnaissance mutuelle des réglementations sans harmonisation préalable de celles-ci, il n'est pas certain que les marges de manœuvre reconnues par la CJUE trouvent grâce aux yeux de ces futurs tribunaux arbitraux.

92. Sauf règle de droit international contraire (v. *supra* I(A)).

93. V. *op. cit.*, note 5.

94. CJUE 6 oct. 2015, *Maximilian Schrems c/ Data Protection Commissioner*, aff. C-362/14.

95. V. par ex., S. Lester, *Should the « Right to be Forgotten » be Reviewed by an International Court ?*, 24 juill. 2014, <www.cato.org>.

Thèmes & Commentaires

INTERNET, ESPACE D'INTERRÉGULATION

Sous la direction de Marie-Anne Frison Roche

Contributeurs

Laurent Benzoni
Régis Bismuth
Sylvain Chatry
Nicolas Curien
Pascal Dutru
Marie-Anne Frison-Roche
Marie Jeunehomme
Frédérick Lacroix
Soumia Malinbaum
Myriam Quéméner
Maryvonne de Saint-Pulgent
Jean-François Vilotte

"Réguler Internet".

Certains affirment que toute régulation est contraire à la nature du numérique. D'autres soutiennent que cela est indispensable, et pour son déploiement économique et pour les libertés publiques.

Internet renouvelle les conceptions et les pratiques. Notamment celles du Droit de la Régulation. En effet, Internet permet d'offrir et d'obtenir des prestations qui relèvent souvent de secteurs régulés : prestations financières, audiovisuelles, de santé, de jeu. Plus encore, elles convergent dans de nouveaux objets : les objets connectés.

Souvent décrit comme un « désert juridique », le numérique apparaît alors comme une sorte de fatras de système de régulations diverses qui se superposent, se déforment et se contredisent.

En réaction, une « interrégulation », de fait ou de droit, en droit plus ou moins souple, est en train de s'établir.

Qui en sera le Régulateur : Les États ? Le juge ? L'internaute ?

L'ouvrage détermine tout d'abord les « Besoins d'interrégulation » pour ensuite décrire et concevoir les solutions d'interrégulation de l'espace numérique.

ISBN 978-2-247-15901-7
2331533
9 782247 159017

46 €

www.editions-DALLOZ.fr