

TITRE 7

La régulation des activités sur Internet : une gestion de risques en réseaux

Pierre TRUDEL*

Sommaire

La régulation qui trouve effectivement application à l'égard des activités se déroulant sur Internet est essentiellement une résultante. Elle découle des décisions des différents acteurs étatiques, corporatifs, associatifs, publics, privés qui gèrent leurs risques. Dans l'environnement d'Internet, la régulation s'applique selon un mode réseautique. Elle est pensée et produite dans les différents lieux qui produisent des normativités qui sont envisagées comme des risques par les autres acteurs. Les instances étatiques, les lieux de conception des normes techniques, de même que les différents acteurs, identifient les risques auxquels les exposent les normativités appliquées au sein du réseau et tentent de les gérer au mieux. Les acteurs relaient à leurs partenaires les exigences et les risques qu'ils ont à gérer. Ainsi envisagée, la régulation des activités se déroulant sur Internet est essentiellement une démarche continue de prise en compte et de gestion des risques perçus à l'égard des différents intérêts protégés.

Améliorer la compréhension des relations qui existent entre ces divers processus de gestion de risques accroît les chances d'une régulation effective des activités prenant place sur Internet. Dans un réseau, les régulateurs et les acteurs sont en position d'accroître ou de réduire les risques pour eux-mêmes ou pour d'autres. La technique joue comme une régulation par défaut qui produit des situations qui augmentent ou diminuent les risques. Il en est de même pour les lois étatiques, principalement celles des entités dominantes comme l'Union européenne ou les États-Unis. Les acteurs du net envisagent les contraintes et possibilités techniques, de même que les lois qui sont susceptibles de s'appliquer à leurs activités

* Professeur titulaire, Centre de recherche en droit public, Faculté de droit, Université de Montréal, www.pierretrudel.net/pierre.trudel@umontreal.ca.

comme autant de risques à gérer. Les acteurs cherchent à accroître, à transférer ou à limiter les risques qu'ils sont en mesure de percevoir. L'efficacité de la régulation des activités sur Internet est fonction de la capacité effective d'accroître les risques de ceux qui mènent des activités à risque et de gérer les risques des utilisateurs légitimes.

Introduction

Dans l'environnement cyberspatial constitué d'une multitude d'objets connectés, les conditions de la circulation de l'information sont transformées. Internet prend l'aspect d'un espace d'interactions ayant vocation à embrasser la presque totalité des dimensions de la vie sociale. Yves Poulet constate qu'Internet favorise une double globalisation. Dans un premier sens, par la dimension internationale des réseaux et leur convergence et, dans un second sens, dans la mesure où l'ensemble des activités est traduit en information numérique¹.

Le processus de globalisation² qui caractérise la généralisation du basculement de la plupart des activités d'interrelations dans les environnements Internet emporte la nécessité de penser en conséquence le droit et la normativité³.

Sur Internet, les repères spatiaux et temporels sont modifiés. Les balises conçues dans un monde dans lequel les réseaux prenaient moins de place sont prises en défaut. Des enjeux inédits dans le monde physique se manifestent avec une grande acuité dans l'espace en réseaux⁴. La disponibilité d'outils de captation et de diffusion comporte un potentiel significatif d'accroissement des risques associés aux droits fondamentaux.

Dans un univers où pratiquement toute personne dispose d'outils capables de capter, d'enregistrer et de diffuser des sons et images, il devient possible de pratiquement tout documenter. Ces possibilités peuvent aider à faciliter le repérage des comportements attentatoires aux droits, mais

¹ Y. POULET, « Mieux sensibiliser les personnes concernées, les rendre acteurs de leur propre protection », [2005] 5 *Revue Lamy Droit de l'immatériel*, 47, note 66.

² Le mot est ici utilisé pour désigner le processus d'interconnexion croissante des économies et sociétés résultant du développement des technologies de l'information. C. GHORRAGOBIN, *Dictionnaire des mondialisations*, Paris, Armand Colin, 2006, p. 185.

³ P. TRUDEL, « Quel droit et quelle régulation dans le cyberspace ? », *Sociologie et sociétés*, vol. 32, n° 2, automne 2000, pp. 189-209.

⁴ Fr. SCHAUER, « Internet privacy and the public-private distinction », [1998] 38 *Jurimetrics* 555.

elles peuvent également augmenter les risques à l'égard de ceux-ci. Les risques pour la dignité humaine se présentent à des échelles différentes. Il y a reconstruction des cercles de la vie privée. Il y a décentrage et recentrage des cercles au sein desquels s'exercent les droits.

On observe un décentrage spatial : l'espace physique semble se dissoudre dans le cyberspace. Le lieu dans lequel est située l'information a peu d'impact sur son accessibilité. Dès lors qu'un document est disponible sur un serveur, les outils de recherche couramment utilisés sur Internet ou certains outils spécialisés sont en mesure de le retrouver. L'éloignement dans l'espace de même que le passage du temps semblent avoir beaucoup moins de prise sur la disponibilité effective de l'information.

Avec la généralisation des environnements en réseau, la dissémination de l'information est banalisée. L'information peut aisément être diffusée en dehors des cercles de circulation légitimes, d'où l'accroissement des risques. Les repères permettant de délimiter le privé du public sont brouillés⁵.

L'échelle spatiale à partir de laquelle s'apprécient les risques pour les droits est modifiée. En dehors du monde en réseau, l'accessibilité à une information demande des ressources qui peuvent être importantes. Dans l'environnement interconnecté, beaucoup d'informations sont à portée d'une requête de moteur de recherche⁶.

Il y a aussi décentrage temporel : la persistance de l'information emporte que celle-ci traverse les cercles dans lesquels elle était tenue pour légitime. Par exemple, une information peut être légitimement disponible au public en raison de l'actualité de l'événement. L'archivage et la disponibilité virtuellement permanente sur Internet iraient au-delà de ce qui est nécessaire afin de rendre compte de l'actualité.

Les capacités d'agglomération d'informations permettent la constitution de gisements d'informations sur les personnes qui peuvent du coup devenir disponibles pour des forces de police, de même que devenir des enjeux pour des malfaiteurs. En somme, la disparition des efforts à consacrer pour trouver l'information emporte la disparition d'une protection par défaut de la vie privée. Cela porte à revoir les raisonnements qui permettraient de déterminer si on se trouvait dans le domaine de la vie privée ou dans le domaine de l'espace public.

⁵ K. D. BELGUM, « Who leads at half-time? Three conflicting visions of internet privacy policy », [1999] 6 *Rich. J.L. & Tech.* 1.

⁶ D. J. SOLOVE, « Access and aggregation: public records, privacy and the Constitution », [2002] 86 *Minn. L. Rev.*, 1137-1218, p. 1139.

Tous ces changements dans les dimensions des enjeux relatifs aux droits indiquent des modifications dans les niveaux de risques causés par la circulation de l'information dans le réseau. Ces dimensionnements nouveaux des risques induisent des mutations au niveau de la raison d'être des règles de droit. Là où l'on prenait pour acquis que le niveau de risques demeurerait faible ou aisément maîtrisé, les mutations dans l'échelle qualitative et temporelle qu'induit la généralisation d'Internet conduisent à postuler que les risques sont accrus. D'où les revendications pour un renforcement de la protection des droits des personnes.

Malgré le caractère global du réseau, les appréciations et les valeurs demeurent différentes dans les divers milieux culturels dans lesquels les règles ont vocation à s'appliquer⁷. Il existe des phénomènes contribuant à moduler les normativités énoncées et qui empêchent leur application de bout en bout du réseau. De tels phénomènes préviennent l'application de règles qui pourraient être décontextuées par rapport aux situations ou au substrat culturel dans lequel la norme s'applique. Au nombre de ces phénomènes, il y a le risque juridique : l'évaluation que font les acteurs des possibilités concrètes d'application effective de lois nationales ou d'autres règles à leurs activités permet d'expliquer que, même si Internet est un réseau global, personne ne se sent tenu de se conformer à la totalité des lois nationales qui peuvent théoriquement trouver application⁸.

Car l'un des traits caractéristiques de l'espace virtuel constitué par Internet est la pluralité des normes qui peuvent potentiellement trouver application. Michel Vivant, après avoir pris acte des divers modèles de régulation agissant sur Internet, constate que « c'est bien de régulations – au pluriel – qu'il convient de parler, de modes de régulation qu'il convient d'articuler au mieux de combiner en raison : contrats, usages (coutumes), lois⁹ ». Philippe Amblard observe que la régulation de l'Internet se caractérise par le pluralisme de son processus normatif qui tendrait à promouvoir l'efficacité sociale d'un droit vivant par opposition à « l'artificialité positiviste de la loi étatique »¹⁰.

Pour plusieurs observateurs, il faut parler d'une multirégulation, de coexistence sur le réseau de plusieurs types de régulation répondant à des

⁷ J. GOLDSMITH et T. WU, *Who Controls the Internet? Illusions of a Borderless World*, New York, Oxford University Press, 2006, chap. 9 « Consequences of borders ».

⁸ Voy., pour une méthodologie d'analyse des risques juridiques : Fr. VERDUN, *La gestion des risques juridiques*, Paris, Éditions d'organisation, 2006, pp. 39 et s.

⁹ M. VIVANT, « Internet et modes de régulation », in É. MONTERO, *Internet face au droit*, Bruxelles, Story Scientia, 1997, 215, p. 229.

¹⁰ Ph. AMBLARD, *Régulation de l'Internet, l'élaboration des règles de conduite par le dialogue internormatif*, Bruxelles, Bruylant, 2004, n° 80.

objectifs différents, par des méthodes différentes et également légitimes¹¹. La régulation des activités se déroulant sur Internet peut être envisagée selon le modèle du réseau. Le cyberspace, constate Thomas Schultz, constitue un laboratoire intéressant des phénomènes juridiques contemporains¹². Le fonctionnement de la régulation doit être examiné en portant attention aux flux de normativité qui constituent la base du droit effectivement appliqué dans le cyberspace.

Prenant acte du fait qu'Internet est essentiellement construit sur un réseau technique ayant engendré un espace numérique au sein duquel se manifeste une pluralité de régulations, des auteurs réunis par Marie-Anne Frison-Roche n'hésitent pas à analyser Internet comme un espace d'interrégulations¹³.

Il existe un large consensus pour convenir qu'une pluralité de normes, de normativités est appliquée dans l'espace-réseau. Mais quels sont les facteurs qui contribuent à déterminer, dans un contexte spécifique donné, laquelle des règles sera effectivement appliquée ?

L'encadrement normatif d'Internet peut s'envisager dans le contexte des risques que la technologie paraît induire. La régulation d'Internet se présente comme un ensemble de décisions de gestion des risques qui sont perçus par les acteurs au sein du réseau.

Chapitre 1. La régulation envisagée selon une logique de risques

Sur Internet, les usagers et autres acteurs gèrent leurs risques. Lors du déroulement d'activités dans le cyberspace, les usagers et autres acteurs ont à décider s'ils acceptent les risques ou, le cas échéant, comment ils les transfèrent. Pour leur part, les États peuvent mettre en place des mesures afin d'accroître ou de limiter les risques que peuvent avoir à prendre les internautes à l'égard desquels s'appliquent leurs lois. Mais encore là, pour

¹¹ Th. SCHULTZ, *Réguler le commerce électronique par la résolution des litiges en ligne*, Bruxelles, Bruylant, 2005, p. 162. Cet auteur rapporte les points de vue de la Mission interministérielle sur l'Internet et du Conseil supérieur de l'audiovisuel. Il relate les observations de M. MAESSCHALCK et T. DEDEURWAERDERE, « Autorégulation, éthique procédurale et gouvernance de la société de l'information », in J. BERLEUR, Chr. LAZARO et R. QUECK, *Gouvernance de la société de l'information*, Bruxelles, Bruylant – Presses universitaires de Namur, 2002, pp. 77-103.

¹² Th. SCHULTZ, « La régulation en réseau du cyberspace », [2005] 55 *R.I.E.J.*, 31, p. 32.

¹³ M.-A. FRISON-ROCHE (dir.), *Internet, espace d'interrégulation*, Paris, Dalloz, 2016.

les acteurs du net, les lois des États se présentent à leur tour comme des risques à gérer. Le droit des États et les autres normativités –comme les normes issues de la technique – créent plus ou moins de risques pour les acteurs qui agissent dans le réseau.

Envisagés selon une logique de réseau, les droits et les obligations sur Internet s'expriment au moyen d'une normativité résultant des décisions de gestion des risques prises par les régulateurs et les acteurs actifs sur le net. Par leurs décisions et leurs comportements, l'ensemble de ces producteurs de normativités crée et relaie à ses cocontractants et partenaires les risques issus de la normativité qui leur est applicable. Les producteurs de normes ne peuvent prétendre à l'entière souveraineté dans le cyberspace, mais ils conservent une pleine capacité de formuler des règles qui engendrent des risques pour les acteurs.

SECTION 1. – Le risque

La régulation d'Internet trouve une grande partie de ses justifications dans les risques perçus à l'égard de ce que peut causer son utilisation mal encadrée¹⁴. Maryse Deguergue relève que le risque peut être classé parmi les notions axiologiques qui traduisent le réel tout en portant sur lui un jugement de valeur, lequel permet de poser des règles juridiques¹⁵.

Les perceptions diverses ou convergentes au sujet des risques d'Internet contribuent à construire les légitimations sur lesquelles se fondent les règles de droit qui prétendent en encadrer le fonctionnement. L'anticipation, la gestion et la répartition des risques figurent parmi les grandes préoccupations des systèmes juridiques. Ulrich Beck remarquait la transformation de la société moderne en société du risque. Le fait de discuter des risques que la société produit elle-même, et le fait de les anticiper et de les gérer sont au cœur de ses préoccupations¹⁶.

Dans son acception générale, le risque peut être envisagé comme un objet social. Yvette Veyret observe que « le risque objet social se définit comme la perception du danger. Le risque n'existe que par rapport à un individu, à un groupe social ou professionnel, une communauté, une

¹⁴ P. TRUDEL, « Le risque, fondement et facteur d'effectivité du droit », in K. BENYKHELF, *Gouvernance et risque-Les défis de la régulation dans un monde global*, Montréal, éd. Thémis, 2013, pp. 241-271.

¹⁵ M. DEGUERGUE, « Risque », in D. ALLAND et St. RIALS, *Dictionnaire de la culture juridique*, coll. Quadrige, Paris, Lamy, PUF, 2003, p. 1372.

¹⁶ U. BECK, « Risque et société », in S. MESURE et P. SAVIDAN, *Le dictionnaire des sciences humaines*, coll. Quadrige, Paris, PUF, dicos poche, 2006, p. 1022.

société qui l'appréhende [...] et le traite par des pratiques spécifiques. Il n'y a pas de risque sans une population ou un individu qui perçoit et pourrait subir ses effets »¹⁷. Le risque n'existe pas dans le vide : il découle forcément d'un contexte sociétal donné.

La protection des droits relève bien d'une logique des risques. Les conséquences de la circulation des informations ne sont pas nécessairement connues des protagonistes lorsque l'information est mise en circulation. C'est souvent l'agglomération d'informations qui est considérée comme porteuse de dangers. Par exemple, une information personnelle anodine peut être diffusée, puis se retrouver combinée avec un autre élément d'information et entraîner de ce fait une divulgation d'un élément de l'intimité d'une personne. Dans une pareille situation, l'intéressé a consenti à la divulgation, ou encore le caractère public de la situation faisait sortir l'information du champ de la vie privée. Mais l'intrusion dans la vie privée survient quand même. C'est dire le caractère factice et insuffisant d'une approche qui persisterait à postuler que le consentement de l'individu est une condition nécessaire et suffisante pour assurer la protection de l'internaute¹⁸.

Une fois reconnu, le risque emporte des obligations de précaution. Le risque juridique découle, en effet, des situations où la violation des droits d'autrui est susceptible de se produire. Même s'ils sont différents, il y a une étroite proximité entre le risque technologique et le risque juridique : lorsque le risque technologique est avéré, il naît presque toujours une obligation d'en tenir compte et de se comporter de façon conséquente. Le risque juridique peut aussi découler de la possible non-conformité à une loi ou à une autre sorte d'obligation également applicable. Le risque juridique, en toute hypothèse, résulte des situations dans lesquelles la responsabilité d'une personne peut être mise en cause.

Ceux qui prennent part à des activités dans le cyberspace le font avec plus ou moins d'intensité selon qu'ils ont ou non conscience qu'ils auront à supporter plus ou moins de risques. La protection des droits sur Internet s'inscrit dans le tissu des impératifs de modulation et de gestion des risques.

¹⁷ Y. VEYRET, « Les risques », *Dossier des images économiques du monde*, FEDES, cité par Fr. VERDUN, *La gestion des risques juridiques*, Paris, Éditions d'organisation, 2006, p. 11.

¹⁸ V. GAUTRAIS et P. TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, éd. Thémis, 2010, pp. 163 et s.

SECTION 2. – La normativité en réseau

La gestion des risques s'inscrit dans un processus de régulation en réseau¹⁹. Dans les espaces constitués par les réseaux, le cyberspace, la normativité s'élabore et s'applique selon un mode réseautique²⁰. Les réseaux sont le résultat d'interactions entre personnes se trouvant en relation. Le réseau suppose des environnements interconnectés unissant les acteurs, les régulateurs, de même que les entités jouant un rôle dans la gouvernance d'Internet²¹. Renaud Berthou voit en Internet « un facteur de développement d'une pluralité de processus réseautiques ». Sans être la seule cause du développement réseautique que connaissent les processus de création du droit à l'ère postmoderne, il est un outil majeur d'évolution²².

Au sein du réseau, l'acteur gère ses risques et va chercher à les limiter ou à les transférer à ses partenaires. Par exemple, l'exploitant d'un site de réseautage social va prévoir des mises en garde afin d'amener les usagers à accepter consciemment les risques découlant de la mise en ligne de leur profil personnel. D'autres acteurs pourront songer à mettre en place des mécanismes afin de consigner les consentements aux traitements de données personnelles aux fins de limiter les risques résultant de l'application des lois nationales sur la protection des données personnelles qui seraient susceptibles de trouver application.

Les régulations peuvent découler de normativités technologiques, de normativités gestionnaires ou de normativités juridiques. Rien n'indique que la normativité juridique ou une autre logique normative soit invariablement en position dominante. Il y a, en effet, concurrence entre les diverses logiques en vertu desquelles se produisent les régulations : les logiques technologiques, celles du marché et les logiques du droit ne

¹⁹ K. J. STRANDBURG, G. CSARDI, J. TOBOCHNIK, P. ÉRDI et L. ZALANYI, « Law and the science of networks: an overview and an application to the "patent explosion" », [2006] 21 *Berkeley Technology L.J.*, pp. 1293-1351 ; A. M. MATWYSHYN, « Of nodes and power laws: a network theory approach to internet jurisdiction through data privacy », (2003) 98 *Nw.U.L.Rev.*, pp. 494-544 ; A. AVIRAM, « Regulation by networks », [2003] *Brigham Young U. L. Rev.*, pp. 1180-1238 ; L. J. STRAHILEVITZ, « Asocial networks theory of privacy », [2005] 72 *U. Chi. L. Rev.*, pp. 919-988.

²⁰ P. TRUDEL, « Un "droit en réseau" pour le réseau : le contrôle des communications et la responsabilité sur Internet », in Institut canadien d'études juridiques supérieures, *Droits de la personne : Éthique et mondialisation*, Cowansville, Éditions Yvon Blais, 2004, pp. 221-262.

²¹ M. CASTELLS, *La société en réseaux. L'ère de l'information*, Paris, Fayard, 1998 ; Fr. OST et M. DE KERCHOVE, *De la pyramide au réseau : pour une théorie dialectique du droit*, Bruxelles, Publications des facultés universitaires Saint-Louis, 2002.

²² R. BERTHOU, *L'évolution de la création du droit engendrée par Internet : vers un rôle de guide structurel pour l'ordre juridique européen*, thèse pour le doctorat de l'Université de Rennes I, mention Droit, Rennes, 2 juillet 2004, p. 373.

concordent pas toujours. Dans certaines situations, les référents juridiques demeurent absents des débats qui sont perçus comme relevant essentiellement d'une problématique de gestion ou d'agencement technique. Dans d'autres contextes, l'enjeu technique est fortement capté par les logiques juridiques.

L'État ou un autre acteur peut agir afin d'augmenter les risques de certains comportements ou activités ou réduire les risques associés à une conduite saine. Par exemple, lorsque l'État adopte une loi sévère contre certaines pratiques, cela accroît les risques associés à celles-ci. À l'égard des usagers qui se livrent à des activités légitimes, l'État peut baliser, voire limiter, les risques des acteurs. Si, dans le cyberspace, l'État semble avoir perdu de son pouvoir, sa capacité d'édicter et d'appliquer des règles qui mettent les acteurs à risque lui procure encore une importante influence sur les entités situées sur son territoire et même sur celles qui sont susceptibles d'être indirectement visées par ses lois.

Dans un réseau, chacun des acteurs en mesure d'imposer sa volonté dispose d'une capacité d'accroître les risques des autres. Ainsi, un État peut imposer des devoirs aux citoyens qui se trouvent sur son territoire. Ces derniers auront alors à gérer leurs risques découlant de ces obligations. Ils chercheront à s'assurer que leurs partenaires agissent en conformité avec les obligations auxquelles ils sont eux-mêmes tenus et à l'égard desquelles leur responsabilité peut se trouver engagée.

En somme, la régulation en réseau découlant des processus multiples de gestion des risques constitue le principal vecteur de maintien des équilibres entre les risques et les précautions. Ces processus de régulation doivent fonctionner de façon à inciter l'ensemble des acteurs à minimiser les risques qui relèvent de situations sur lesquelles ils sont effectivement en mesure d'avoir une prise et à accroître le plus possible les risques des acteurs qui choisissent d'avoir des comportements dommageables ou qui augmentent indûment les risques des usagers légitimes.

Sur Internet, les régulateurs ont à composer avec les traits caractéristiques du cyberspace. C'est en augmentant les risques de ceux qui font des activités que l'on souhaite encadrer qu'ils ont le plus de chances d'assurer effectivement un meilleur niveau de régulation.

Le risque en tant que construction sociale sera apprécié de façon différente selon les époques et selon le contexte culturel, politique ou social²³. Les représentations des dangers et des bienfaits des technologies contribuent à la construction des perceptions collectives des risques et des bénéfices des objets techniques. Ces perceptions varient dans le temps :

²³ Chr. NOVILLE, *Du bon gouvernement des risques*, Les voies du droit, Paris, PUF, 2003.

elles ne sont pas identiques à toutes les époques. Elles diffèrent également selon les contextes sociaux : le droit et les autres normativités procèdent en grande partie de ces perceptions variables reflétant les contextes sociétaux et historiques.

Les acteurs d'Internet évaluent les risques qu'une mesure ou une règle s'applique à leur activité. La décision de se conformer à telle règle et pas à d'autres procède d'une démarche d'évaluation des risques juridiques. Le potentiel d'application du droit de tel ordre juridique est évalué par chacun des acteurs en fonction de divers facteurs, tels que les possibilités effectives de poursuites, la possession d'actifs sur le territoire étatique concerné, le désir d'inspirer confiance ou de se comporter en « bon citoyen ». Ces facteurs concourent aux analyses par lesquelles les acteurs orientent leurs stratégies de gestion de risques.

Chapitre 2. La gestion des risques en réseau

Internet peut être envisagé comme un univers constitué de nœuds et de relais de normativité qui sont en lien d'influence. La normativité effective est une résultante du dialogue entre les acteurs et de leur capacité à relayer les normes et principes. Pour connaître les normes qui ont vocation à régir un environnement raccordé à Internet, il faut identifier les nœuds au sein desquels s'énonce la normativité qui s'applique effectivement²⁴. Par exemple, un État énonce des lois qui seront obligatoires pour ceux qui sont situés sur son territoire. Les relais contribuent à la fois à mettre les nœuds de normativité en présence l'un de l'autre ou à les distancier. Par exemple, une entreprise régie par les lois du Québec devra, pour gérer adéquatement ses risques, exiger de ses cocontractants qu'ils assurent la protection des données personnelles telle que prévue par le législateur québécois. En vertu d'autres relations juridiques, cette même entreprise sera possiblement tenue de respecter les règles de la législation européenne. À leur tour, les cocontractants vont devoir s'assurer de respecter les exigences contractuelles, tout en composant avec les normes techniques qui s'imposent à eux.

Ainsi, une stratégie de renforcement de la protection des droits s'envisage comme un ensemble de mesures conçues de manière à se renforcer les unes et les autres afin de limiter les risques pour les internautes qui

²⁴ P. TRUDEL, « Un "droit en réseau" pour le réseau : le contrôle des communications et la responsabilité sur Internet », *op. cit.*, pp. 221-262.

s'adonnent à des activités licites. La stratégie doit se déployer en réseau : imposer des règles aux acteurs et inciter ces derniers à relayer ces exigences à tous ceux à l'égard desquels ils exercent une influence.

Dans une logique de gestion de risques, les mesures étatiques seront plus efficaces si elles empruntent des approches conséquentes présentant un potentiel de générer un degré significatif de conformité. Une législation notoirement non appliquée pourra plus aisément être perçue par les acteurs comme engendrant moins de risques.

Pour plusieurs acteurs dans le cyberspace, le droit de la responsabilité énoncé et appliqué par les États fournit une part importante du cadre délimitant leurs actions et prescrivant l'étendue de leurs obligations. C'est pour gérer leurs risques et limiter la mise en cause possible de leur responsabilité que les acteurs, tant collectifs qu'individuels, se donnent des règles de conduite. Ainsi se relaient les exigences énoncées dans les pôles de normativité. Au niveau de chaque environnement, les principes énoncés dans les pôles de normativité comme les lois des États et les principes largement reconnus sont relayés en microrégulation ou en autoréglementation.

La structure en réseau du droit du cyberspace permet de rendre compte des relations multiples qui existent entre les différents ordres normatifs agissant sur le net. Le paradigme de la gestion du risque procure une hypothèse explicative au regard de l'effectivité des normes. L'effectivité des règles serait fonction de leur capacité à promouvoir une gestion optimale du risque qu'elles permettent aux acteurs de visibiliser. Le risque concernant ici aussi bien le péril justifiant la mise en place de la norme elle-même que les sanctions et autres contraintes qu'engendre cette dernière.

Dans le réseau, on observe des interrelations diversifiées entre les normes. Les normes sont proposées, voire imposées, dans divers nœuds de normativité ; ces nœuds de normativité sont en concurrence ou en complémentarité avec d'autres. Les relais de la normativité assurent l'application effective des règles. Dans les relais s'explicitent et se diffusent les normativités et les conséquences de celles-ci.

On peut identifier plusieurs rapports entre les normativités. Dans la plupart des situations, on se trouvera en présence d'un rapport d'obligation. Une loi est obligatoire à l'égard d'une personne située sur le territoire d'un État. Cette dernière – au risque de devoir subir des sanctions – doit forcément relayer les obligations découlant de la loi. On voit ici l'importance du risque découlant de l'effectivité de la loi. Une loi non appliquée par les autorités pourra être perçue comme engendrant un risque négligeable. C'est dire l'importance de limiter la quantité de lois. La multiplication des textes ne visant que des effets d'annonce sans les ressources

assurant l'effectivité de son application contribue à affaiblir l'efficacité de la loi étatique.

Dans d'autres situations, l'application indirecte de normes émanant en tout ou en partie d'autres ordres juridiques sera envisagée comme un risque. Par exemple, les directives européennes ont des effets non seulement sur le droit des pays membres, mais aussi sur les obligations des acteurs situés dans des pays entretenant des relations importantes avec les ressortissants de cette entité. Il en est de même des lois américaines : plusieurs sites exploités partout dans le monde considèrent qu'il est de bonne pratique de se conformer à certaines lois américaines puisqu'ils ambitionnent de rejoindre des ressortissants de ce pays.

La régulation des usages sur Internet résulte donc souvent aussi bien du droit national du pays où l'on se trouve que du droit des ordres juridiques des entités en position d'exercer une influence sur les autres lieux d'élaboration de normes.

Des lieux de normativité produisent des normes ou des processus de coordination, tandis que d'autres fonctionnent comme des espaces de négociation ou d'équilibrage appliquant des régulations dans un rapport de dialogue avec d'autres lieux de normativité. Par exemple, c'est souvent à la suite d'invitations de la part des organisations internationales que les États sont amenés à relayer des normes dans leurs législations. Par exemple, la *Convention sur la cybercriminalité*²⁵ a été mise de l'avant par les instances européennes et ouverte à la signature d'autres pays.

En fin de compte, lorsqu'on s'engage dans une activité sur Internet, il faut habituellement envisager les risques de possible non-conformité à une gamme étendue de normes. Si les lois du territoire sur lequel on se trouve s'imposent d'office, on peut aussi avoir à composer avec des règles, légales, techniques ou des pratiques qui émanent d'un vaste ensemble de lieux normatifs.

Conclusion

Sur Internet, l'utilisateur et les autres acteurs gèrent leurs risques : ils les acceptent ou les transfèrent, ils peuvent choisir de les limiter ou de les minimiser. C'est pourquoi la régulation des activités se déroulant sur

²⁵ Conseil de l'Europe, *Convention sur la cybercriminalité*, Budapest, 23 novembre 2001 < <http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185> (consulté le 15 septembre 2017).

Internet fonctionne selon un modèle de gestion de risques. Un ensemble de systèmes de normes se discute et s'applique dans le cyberspace. Aux réglementations étatiques et celles des acteurs s'ajoutent des processus ayant vocation à procurer les encadrements pour des activités qui ne peuvent être entièrement régies par les droits territoriaux. La technique et les contraintes qu'elle induit sont aussi source de normativité dans les réseaux. L'espace auquel on a affaire est un ensemble interconnecté constitué de pôles interagissants de normativités. Il est constitué d'espaces dans lesquels prévalent en tout ou en partie des normes qui s'imposent aux usagers.

Envisagée comme un ensemble de risques à gérer, la régulation d'Internet se comprend comme un ensemble de normes qui sont forcément relayées via une pluralité de processus. L'incitation à relayer les exigences d'une règle de manière à obliger l'autre dépend de la capacité de cette règle à générer un risque qui sera perçu comme significatif par les acteurs concernés.

La normativité issue de la technique augmente les risques ou se propose afin de procurer des solutions limitant les risques pour la vie privée. L'État et les autres régulateurs peuvent accroître ou limiter les risques. Les décisions de gestion des risques qui se prennent dans les divers lieux en mesure d'imposer leur volonté engendrent des normes qui, à leur tour, sont relayées par les autres acteurs. Les États peuvent imposer des obligations qui limitent les risques pour la vie privée. Sur Internet, ces mesures seront à leur tour généralement perçues par les acteurs comme autant de risques à gérer et à transférer aux cocontractants.

L'ensemble des normativités agissant sur Internet peut être représenté selon un modèle réseautique. Les activités se déroulant sur Internet sont ainsi encadrées par une normativité en réseau dont le caractère effectif dépend largement de la capacité des producteurs de normes à créer des risques suffisants pour les autres entités afin de motiver chez les autres acteurs une volonté de les gérer. Tout se passe comme si le réseau était un vaste lieu au sein duquel les acteurs gèrent les risques qu'ils perçoivent en les relayant à ceux avec lesquels ils viennent virtuellement en contact.