Melanie Dulong de Rosnay, Responsabilité, in Cécile Méadel, Francesca Musiani (dir.), *Abécédaire des architectures distribuées*, Presses des Mines, November 2015, p. 203-208.

Les architectures distribuées, ne disposant pas d'autorité centrale, remettent en question la notion juridique de responsabilité qui alloue traditionnellement une action à un auteur ou un groupe d'auteurs identifiables. Cette entrée propose de discuter l'impact des caractéristiques socio-techniques de fragmentation et d'anonymisation des communications des architectures distribuées sur le droit de la responsabilité. Le contexte du droit positif français, européen et international est prolongé par un éclairage sur le rôle des usagers et leur responsabilité éthique à la pérennité de services sur la base de biens communs. Ces services peuvent en effet s'avérer indispensables, en l'absence d'alternatives publiques ou privées, dans un contexte d'infrastructures défaillantes ou inaccessibles en raison de la crise économique, d'une catastrophe naturelle ou d'une surveillance des réseaux par les gouvernements et les entreprises.

L'impact de la fragmentation et de l'encryption

L'architecture des applications distribuées rend difficile ou impossible l'identification des parties et des informations qui circulent. Le droit a pour habitude de déterminer des responsabilités, des droits, des devoirs, des interdictions, des conditions entre des personnes physiques ou morales fixes et dans des juridictions déterminées ou localisées. Or les AD, non seulement ne sont localisées en un ou plusieurs lieux déterminés, mais fragmentent les données dans un processus partagé entre des acteurs qui n'ont pas de contrôle ni de visibilité complète sur ce qui circule. L'encryption et la fragmentation des données conduisent à l'anonymat relatif des acteurs et à un brouillage des responsabilités si on ne peut pas attribuer un acte à une personne précise, s'il y a une distinction entre la demande de l'action et la mise en œuvre de l'action. Ces services remettent en question la méthode de recherche de la personne « responsable » (Dulong de Rosnay, 2014).

Dans le cas du stockage distribué (lien entrée Stockage distribué), l'utilisateur n'a pas connaissance des fragments qu'il stocke, dans la mesure où ils sont encryptés à la sortie de la machine de l'utilisateur qui demande le stockage et sera la seule personne a avoir accès au mot de passe, qui n'est pas stocké par un serveur central du service. Aucune entité extérieure (la police, l'Hadopi ou une major du disque) ne peut surveiller les fichiers qui ne circulent à aucun moment dans un format reconstitué perceptible aux sens, en dehors de la machine du premier pair qui télécharge frangement encrypté par fragment encrypté. Dans le cas des réseaux wifi communautaires à l'AD (lien entrée mesh), les utilisateurs reliés ensemble créent un réseau ouvert à d'autres, sans tracer ni stocker les métadonnées des connexions ni leur contenu. De même, Tor (lien entrée Tor) va dissimuler l'origine et la destination des communications en opérant par au moins trois routeurs intermédiaires qui ne verront pas ce qui transite.

L'absence de propriétaire et de contrat entre les parties ne donne pas d'indice de relation juridique préexistante. Les utilisateurs ne sont ni enregistrés ni identifiés, leur présence est instable et il est difficile d'assigner une responsabilité à un réseau complexe d'utilisateurs. Il n'est pas possible d'inférer de leur présence en ligne leur connaissance des paquets qu'ils aident à circuler partiellement et par intermittence. Leur présence n'est d'ailleurs pas essentielle, s'ils ne sont pas connectés, le paquet prendra une route différente et la redondance assurera le fonctionnement du service, ce qui diminue encore la responsabilité technique individuelle de chaque nœud. Les AD agrègent et redistribuent des fragments insignifiants ou des paquets encryptés de manière imprévisible, alors que le droit recherche des personnes actives ou pouvant avoir connaissance des faits ou avoir commis une négligence. On peut d'interroger sur la complicité des titulaires ou hôtes des nœuds qui aident autrui à reproduire de manière transitoire et partielle un fichier illicite. Il semble impossible d'assigner une intention ou une connaissance de la nature des fichiers qui n'est pas accessible techniquement ni pour les pairs ni pour les développeurs du service.

Le droit de la responsabilité des intermédiaires techniques et des fournisseurs d'accès

La responsabilité peut prendre différentes significations : la sécurité des données, la qualité du service, la cybercriminalité, l'atteinte aux données personnelles, la contrefaçon et la circulation de fichiers contenant des données confidentielles ou sans autorisation des titulaires de droit d'auteur. Au regard des caractéristiques techniques des AD, les personnes derrières les nœuds du réseau qui aurait fait circuler un contenu illicite ne voient pas et ne peuvent pas contrôler ou supprimer ce qu'elles font circuler dans la mesure où les données sont fragmentées et encryptées.

Le régime juridique de responsabilité limitée des intermédiaires[1] (ou safe harbour) viendra donc à s'appliquer partiellement : les intermédiaires n'ont pas connaissance des activités illicites, ce qui les qualifient pour l'exonération de responsabilité. Cependant, même s'ils en sont notifiés, ils ne pourraient pas retirer promptement le contenu en cause, ce qui est la deuxième condition d'exonération de responsabilité, dans la mesure où ils n'ont pas le contrôle technique du ou des noeuds en cause. Responsabiliser les noeuds d'un service de stockage ou d'accès nécessiterait de les identifier, et conduirait à condamner des personnes alors que ce sont peut-être d'autres qui ont faciliter le relais de l'information illégale, action demandée par un tiers. De plus, s'il n'existe pas d'index répertoriant l'information disponible, il n'y a pas de page à bloquer ou de lien à retirer.

Le seul moyen de contrôler les AD serait de mettre en place des lois pour les interdire, pour empêcher leur développement en condamnant leurs développeurs ou leurs opérateurs, ou en allouant des devoirs ou responsabilités de manière arbitraire. Cela a été le cas en Italie[2] (lien entrée mesh), entre 2005 et 2011 qui contraignait les fournisseurs d'accès à conserver la carte d'identité et les traces de connexions des utilisateurs. De même, les lois de riposte graduée pour mettre un terme aux échanges pair-à-pair[3] visent notamment à responsabiliser les intermédiaires publics, privés ou associatifs qui mettent à disposition une connexion wifi gratuitement. Ces procédures requièrent soit l'identification de l'utilisateur contrevenant, or l'adresse IP n'est pas une preuve valable car elle peut changer dynamiquement ou être modifiée (lien avec entrée preuve), soit une obligation de sécurisation, qui est incompatible avec l'architecture des réseaux distribués. Cette disposition de la loi Hadopi introduite en 2009 pour responsabiliser leurs utilisateurs pour ne pas sécuriser leur connexion et permettre à d'autres d'effectuer des actes illicites a été révoquée en 2013 après qu'une seule connexion ait été suspendue. Les nœuds bénéficieront d'une immunité en tant que simples routeurs (Hatcher, 2007) et la responsabilité des intermédiaires risque de porter atteinte à la liberté d'expression (La Rue, 2012).

La distribution de la responsabilité socio-économique de fournir un service et de l'entretenir

On remarque au sein des communautés distribuées (lien entrée Communautés distribuées) une nécessaire « responsabilisation » des usagers de ces services qui par leur présence et leur participation assurent le bon fonctionnement technique des échanges ou du stockage d'information. Mais la collaboration et la responsabilité sociale n'équivalent pas à la responsabilité civile ou pénale.
Il existe des cas de distribution de la responsabilité de vérifier qu'aucun contenu illicite ne circule sur certains services qui prévoient une fonctionnalité de rapport ou de dénonciation par les utilisateurs des contenus contrevenant. Le crowdsourcing ou la production participative de surveillance ne peut s'opérer que sur des services et au sein de communautés qui présentent un certain degré de centralisation technique. Ainsi, Diaspora, le réseau social distribué, peut contacter

1 Digital Millennium Copyright Act (DMCA) aux Etats-Unis, 1996, Directive européenne sur le commerce électronique, 2000, loi française pour la confiance dans l'économie numérique (LCEN), 2009.
2 Décret anti-terrorisme n.144 du 27 juillet 2005 aboli en 2011
3 Loi favorisant la diffusion et la protection de la création sur internet, dite loi Hadopi ou loi création et internet, 2009.

les administrateurs des nœuds qui hébergent de la propagande pour ISIS[4] et les éditeurs de Wikipédia peuvent patrouiller et retirer les images sous droit d'auteur, protégeant ainsi la fondation de tout recours juridique. La mise en place d'une police communautaire, dans une certaine mesure la coordination d'une action distribuée, peut conduire à préserver des biens communs sur la base des principes 4 et 5 d'autorégulation pour le maintien de ressources communes développés par Elinor Ostrom (1990, 2010) : les mécanismes de contrôle et les sanctions graduées pour ceux qui violeraient les règles de la communautés. La privatisation de la police peut aussi mener à la discrimination et l'exclusion de certains utilisateurs sur la base de leur adresse IP[5]. Mais de manière plus pragmatique, si l'encryption est infaillible, les infractions ne pourront pas être détectées et il est peu probable qu'un sentiment de responsabilité communautaire se développe dans le cadre de services anonymes.

Les règles juridiques applicables aux architectures distribuées ont été développées pour des personnes individualisées, pas pour des réseaux évolutifs et distribués. La distribution de la responsabilité au sein d'un système complexe nécessiterait de fragmenter la faute entre les membres du réseau, ce qui implique une relation de confiance entre les membres, ou alors le partage du risque collectif par la mise en place de mécanismes d'assurance collective ou de mutualisation.

Références

Dulong de Rosnay, M. (2014). Peer-To-Peer Law. Distribution as a Design Principle for Law. *Media@LSE Electronic Working Paper Series* WP#31.

Hatcher, J. (2007). Mesh Networking: A look at the legal future. *Journal of Internet Law*, 11(1), 1-16. Preprint available at SSRN: http://ssrn.com/abstract=814984

La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Office of the United Nations High commissioner for Human Rights, 22 p. http://www.article19.org/data/files/pdfs/reports/report-of-the-special-rapporteur-on-the-promotion-and-protection-of-the-righ.pdf

Ostrom, E. (2010). *La gouvernance des biens communs : Pour une nouvelle approche des ressources naturelles* [traduction de « Governing the Commons: The Evolution of Institutions for Collective Action », 1990], De Boeck**,** 2010, 304 p.

4 http://www.theguardian.com/technology/2014/aug/21/islamic-state-isis-social-media-diaspora-twitter-clampdown

5 http://www.ethanzuckerman.com/blog/2013/02/12/who-let-all-those-ghanaians-on-the-internet-jenna-burrell-on-internet-exclusion/