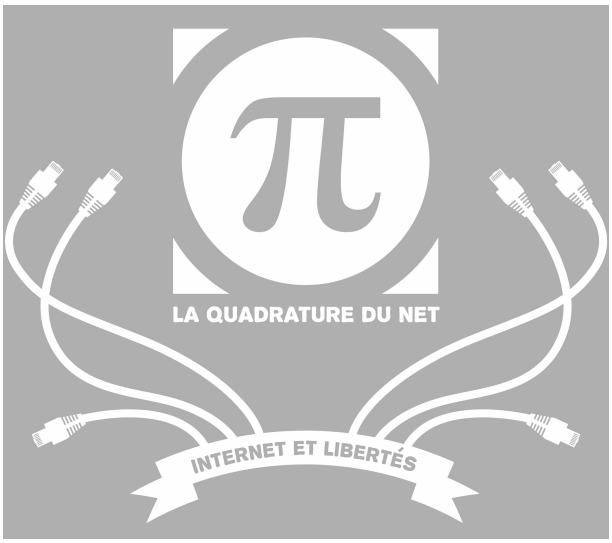

PROPOSITIONS

de La Quadrature du Net
pour adapter les politiques publiques
aux réalités sociales
et technologiques
d'Internet

Édition 2016

LA QUADRATURE DU NET
www.laquadrature.net

LES PROPOSITIONS DE LA QUADRATURE DU NET

Suivant trois axes, nos propositions visent à faire de ce réseau partagé un outil au service de la démocratie et du développement socio-économique de notre société.

Elles ne pourront être débattues et surtout mises en œuvre que si nous savons au préalable assurer le caractère démocratique de nos institutions. Cela suppose notamment que le débat public se fonde sur des informations transparentes.

Les propositions de La Quadrature du Net s'organisent selon les axes principaux du travail mené autour des législations françaises et européennes, mais cherchent surtout à porter une vision d'ensemble équilibrée de la vision d'Internet que nous promouvons :

ACCÈS À UN INTERNET LIBRE ET OUVERT

Internet et ses bénéfices socio-économiques sont fondés sur des principes techniques simples qu'il importe de protéger. Le plus important d'entre eux est sans doute le caractère décentralisé du réseau, qui maximise la liberté de communication, et donc la libre expression et l'innovation en ligne. De manière générale, il s'agit de mettre chaque personne en capacité de créer, d'échanger avec ses pairs, d'accéder à une plus grande diversité de biens informationnels.

GOUVERNANCE D'INTERNET

Depuis environ 15 ans, les rencontres pour la « Gouvernance de l'internet » ont attiré l'attention, et conduit notre imaginaire à croire que des règles consensuelles pour Internet peuvent émerger de discussions « multi-acteurs » (multi-stakeholder) dans des processus « descendants » (top-down). Cependant, les derniers sommets (NETmundial, IGF Istanbul, etc.) montrent que rien n'est sorti de ces 15 années de réunions multipartites, alors que dans le même temps, de nombreuses décisions politiques, économiques ou technologiques ont été prises dans le but de mettre à mal les droits fondamentaux dans l'espace numérique. De multiples révélations montrent notamment que la technologie est trop souvent retournée contre ses utilisateurs, transformée en un outil de surveillance, de contrôle et d'oppression.

Les problèmes posés par la surveillance de masse, la protection des libertés numériques, la neutralité du Net ou l'accès universel à un Internet libre ne peuvent être réglés dans des discussions multipartites stériles où la liste des participants et des sujets est définie en amont par des organisateurs dévoués aux États ou aux entreprises des télécoms ou des services en ligne. Ces acteurs, États, entreprises ou services de renseignement, n'ont pas attendu les rencontres sur la gouvernance pour modifier la structure et le fonctionnement d'Internet vers plus de surveillance et de distorsion de l'accès libre et universel au réseau.

Cette « gouvernance mondiale multi-acteurs » cache la réalité d'une perte de contrôle du politique, sous l'influence et au bénéfice de grands groupes industriels. Dans une approche bottom-up (venant de « la base »), en sens inverse, les citoyens et les parlements nationaux feraient pression sur les États et les acteurs industriels pour forcer des décisions protégeant les libertés, afin de tenter de les propager de proche en proche dans les espaces politiques voisins. La seule chose que nous pouvons attendre des États, c'est qu'ils considèrent et sécurisent l'Internet comme un bien commun appartenant collectivement à tous ses usagers. Au même titre que l'eau, l'air, les réserves naturelles ou même la santé, les États doivent sans délai protéger Internet sans compromis, en sécurisant ses fondements : neutralité, non-surveillance, décentralisation.

À partir de là, les citoyens pourront ensuite s'engager collectivement dans un débat approfondi sur la nature de la confiance qui peut être placée dans les acteurs publics ou privés qui vont gérer cette ressource commune. Quelles conditions de transparence et de responsabilité demander – comme l'utilisation de logiciels libres et la capacité pour le public de

le vérifier – dans une société démocratique, à ceux qui sont responsables de la protection de nos libertés fondamentales, du fait de leur contrôle sur une partie de notre infrastructure commune ?

Sans garanties internationales fortes sur la protection d'Internet comme bien commun, et l'implication réelle des citoyens, toutes les actions de « gouvernance » ne sont vouées qu'à être perverties par les intérêts des États et des entreprises privées.

PROTÉGER LA NEUTRALITÉ DU NET

Internet et ses bénéfices socio-économiques sont fondés sur des principes techniques simples qu'il importe de protéger. Le plus important d'entre eux est sans doute le caractère décentralisé du réseau, qui maximise la liberté de communication, et donc la libre expression et l'innovation en ligne.

Deux cas doivent dès lors être distingués pour protéger le principe de neutralité :

• d'une part l'Internet dit best-effort, fondé sur un traitement absolument neutre des flux, contenus, services et applications,

• d'autre part les services spécialisés, c'est-à-dire des offres d'accès reposant sur une qualité de service optimisée pour une application donnée (la VOIP, la vidéo, les jeux en ligne par exemple).

POURQUOI EST-CE IMPORTANT ?

Le développement d'Internet et du web a conduit, en France et dans le monde, à faciliter la participation démocratique du plus grand nombre, en permettant à tous d'avoir un accès égal aux réseaux de communication. Ces avancées sont incompatibles avec un Internet « à deux vitesses », réservant aux plus offrants certains privilèges dans l'acheminement du trafic Internet. En parallèle de la lutte contre la fracture numérique, la protection de la neutralité du Net est la clé de la promotion d'un accès universel à Internet.

La neutralité du Net est considérée comme un vecteur d'innovation car elle permet à de nouveaux entrants d'innover et de faire concurrence aux acteurs les mieux établis. Cet écosystème ouvert d'innovation est une véritable source de PIB et d'emplois : en 2011, on estimait que 25% des emplois nets créés en France étaient dus à Internet, directement ou indirectement.

Si, demain, les opérateurs pouvaient donner une priorité aux flux des entreprises les plus offrantes, ce moteur de l'économie numérique serait mis en pièce. Les PME innovantes ont besoin de voir garanti un accès neutre et inconditionnel, non seulement à l'Internet « best-effort » mais également aux offres d'accès fondées sur une qualité de service optimisée. C'est là la condition de leur développement, de

leur croissance et donc de l'innovation et la liberté de choix des consommateurs dans l'économie numérique.

La neutralité permet alors d'éviter les risques anticoncurrentiels liés aux rapprochements entre les grands acteurs américains de l'économie numérique et certains opérateurs télécoms, ou face aux stratégies d'intégration verticale des opérateurs qui investissent dans le marché des contenus et des services en ligne. En outre, dans un contexte de concentration croissante du secteur télécoms, par ailleurs largement défendue et encouragée par le gouvernement français, la neutralité des réseaux est une garantie essentielle face au risque d'abus de position dominante.

COMMENT PROTÉGER DANS LA LOI LA NEUTRALITÉ DU NET ?

• Il faut inscrire dans la loi une définition d'Internet assise sur le principe de neutralité (sur le modèle du best-effort, les paquets de données étant gérés indistinctement), afin de garantir la pérennité de son architecture technique.

• Le principe de neutralité doit s'appliquer à tous les mode d'accès à Internet (fixe ou mobile). Les exceptions à ce principe, en cas de congestion non prévue ou de menace sur la sécurité du réseau, doivent être rigoureusement encadrées au niveau réglementaire.

• Si les opérateurs télécoms sont autorisés à proposer à leurs abonnés des « services spécialisés » — c'est-à-dire des modes d'accès offrant une qualité de service optimisée (non best-effort) pour telle ou telle application (comme la VoIP, les flux vidéos, ou les jeux en ligne) —, alors les abonnés ayant souscrit à ces offres doivent cependant rester libres d'utiliser ces modes d'accès à qualité de service optimisée pour accéder à et utiliser n'importe quel service disponible sur Internet fonctionnellement équivalent à l'application en question.

• Sur les réseaux, les conditions d'équilibre entre les « services spécialisés » et Internet best-effort sur les réseaux de communication doivent être pérennes, afin de préserver l'accès universel à Internet.

• Les atteintes à ces principes par les opérateurs doivent faire l'objet de sanctions dissuasives, et n'importe quel citoyen s'estimant lésé par les pratiques d'un opérateur doit pouvoir en référer au régulateur.

• Il est nécessaire d'encadrer l'utilisation des technologies d'inspection des paquets de données afin de protéger le secret des correspondances et l'intégrité des communications électroniques.

Pour aller plus loin :
– voir le rapport parlementaire sur la neutralité du Net d'avril 2011,
– notre réponse à la consultation européenne sur le sujet,
– notre rapport,
– à lire également, notre tribune parue dans les cahiers de l'Arcep.

LA LOYAUTÉ DES PLATEFORMES

Le concept de « Neutralité des plateformes », ou « Loyauté des plateformes » a émergé du côté des éditeurs et hébergeurs qui souffrent des positions dominantes des gros acteurs du web, principalement anglo-saxons, ou les contestent. Ces notions de loyauté et de neutralité des plateformes ont pu être utilisées pour distraire les parlementaires du débat sur la neutralité du Net.

La question de la loyauté des plateformes doit être envisagée dans un univers où, de plus en plus, sont liées les questions de maîtrise par l'utilisateur de ses terminaux numériques (ordinateur, tablette, téléphone portable, autres objets connectés comme ceux du quantified self, etc.), de situations de monopoles de fait par certaines entreprises, de problématiques de fiscalité et de partage des revenus.

La neutralité (ou la loyauté) des intermédiaires techniques n'est pas liée à la notion de plateforme, elle-même très mal définie et recouvrant des modèles de réalisation et non un usage ou un rôle définis dans l'univers numérique. Le rôle tenu par une « plateforme » donnée (par exemple Facebook) peut être réalisé par d'autres méthodes (par exemple Diaspora*), où l'on ne parle alors plus de « plateforme ».

Il s'agit donc de ne pas débattre de la loyauté des « plateformes » en général, mais de leurs obligations, attachées à des rôles fonctionnels et indépendamment de leur mode d'organisation (centralisé ou acentré).

RECONNAÎTRE LE RÔLE DE L'AFFICHEUR

Un des rôles fonctionnels est celui d'afficheur. Il se pose entre l'éditeur qui publie et sélectionne des données et l'hébergeur qui stocke de manière brute, sans intervention sur le contenu.

La notion de plateforme telle que le Conseil national du numérique l'envisage, englobe toujours un hébergeur et un afficheur.
Par exemple, Google stocke des liens et choisit l'ordre dans lequel il affiche ceux qui sont trouvés.

DÉFINIR LA NOTION DE PLATEFORME

En conservant l'idée de l'afficheur, la notion de plateforme peut se référer à « l'environnement d'exécution d'une application, d'un afficheur, d'un outil ».

Ainsi la notion de plateforme recouvre les équipements (système d'exploitation et MarketPlace) ou certains sites web (Facebook agrège des applications externes, Google Apps agrège des applications internes et externes, etc.). Le fait que l'exécution des applications se fasse dans un site web (Facebook), sur un système d'exploitation (iPhone) ou sur un serveur personnel du client (CozyCloud), relève des détails d'implémentation.

DÉFINIR LA LOYAUTÉ DE L'AFFICHEUR OU DE LA PLATEFORME

Une obligation de loyauté attachée à ce rôle d'afficheur devrait reprendre quelques points clefs :

• la transparence vis-à-vis de l'utilisateur sur ce que fait la plateforme (critères de choix, critères sur l'ordre, etc.) ;
• permettre à l'utilisateur un contrôle de ce que fait l'afficheur (modifier les choix) ;
• garantir que l'utilisateur peut utiliser un autre afficheur (dans le cas des plateformes, cela entraîne une obligation de portabilité des données, pour changer de plateforme, l'afficheur étant intégré).

Dans le cas d'une obligation de loyauté attachée à la plateforme, les points à garantir seraient les suivants :
• l'utilisateur choisit les applications qu'il utilise, on ne peut pas lui en imposer ;
• l'utilisateur peut décider d'installer une application qui ne soit pas certifiée par la plateforme (à ses risques et périls) ;
• l'utilisateur peut choisir une autre source d'applications certifiées que celle fournie par la plateforme ;
• l'utilisateur peut produire sa propre application, s'en servir et la diffuser, soit via les applications certifiées par la plateforme, soit via une autre source d'applications certifiées, soit par ses propres moyens (en devenant une source d'applications) ;
• les systèmes informatiques doivent avoir la capacité de fonctionner avec d'autres systèmes ou plateformes, autrement dit d'être interopérables.
l'intéropérabilité des systèmes consiste ainsi à garantir l'échange d'information sans tenir compte du logiciel utilisé, et éviter des restriction d'accès à celle-ci.

Les autres critères s'apparentent plus à des obligations liées au droit de la concurrence (le fait par exemple de ne pas favoriser ses propres services) et dépendent beaucoup du degré de monopole de la plateforme sur son marché et de ses pratiques éventuellement anticoncurrentielles (à l'image de Google, par exemple).

ENCOURAGER LE DÉVELOPPEMENT DES RÉSEAUX SANS FILS PARTAGÉS

Le spectre hertzien doit redevenir une ressource publique, grâce à l'ouverture de nouvelles bandes de fréquences à des accès partagés et sans licence, sur le modèle du WiFi.
Il faut expérimenter au plus vite l'utilisation de nouvelles technologies radio permettant la mise en place de réseaux sans fil partagés (technologies radio « intelligentes » et femtocells).
Les personnes partageant des accès Internet sans fil doivent pouvoir le faire sans risque juridique.

Pour de plus amples informations, lire la tribune « Le spectre de nos libertés » et la présentation de l'Open Wireless Movement.

SOUTENIR LE DÉVELOPPEMENT DE TERMINAUX ET DE SERVEURS CONTRÔLÉS PAR LES USAGERS

Afin d'éviter toute distorsion de concurrence, il incombe aux régulateurs de garantir l'interopérabilité des terminaux avec différents systèmes d'exploitation.

Les pouvoirs publics doivent encourager l'utilisation de logiciels libres, notamment dans le cadre des marchés publics.

Les ressources essentielles du réseau, notamment les serveurs, doivent être rendues plus accessibles afin de garantir le caractère décentralisé de l'architecture d'Internet.

Au sujet de la promotion des logiciels libres, voir les recommandations de l'April. Sur la manière dont les utilisateurs d'Internet peuvent reprendre le contrôle des ressources essentielles du réseau, voir la présentation du projet « Freedom Box » par Eben Moglen.

LES DROITS DE L'HOMME DANS LA SOCIÉTÉ NUMÉRIQUE

La liberté de communication et d'expression est première dans l'ordre démocratique. Elle permet l'échange des idées, des opinions et des informations qui façonnent notre vision du monde , elle est le fondement des sociétés libres. En ce qu'Internet offre à chacun l'occasion d'émettre et de recevoir n'importe quel type d'information, il constitue une rupture technique et politique. Mais pour que le champ des possibles reste ouvert, la liberté de communication et les autres droits fondamentaux doivent être rigoureusement protégés sur Internet. La garantie de ces droits passe par l'application rigoureuse des principes de l'État de droit à l'espace public en ligne.

CENSURE ET LIBERTÉ D'EXPRESSION

La Loi pour la Confiance en l'Économie Numérique (LCEN) votée en 2004 et constamment modifiée depuis lors, fixe en France les dispositions concernant la censure et le retrait de contenus sur Internet.

La Quadrature du Net s'oppose régulièrement à l'extension des champs d'application de la LCEN ou à certaines dispositions qui y sont inscrites, et propose donc les modifications suivantes :

MORATOIRE SUR LES MESURES DE BLOCAGE

La censure administrative de site est une atteinte inacceptable non seulement à la liberté d'expression mais également au principe de séparation des pouvoirs, et La Quadrature du Net s'y oppose catégoriquement, notamment au travers d'un recours devant le Conseil d'État. Toutefois, même lorsqu'elles sont prononcées par les autorités judiciaires, les mesures de blocage apparaissent à la fois inefficaces et disproportionnées :

• Disproportion : en 2011, suite à un rapport d'information bipartisan sur la neutralité du Net, le groupe socialiste à l'Assemblée nationale proposait d'instaurer dans la loi un moratoire et une évaluation des mesures de blocage de sites Internet. Quelques semaines auparavant, un rapport de l'ONU soulignait également que les mesures de blocage étaient le plus souvent adoptées par les États en violation de leurs obligations au regard du droit international. Compte tenu des problèmes de surblocage et de l'efficacité douteuse de ces mesures, le blocage de site apparaît contraire au principe de proportionnalité et de nécessité, tant au regard du droit européen que de la constitution. Et ce d'autant plus que des mesures alternatives existent, telles que le retrait des contenus à la source, même si l'efficacité de ces dernières reste entravée par l'absence d'effort au niveau diplomatique pour faciliter la coopération policière et judiciaire en vue de faire respecter le droit international dans l'espace transfrontières qu'est Internet.

• Manque de base légale : outre le manque de proportionnalité, un autre problème attenant au développement du blocage légal et de son

utilisation par les tribunaux français tient au manque de base légale pour de telles mesures de censure. En effet, celles-ci sont prononcées sur le fondement de dispositions législatives particulièrement vagues, et en particulier le vocable selon lequel l'autorité judiciaire peur ordonner « toutes mesures propres » à prévenir ou à faire cesser un dommage (article 6-I-8 de la LCEN). Or, le droit européen impose que de telles mesures soient prévues par la loi française de « façon expresse, préalable, claire et précise » (expression de l'avocat général à la Cour de Justice de l'Union européenne dans l'affaire Scarlet Extended).

Dans cet esprit, dans une opinion concordante annexée à l'arrêt Yildrim c. Turquie du 18 décembre 2012, le juge de la CEDH Pinto De Albuquerque avait proposé une liste de critères devant figurer dans le droit national pour encadrer les mesures de blocage de site. Il indiquait notamment que la loi devrait préciser les catégories de personnes et d'institutions susceptibles de voir leurs publications bloquées, une définition des intérêts pouvant justifier de telles mesures, ainsi qu'un définition des catégories d'ordonnances de blocage et leurs modalités techniques. Il proposait également que la loi garantisse le principe du droit au procès équitable et donc la possibilité pour la personne ou institution lésée par le blocage d'être entendue avant l'édiction de l'ordonnance de blocage. Il précisait enfin que « ni les dispositions ou clauses générales de la responsabilité civile ou pénale ni la directive sur le commerce électronique ne constituent des bases valables pour ordonner un blocage sur l'Internet ».

Autant d'aspects sur lesquels le droit français comme le droit de l'Union européenne sont très lacunaires. Dans ces conditions, et à défaut d'un moratoire sur les mesures de blocage, le gouvernement et le parlement doivent s'engager à un encadrement précis des conditions et des modalités du blocage judiciaire de contenus sur Internet, en revenant sur la formule lapidaire consacrée en 2004 et étendue depuis à de nombreux autres textes de loi.

INTERDICTION DU NOTICE-AND-STAYDOWN

De nombreux responsables politiques et rapports officiels appellent au contournement de l'esprit du droit (article 15 de la directive eCommerce et article 6-I-7 de la LCEN) et de la jurisprudence de la Cour de cassation en affirmant leur volonté de consacrer le notice-and-staydown.

• Outre qu'elles semblent parfaitement contraires à l'intention des législateurs européens et français, La Quadrature du Net rappelle que ces mesures techniques visant à empêcher la réapparition de contenus sur Internet sont assimilables à une forme de censure préalable et automatique.

• Or, non seulement la base légale fait là encore défaut mais, plus fondamentalement, de telles mesures sont incapables d'apprécier concrètement si une utilisation donnée constitue ou non une infraction. Par exemple, dans le cas où il s'agit d'empêcher la remise en ligne d'un contenu au nom du droit d'auteur, ceux qui auront la charge de ces dispositifs risquent de les calibrer de manière à assurer un maximum de sécurité juridique sans considération pour les utilisations licites, telles que la parodie, l'information du public ou le droit de citation. Déléguer à des acteurs privés et aux outils

techniques qu'ils mettent en place la tâche de qualifier d'une situation juridique est une tendance délétère pour l'État de droit, tout particulièrement dans un contexte de montée de la « gouvernance algorithmique ».

• Le cas échéant, la loi devrait être clarifiée et renforcée pour mettre un terme aux atermoiements réglementaires et jurisprudentiels sur ce sujet.

MISE EN PLACE D'UN RÉGIME DE NOTICE-AND-NOTICE

Le régime de responsabilité dite « limitée » incombant aux intermédiaires techniques, et notamment aux hébergeurs, s'accompagne dans la LCEN de nombreuses obligations qui aboutissent de fait à privatiser la régulation de l'expression publique dans l'espace numérique.

• La notion de « manifestement illicite » dépassée : l'article 6-I-7 et le régime de notice-and-takedown institué par cette disposition, elle-même issue de la directive européenne eCommerce, a abouti à une situation contre laquelle le Conseil constitutionnel avait mis en garde. Le Conseil expliquait dans les commentaires sur sa décision relative à la LCEN que les hébergeurs ne devaient pas être contraints à se prononcer sur la licéité des contenus en ligne, du fait que « la caractérisation d'un message illicite peut se révéler délicate, même pour un juriste ». La réserve d'interprétation du Conseil sur la notion de « manifestement illicite » devait permettre d'éviter les dérives, en réservant la procédure extra-judiciaire de notice-and-takedown aux infractions les plus graves dès lors que les contenus signalés étaient « manifestement illicites ». Or cette notion a fait l'objet d'une extension jurisprudentielle à de nouvelles catégories de contenus (infraction au droit d'auteur ou diffamation, par exemple), la vidant de sa portée protectrice de la liberté de communication. En effet, cette extension renforce immanquablement l'insécurité juridique pesant sur les hébergeurs et leur propension à censurer des contenus en ligne, par crainte d'être ensuite condamnés par un juge qui estimerait que ces contenus étaient « manifestement illicites ». Les juges tendent même à condamner un hébergeur pour ne pas avoir retiré un contenu dont l'illicéité était seulement « vraisemblable » (cf. TGI Paris, 15 avril 2008, Jean-Yves Lafesse c/ Dailymotion), ou, ce qui revient au même, en distinguant la notion de « manifestement illicite » de la notion de « certainement illicite » (cf. TGI de Brest, 11 juin 2013, Josette B. c/ Catherine L. et Overblog).

• Restaurer la compétence de l'autorité judiciaire : la procédure de notice-and-takedown doit être réformée pour consacrer un régime dit de notice-and-notice :
– L'hébergeur ne doit être qu'un relais entre une personne qui se plaint d'un contenu qu'elle estime illicite et la personne qui l'a mis en ligne.
– Une fois le signalement reçu par l'hébergeur, ce dernier doit donner à son éditeur un délai raisonnable pour décider si oui ou non il accepte de le retirer. En cas de contre-notification de la part de l'utilisateur (s'il estime que le contenu litigieux est licite), le fournisseur doit notifier à la partie tierce qui a envoyé la demande de retrait que l'utilisateur s'y oppose, et proposer que l'affaire soit renvoyée devant un tribunal.
– Pour les signalements de contenus correspondant à des catégories d'infractions très graves (qui devront être précisées dans la loi) et pouvant justifier une mesure préventive (pédopornographie par exemple), l'hébergeur

devra adopter une mesure de suspension de l'accès au contenu dès qu'il prend connaissance du signalement, le temps que le litige soit tranché (soit à l'amiable, soit par le biais d'une procédure judiciaire).
– Enfin, il importe de réfléchir à la création d'une plateforme permettant de faire la transparence sur les mesures extra-judiciaires de retrait de contenu, particulièrement au cas où le droit en resterait à un régime de notice-and-staydown. À l'heure actuelle, en dehors des transparency reports publiés par certaines grandes plateformes, les citoyens, décideurs, chercheurs et journalistes ne disposent d'aucune information fiable et transparente sur l'étendue et la nature des retraits effectués suite à des signalements par des tiers ou par l'autorité administrative. La plateforme américaine « Lumen » peut constituer à cet égard un modèle dont il est possible de s'inspirer.

PROHIBER LA CENSURE PRIVÉE PAR LES INTERMÉDIAIRES TECHNIQUES

Dans son étude de septembre 2014 sur le numérique et les droits fondamentaux, le Conseil d'État a décidé de prendre la position selon laquelle « la possibilité pour une plateforme d'exclure certains contenus alors qu'ils sont autorisés par la loi n'est pas contestable : elle relève de sa liberté contractuelle et de sa liberté d'entreprendre ». Et pourtant, ces dernières années, les politiques mises en place par des plateformes comme Google ou Facebook en la matière ont montré les risques de telles politiques de censure de contenus licites par des acteurs qui, par ailleurs, revendiquent le statut d'hébergeur et donc d'intermédiaire technique neutre. La transparence et la possibilité d'un recours auprès de ces acteurs ne saurait suffire à eux seuls à fournir une protection satisfaisante.

• Reprenant une proposition portée dès 1999 par Laurent Chemla, le collectif NumNow a récemment proposé d'inscrire dans le code pénal des dispositions générales réprimant le fait de porter atteinte à la liberté d'expression, et qui permettraient notamment d'éviter que les conditions d'utilisation des intermédiaires techniques bénéficiant par ailleurs d'une exemption de responsabilité ne servent à mettre à mal la liberté d'expression de leurs utilisateurs.

• À partir de ces propositions, La Quadrature du Net appelle à prohiber la censure privée par des intermédiaires techniques, sous peine de sanctions dissuasives indexées sur leur chiffre d'affaire. Une telle disposition devrait être limitée aux intermédiaires techniques (n'exerçant aucun contrôle éditorial), fournissant un moyen d'expression publique, et pouvant être qualifiés d'« universels » au sens où il ne s'adressent pas à une communauté d'intérêt restreinte (une communauté d'intérêt étant définie au sens de la Cour de cassation comme « un groupe de personnes liées par une appartenance commune, des aspirations et des objectifs partagés »). Ainsi, un réseau social universel comme Facebook, rentrerait dans le champ d'une telle disposition, à l'inverse d'un réseau social destiné à une communauté d'intérêt définie dans ses statuts ou ses conditions générales d'utilisation (et qui serait, par exemple, réservé à une entreprise, à une communauté religieuse, ou qui se donnerait un thème de discussion défini).

COMPÉTENCE EXCLUSIVE DES SERVICES DE L'ÉTAT POUR RECUEILLIR LES SIGNALEMENTS DE CONTENUS ILLICITES

Face à l'extension des obligations de surveillance incombant aux hébergeurs à travers de nombreux textes de loi en vertu de l'article 6-I-7 de la LCEN, il importe de rationaliser le dispositif en conjurant le risque de la censure privée. Parallèlement à l'instauration d'un régime de notice-and-notice, La Quadrature du Net recommande de centraliser le recueil des signalements d'informations illicites dans les mains des services de l'État. Les hébergeurs devraient avoir pour seule obligation celle de mettre à disposition de leurs utilisateurs un dispositif (un outil logiciel conçu par les pouvoirs publics) transmettant directement les signalement des citoyens aux pouvoirs publics (notamment via la plateforme internet-signalement.gouv.fr de l'OCLCTIC, qui a été prévue à cet effet mais reste largement sous-utilisée et sous-dotée), le tout sans que les hébergeurs n'aient à en prendre connaissance (en dehors de l'obligation, dans le cadre de la procédure de notice-and-notice, de relayer les signalements auprès des auteurs ou éditeurs des contenus, le cas échéant en en suspendant temporairement l'accès si la gravité de l'infraction alléguée le justifie).

HABILITATION LÉGISLATIVE À AGIR EN JUSTICE POUR LES ASSOCIATIONS DE DÉFENSE DES DROITS SUR INTERNET

Comme l'a illustré dernièrement l'affaire The Pirate Bay en France, nombre de restrictions des libertés sur Internet sont prononcées sans que les personnes concernées n'aient eu la possibilité de se défendre en justice. Le droit, et notamment la LCEN, permet de solliciter directement les intermédiaires techniques, par exemple en assignant les fournisseurs d'accès à Internet en vue d'obtenir le blocage d'un site. Or, ces derniers se limitent la plupart du temps à opposer des arguments économiques et techniques, pointant le coût des mesures demandées et leur inefficacité. Dans une telle configuration, le jugement du litige fait généralement peu de cas des arguments ayant trait aux droits fondamentaux.

• De manière générale, comme souligné plus haut, il faut faire en sorte que les procédures aboutissant à des décisions restrictives de droits offrent la possibilité à la personne ou institution lésée d'être entendue, afin de garantir le droit au procès équitable.

• En outre, en particulier dans les cas où les personnes visées par une mesure restrictive de liberté ne peuvent être représentées à l'audience (par exemple parce qu'elles ont préféré rester anonymes), l'action en justice d'associations de défense des droits permettrait de défendre leurs droits fondamentaux. Toutefois, à l'heure actuelle, les associations compétentes, et notamment celles spécialisées dans la défense des droits sur Internet, ne disposent pas des moyens juridiques, matériels et humains pour intervenir dans les affaires représentant un intérêt stratégique au plan jurisprudentiel. En outre, en l'absence d'habilitation expresse, la reconnaissance de leur intérêt à agir par les juridictions n'est pas non plus acquise, en particulier devant les juridictions pénales.

Dans ce contexte, La Quadrature du Net recommande l'adoption en faveur des associations d'une habilitation législative à agir en justice au nom de la défense des droits fondamentaux sur Internet, dès lors que celle-ci entre dans l'objet social de l'association, et ce tant devant les juridictions civiles et pénales qu'administratives. Une telle habilitation devrait leur permettre de se voir octroyé des dommages et intérêts et de se constituer partie civile, notamment en vue de permettre par ce biais le financement de leurs actions en justice.

VOIR ÉGALEMENT :

• notre réponse à la consultation sur la directive européenne relative aux services de la société de l'information

• les conclusions du rapporteur de l'ONU pour la liberté d'expression

• notre mémoire transmis au Conseil constitutionnel sur la loi LOPPSI 2

SURVEILLANCE

La Quadrature du Net a développé, notamment depuis le vote de la Loi de Programmation militaire de 2013 et les révélations d'Edward Snowden sur la surveillance exercée par la NSA, des analyses et propositions concernant la surveillance exercée par les États sur les citoyens.

Le sujet de la surveillance recouvre plusieurs techniques :

LES INTERCEPTIONS DU CONTENU DES COMMUNICATIONS

Il faut tout d'abord distinguer les interceptions judiciaires des interceptions administratives.
Les premières étant encadrées par le Code pénal et mises en place sur demande d'une autorité judiciaire ; tandis que les secondes peuvent-être demandées par un agent administratif dans certains cas (par exemple, la prévention du terrorisme).

La loi Renseignement, qui ouvre un champ très large aux écoutes, dispositifs de sonorisation etc. porte par exemple sur les interceptions administratives, conduites en particulier par les services de renseignement.

La Quadrature du Net considère que les interceptions administratives des communications :

• devraient être autorisées par un juge judiciaire et contrôlé par lui pendant et après la réalisation des interceptions ou par un organe indépendant doté de véritable pouvoirs d'enquête ;

• devraient pouvoir faire l'objet d'un recours contentieux devant le Conseil d'État, dans le respect du droit à un procès équitable, notamment par la mise en place d'audiences publiques, ainsi que par la communication des documents au requérant. Dans le cadre des documents secret-défense, le Conseil d'État devrait être doté d'un pouvoir de déclassification de ces documents soumis par l'administration en cours de procédure, lorsqu'il estime que le secret n'est pas justifié ;

• devraient faire l'objet d'une information au public sur le nombre de situations d'illégalité et d'infractions mises à jour par la CNCTR et le Conseil d'État, et ainsi ne pas étendre de manière disproportionnée les informations couvertes par le secret de la défense nationale.

LA CONSERVATION ET L'ANALYSE DES DONNÉES DE CONNEXION

Aujourd'hui, les données de connexion révèlent énormément de choses sur notre vie privée et sont pour cette raison très sollicitées par les pouvoirs publics (administratif et judiciaire) dans le cadre d'activités de surveillance. Lors de l'audience de la Question prioritaire de constitutionnalité posée par La Quadrature du Net, FDN et la Fédération FDN sur la Loi de Programmation Militaire, le rapporteur public expliquait ainsi :

« Ce changement de nature se traduit à la fois par une augmentation exponentielle des données de connexion (...) que par une amélioration sans précédent de la qualité et de la précision des informations et une exploitation raisonnée [des données] accumulées sur une personne déterminée, ce qui explique l'intérêt des services de renseignement. »

La situation est telle que :

« la summa divisio entre accès de données et accès de contenus n'a probablement plus la même portée qu'il y a quelques années, et sans doute l'ingérence dans la vie privée que constitue l'accès aux données de connexion doit être réévalué ».

Le régime juridique de conservation et d'analyse des données de connexion doit donc s'adapter en prenant compte ce nouveau contexte.

Le régime juridique de conservation et d'analyse des données de connexion doit donc s'adapter en prenant compte ce nouveau contexte. L'arrêt de la CJUE Digital Rights rendu le 8 avril 2004 contre la conservation généralisée des données invite à revoir le droit national applicable (articles L. 34-1 et R. 10-13 du Code des postes et télécom) sur ce sujet. Le principe de la conservation généralisée des données est d'autant plus critiquable que les mesures de conservation ciblée pratiquées dans une trentaine de pays, qui permettent aux enquêteurs d'enjoindre les opérateurs et autres intermédiaires techniques de préserver certaines données ou de leur communiquer les données techniques en leur possession, s'avèrent efficaces et montrent donc l'existence de solutions alternatives respectueuses des libertés et donc plus proportionnées.

Il faut donc :

• abroger les dispositions de l'article L. 851-1 et suivants du CSI, instaurés par la loi Renseignement du 24 juillet 2015, manquant de définir la notion « d'informations et documents » ;

• prévoir les mêmes formes de contrôle (a priori, pendant, a posteriori) pour l'accès aux données de connexion que pour les interceptions de contenu ;

• faire la transparence sur le nombre de données recueillies chaque année auprès des opérateurs et pour quels motifs ;

• interdire des dispositifs d'analyse massive des données de connexion, à l'exemple des « boîtes noires » de l'article 851-3 de la loi sur le Renseignement du 24 juillet 2015.

LA SURVEILLANCE INTERNATIONALE ET LA COOPÉRATION INTERAGENCES

Les autorités de contrôle ont-elle connaissance des détails de la collaboration entre la NSA, la DGSI & d'autres services de renseignement ?

La surveillance internationale opérée par la coopération entre les agences permet de contourner le droit national, et peut servir à d'autres fins que celle de la prévention du terrorisme. Le rapport Campbell (page 22) cite ainsi des exemples d'utilisation d'informations tirées d'une interception, afin de constituer un avantage économique pour une entreprise.

De telles écoutes sont illégales et illégitimes et font porter des problèmes graves sur l'ensemble de la sûreté de nos sociétés, les services conservant ainsi pour eux des failles et défauts de protocoles que d'autres (mafias, criminels) pourraient exploiter aussi.

Il faut donc :

• protéger l'universalité en prévoyant des mêmes régimes de contrôle lorsque les communications sont internationales et/ou collectées/analysées depuis l'étranger. Le recueil des communications internationales doit intervenir suite à un contrôle préalable, et un contrôle a posteriori efficace, qui nécessitent que celles-ci ne soient pas soumises à un régime dérogatoire.

• prévoir un contrôle indépendant sur les accords de coopération avec d'autres agences de renseignement, afin de s'assurer qu'ils ne soient pas utilisés pour contourner le droit national, au détriment de la vie privée des citoyens.

LA DÉFENSE DE LA CORRESPONDANCE PRIVÉE ET L'AMÉLIORATION DES INFRASTRUCTURES CRITIQUES, PUBLIQUES ET PRIVÉES

Nous assistons depuis ces derniers mois à une nouvelle « crypto war » (ou guerre de la cryptographie), où l'inculture numérique conduit le pouvoir politique à une méfiance et à des volontés de répression disproportionnée à l'encontre outils de chiffrement. La technique du chiffrement nourrit ainsi les fantasmes et la suspicion de la classe politique et des juges, comme l'illustre la tribune signée par le Procureur de Paris sur le chiffrement des téléphones.

Or, le chiffrement des communications est à la fois l'expression d'un droit à l'anonymat et une nécessité pour se protéger, encouragé par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ainsi que par différentes instances européennes.

La Quadrature du Net appelle à :

• favoriser le chiffrement des communications en exigeant des opérateurs ou fournisseurs de services qu'ils soient au mieux de l'état de l'art (typiquement, orange ne fournit pas SSL/TLS pour ses mails...)

• garantir le droit au chiffrement et à l'anonymat en ligne.

LA REPRISE EN MAIN DU CONTRÔLE DE LA TECHNOLOGIE ET DE LEURS DONNÉES PAR LES CITOYENS

Les citoyens doivent pouvoir protéger leurs données et leur vie privée contre la surveillance généralisée et l'intelligence économique. À cette fin, ils doivent être informés des conséquences de la mise en danger de leur vie privée et avoir connaissance des solutions et des outils s'offrant à eux pour protéger leurs données. Il s'agit donc de confier un réel pouvoir de décision et de contrôle dans les mains du citoyen.

Il faut donc :

• favoriser le développement de logiciels libres de services décentralisés et de chiffrement bout à bout (autrement dit que les messages envoyés à un destinataire soient chiffrés localement avant même d'être envoyés sur le réseau), afin de permettre aux utilisateurs de reprendre en main le contrôle de leur infrastructure ;

• permettre le développement des outils de sécurisation par des mécanismes d'incitation fiscale, de commande publique mais également en soutenant des programmes de développement et d'utilisation dans l'enseignement supérieur et la recherche ;

• favoriser le développement de matériel de confiance, en design libre, notamment pour l'équipement en communications mobiles, sans-fil et le routage.

PROTECTION DES LANCEURS D'ALERTE ET DU SECRET DES SOURCES

À l'heure des révélations d'Edward Snowden sur les pratiques de surveillance de la NSA et de ses partenaires internationaux comme la DGSE française, le statut des lanceurs d'alerte est plus que jamais au centre d'une réflexion politique et juridique, notamment en ce qui concerne les questions de surveillance. Beaucoup reste à faire cependant pour assurer pleinement le droit à l'information du public, sans lequel il ne peut y avoir de vraie démocratie.

Le statut de lanceurs d'alerte doit pouvoir bénéficier à toute personne qui signalerait, dévoilerait, ou dénoncerait des faits, passés, actuels ou à venir, de nature à violer des droits ou entrant en conflit avec le bien commun ou l'intérêt général. Dans le champ de la surveillance, ce statut doit permettre de déroger au silence que l'État impose légalement à ses agents et prestaires, pour protéger des personnes qui, comme Edward Snowden et nombre d'autres sources anonymes, permettent la tenue d'un véritable débat public sur les dérives de la raison d'État et des politiques de sécurité.

Les députés ont inclus dans la loi Renseignement, adoptée en juillet 2015, plusieurs dispositions qui concernent directement les lanceurs d'alerte issus des services de renseignement (article 862-1 du Code de la sécurité intérieure et L. 881-1 du code de la sécurité intérieure, tel que modifié par l'article 13 de la loi). Mais en réalité, ces dispositions aboutissent à un véritable recul. Elles n'autorisent le signalement qu'auprès de l'autorité administrative en charge du contrôle des opérations de surveillance, la CNCTR, dans des conditions qui conduisent à une extraordinaire insécurité juridique qui ne vise qu'à dissuader les lanceurs d'alerte de témoigner. Pire, la CNCTR n'est pas tenue de saisir les juridictions lorsqu'elle reçoit des signalements relatifs à des infractions pénales, tandis que la loi aggrave la répression des divulgations publiques concernant les activités de surveillance.

Au regard de la jurisprudence de la CEDH (CEDH, 12 février 2008, Guja c. Moldavie) et des principes mondiaux sur la sécurité nationale et le droit à l'information (principes de Tschwane), La Quadrature du Net recommande :

• d'abroger les dispositions L. 862-1 et suivants du CSI et d'adopter des mesures protectrices de la procédure d'alerte, indiquant que l'agent peut dénoncer tout crime, délit ou violation des droits, que les informations révélées soient couvertes ou non par le secret de la défense nationale ;

• d'assurer la possibilité de dénoncer ou de révéler ces faits et ces informations par le biais d'une procédure interne ou d'une divulgation publique. Le droit de révéler à la presse ou de divulguer publiquement l'existence d'abus et a fortiori de crimes et délits commis dans le cadre des activités de surveillance doit être reconnu lorsqu'une telle divulgation est d'intérêt public et que l'alerte interne à l'administration est objectivement risquée ou inefficace ;

• dans le cas de la procédure interne, la CNCTR (en tant qu'autorité administrative indépendante en charge du contrôle des services de renseignement) peut recueillir les signalements mais devra systématiquement en aviser le Conseil d'État, lequel devra saisir le procureur de la République.

• d'étendre le bénéfice de la protection légale aux tiers (co-contractants, fournisseurs, clients, associations, journalistes). Les journalistes et les citoyens ne devraient pas être visés par une loi de protection de la sécurité nationale les empêchant de divulguer ou d'avoir accès à l'information si celle-ci représente un intérêt public. Dans cette idée, il est nécessaire d'élargir la protection des sources à tous ceux qui exercent une activité journalistique, qu'il s'agisse de grands groupes de presse et de médias officiels, mais aussi plus généralement de la diffusion de l'information, sous la forme, par exemple d'un site web lanceur d'alerte comme WikiLeaks. Les recommandations de Reporters Sans Frontières sur le secret des sources, datant de 2013, avaient déjà mis en relief l'importance de l'extension de cette protection : « les personnes devant bénéficier de la protection des sources ne sont pas seulement les journalistes et les collaborateurs de la rédaction mais toutes les personnes contribuant directement à la collecte, au traitement éditorial, à la rédaction, à la production ou à la diffusion de l'information et ce quel que soit le vecteur » ;

• d'améliorer le régime d'indemnisation et créer un fond de soutien aux lanceurs d'alerte, comme cela avait été proposé par le rapport du Service

central de prévention de la corruption, placé auprès de la garde des Sceaux.

DONNÉES PERSONNELLES

C'est par une directive de 1995 que l'Union européenne régit actuellement la vie privée des Européens sur Internet. Elle encadre la collecte, l'exploitation et la revente de leurs données personnelles.

Chaque État membre de l'Union européenne a transposé la directive de 1995 dans son droit national en votant de nouvelles lois. En France, cela s'est fait en 2004 par une réforme de notre loi Informatique et libertés, qui encadre depuis 1978 l'exploitation des données personnelles des citoyens français. La directive a instauré une autorité de contrôle dans chaque État, chargée d'en faire respecter les règles auprès des administrations et des entreprises. En France, c'est la CNIL (la Commission nationale de l'informatique et des libertés), qui existait déjà depuis 1978, qui se charge de ces missions. Si cette directive est une avancée certaine dans la protection des données personnelles, elle n'est pas exempte de défauts. Ainsi, l'ensemble de ses dispositions n'ont pas été transposées à l'identique d'un État membre à un autre, alors que d'autres règles n'ont pas été assez précisément définies. Il en résulte que la protection des données personnelles connaît aujourd'hui d'importantes failles.

Le nouveau Règlement en discussion depuis 2012 a pour mission de corriger un certain nombre de ces failles et d'adapter la protection des données personnelles à l'expansion de la collecte et du traitement des données à caractères personnel. La Quadrature du Net a élaboré des propositions pour garantir aux citoyens la maîtrise et la bonne utilisation de leurs données personnelles :

GARANTIR LE CONSENTEMENT ÉCLAIRÉ DE L'UTILISATEUR

• L'utilisateur doit consentir à l'utilisation de ses données lorsque celles-ci vont faire l'objet d'un traitement ;

• son consentement doit-être spécifique, informé et explicite, donné librement, d'une manière claire et affirmative, signifiant l'accord de voir ses données personnelles faire l'objet d'un traitement ;

• le consentement de l'utilisateur ne doit pas être détourné pour accomplir des finalités autres que celles pour lequel celui-ci avait été initialement donné.

INTERDICTION DU PROFILAGE

Le « profilage » est une méthode informatisée de traitement de l'information qui a recours à des procédés de data mining sur des catalogues de données et qui permet de classer avec une certaine probabilité, et donc avec un certain taux d'erreurs induit, un individu dans une catégorie particulière, afin de prendre des décisions individuelles à son égard.

Le catalogue de données comprend tous les messages transmis sur le Net ainsi que les sites et vidéos consultés par tous les internautes sont analysés par les géants de l'Internet et par des sociétés dont le métier est de vendre de la

publicité ciblée sur des profils.
L'utilisateur doit voir inscrit dans le Règlement le droit de refuser de faire l'objet du profilage et ce droit doit être concrètement applicable au quotidien.

GARANTIR LE DROIT À LA PORTABILITÉ DES DONNÉES

Lorsqu'un utilisateur souhaite transférer ses données d'un service à un autre, quitter un service ou développer un autre service, il n'a actuellement pas toujours la possibilité de récupérer ses données pour les transférer.

Le droit à la portabilité des données doit être inscrit dans la loi et cette portabilité doit être effective, c'est-à-dire que les formats d'export de ces données doivent être ouverts, les services interopérables et la portabilité ne doit pas faire l'objet d'un paiement quelconque.

CLARIFICATION DU CONCEPT D'INTÉRÊT LÉGITIME

La rédaction actuelle du Règlement européen sur la protection des données donne aux entreprises qui effectuent une collecte et un traitement de données à caractère personnel le droit d'aller au-delà de l'objet initial de la collecte tel que l'utilisateur l'a accepté, lorsque ces entreprises ont un « intérêt légitime » à le faire.

La notion d'« intérêt légitime » ne possède pas de définition légale. Ce concept pose un problème puisqu'il permet aux entreprises et autorités publiques de procéder à un traitement des données personnelles sans le consentement de l'utilisateur, sans que le traitement soit absolument nécessaire, et sans obligations légales, si elles estiment qu'elles ont un intérêt légitime plus important que celui des personnes concernées. Il s'agit donc d'un réel contournement de la règle du consentement préalable.

L'intérêt légitime peut-être largement interprété. Ainsi, le simple fait pour un utilisateur d'être client d'une entreprise suffit à conférer à celle-ci un intérêt légitime pour procéder au traitement de données.

La Quadrature du Net propose donc de :

- définir et circonscrire la notion d'intérêt légitime ;

- ne permettre l'utilisation de l'intérêt légitime qu'en cas de dernier recours, quand aucune base légale n'existe, que son recours soit justifié et fasse l'objet d'une communication de l'entreprise ou de l'entité publique.

LIMITER LA « PSEUDONYMISATION » DES DONNÉES ET PROMOUVOIR L'ANONYMISATION

Les données « anonymisées » sont des données à partir desquelles il n'est pas possible d'isoler et d'identifier un individu. Son anonymat est ainsi pleinement respecté. Les données « pseudonymisées » restent en revanche relatives à un individu identifiable, en raison du lien existant entre le pseudonyme et les données d'identification (nom, prénom, adresse...) disponibles pour l'organisation collectant l'information. Il est donc extrêmement aisé d'identifier un individu avec relativement peu de données pseudonymisées.

Par conséquent, la pseudonymisation n'est pas une solution suffisamment protectrice pour les utilisateurs qui peuvent être identifiés trop facilement. Elle est malheureusement trop souvent présentée par les entreprises comme suffisamment protectrice et risque d'être autorisée par le Règlement, au détriment des citoyens.

La Quadrature du Net recommande donc de :

• favoriser l'utilisation de données anonymisées pour une meilleure préservation de l'identité des utilisateurs, et informer ce dernier sur les « risques » d'identification avec les données pseudonymisées ;

• exiger le consentement des utilisateurs pour l'utilisation de tous types de données personnelles, qu'elles soient anonymisées ou seulement pseudonymisées.

METTRE FIN À L'ACCORD DU SAFE HARBOR

Le Safe Harbor est un accord permettant aux entreprises américaines opérant en Europe de transférer les données des citoyens européens vers les États-Unis et de les exploiter commercialement. En contrepartie, l'entreprise est tenue de respecter les lois européennes, plus protectrices que les lois américaines dans le domaine de la protection des données. Par exemple, le transfert de données n'est possible que si l'individu a la liberté de s'y opposer.

Cet accord comporte cependant de nombreuses failles, dangereuses pour la protection des données des utilisateurs. Le Parlement européen a ainsi appelé à le renégocier en 2014.

Le Safe Harbor prévoit uniquement un mécanisme d'auto-certification, et non une véritable autorité de contrôle pour vérifier respect de cet accord. De même, le recours est très limité pour les citoyens européens, car il est plus difficile pour eux de saisir une autorité judiciaire ou administrative américaine que pour les résidents américains.

Un problème plus grave encore concerne les politiques de confidentialité des entreprises du Safe Harbor, et l'accès aux données par des tiers. Les révélations d'Edward Snowden ont ainsi mis en lumière la possibilité pour les autorités publiques américaines de recueillir et de traiter les données transférées dans le cadre du Safe Harbor.

La Quadrature du Net propose de :

• instaurer une véritable autorité indépendante de contrôle pour vérifier le respect des accords internationaux ;

• faciliter la procédure de recours pour les ressortissants européens concernant des entreprises étrangères ;

• encadrer l'accès et le traitement des données en le limitant aux seules entreprises ayant pris part dans l'accord.

DROIT AU DÉRÉFÉRENCEMENT

Les recommandations sur le droit au déréférencement, appelé (abusivement) « droit à l'oubli » dans les médias, ont été élaborées à l'été 2014 conjointement entre La Quadrature du Net et Reporters sans Frontières suite à l'arrêt du 13 mai 2014 de la Cour de justice de l'Union européenne contre Google Spain.

INTRODUCTION

La décision Google Spain de la CJUE, rendue le 13 mai 2014, a mis au grand jour la problématique du droit au déréférencement, et plus largement du droit à l'oubli, pour la protection de la liberté d'expression et du droit à l'information. Par sa décision, la CJUE impose aux moteurs de recherche, tels que Google, de prendre en charge les demandes de déréférencement formulées par les internautes, déléguant de fait à un acteur privé une tâche revenant normalement à l'autorité judiciaire, seule compétente pour garantir les libertés individuelles. Cette délégation est d'autant plus dangereuse que l'arrêt se fonde sur des principes vagues et généraux qui n'apportent aucune garantie pour la liberté d'expression.

Suite à cette décision, Google a mis en place un comité consultatif qui travaille actuellement à déterminer des règles plus précises permettant aux moteurs de recherche de répondre aux demandes de déréférencement qui leur sont adressées. Si les questionnements de Google sur la manière de trouver un juste équilibre entre le droit au déréférencement d'une personne et la liberté d'expression et d'information du public sont parfaitement légitimes, le fait que ce soit une entreprise privée qui s'en saisisse accentue la privatisation rampante l'application de la régulation d'Internet et est de ce point de vue inacceptable.

Dans le même temps, les autorités nationales de protection des données (telles la CNIL en France) se sont elles aussi attelées à l'édiction de règles précises pour faire suite à l'arrêt de la CJUE. Mais, ce faisant, elles outrepassent leurs prérogatives. En l'absence d'une législation suffisamment claire en la matière, ces autorités administratives sont à la fois illégitimes et incompétentes pour adopter et appliquer des règles visant à garantir un équilibre entre la protection de la vie privée et la liberté d'expression.

La vie privée et la liberté d'expression sont des droits fondamentaux de valeur équivalente (Articles 8 et 10 de la Convention européenne des droits de l'Homme, articles 8 et 11 de la Charte des droits fondamentaux de l'Union européenne). Lorsqu'ils entrent en conflit, ils doivent être mis en équilibre dans chaque cas d'espèce, sous l'autorité du juge, l'un ne pouvant prévaloir sur l'autre par principe. La décision de la CJUE met à mal ce principe : outre qu'elle aboutit à contourner l'autorité judiciaire, le droit au déréférencement y est considéré comme quasiment automatique.

La réponse doit donc venir des législateurs européens et nationaux. C'est à eux qu'incombe la responsabilité de mettre en place un cadre juridique clair, prenant pleinement en compte la liberté d'expression, et dont la mise en œuvre devra relever de l'autorité judiciaire.

Dans cet esprit, Reporters sans frontières et La Quadrature du Net se sont associés pour travailler sur une série de points de vigilance et de recommandations destinés à assurer une conciliation raisonnable entre le droit à la vie privée et la liberté d'expression, sous l'égide du juge judiciaire et non d'acteurs privés ou administratifs. Ce sont ces réflexions qui sont aujourd'hui soumises au débat.

1. SUR L'APPLICATION ABUSIVE DU DROIT DES DONNÉES PERSONNELLES AUX CONTENUS ÉDITORIAUX

En définissant de manière large « les données à caractère personnel » (« toute information concernant une personne physique identifiée ou identifiable »), le régime de protection des données personnelles inscrit dans la directive du 24 octobre 1995 trouve à s'appliquer aux contenus éditoriaux et autres informations d'intérêt public, en dépit de l'exception journalistique énoncée à l'article 9 de la même directive et que l'on retrouve à l'article 67 de la loi Informatique et Libertés française.

De fait, outre le droit au déréférencement ouvert par la CJUE, le droit des données personnelles est déjà largement utilisé pour faire obstacle à la liberté d'expression, sous l'autorité de la CNIL. En témoignent les propos de Mme Isabelle Falque-Pierrotin, présidente de la CNIL : « les plaintes concernant le droit à l'oubli sont quasiment toutes honorées, et le contenu est retiré. Il s'agit de propos dans des blogs, d'une image qui ne plaît pas, d'une décision judiciaire qu'on veut supprimer. » (Le Monde, 19 mai 2014).

Le recours au droit des données personnelles pour obtenir le retrait d'une publication et restreindre la liberté d'expression (à travers le droit d'opposition et de rectification), le tout sous l'égide d'une autorité administrative, constitue un contournement extrêmement dangereux des garanties entourant traditionnellement la liberté d'expression, et notamment le principe d'une protection judiciaire institué en France par la loi du 29 juillet 1881 sur la liberté de la presse.

C'est ainsi que, dans une ordonnance du 12 octobre 2009, le vice président du Tribunal de grande instance de Paris a jugé que « le principe constitutionnellement et conventionnellement garanti de la liberté d'expression interdit de retenir une atteinte distincte liée à une éventuelle violation des règles instituées par la loi du 6 janvier 1978, laquelle n'est pas une des normes spécialement instituées pour limiter cette liberté dans le respect du second alinéa de l'article 10 de la convention européenne susvisée [la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales] ».

Dans le même sens, un arrêt de la Cour d'appel de Paris du 26 février 2014 précise que le déréférencement d'un article sur le fondement de la loi de 1978 porte atteinte à la liberté de la presse. Il est ainsi jugé « qu'imposer à un organe de presse, de supprimer de son site Internet dédié à l'archivage de ses articles, lequel ne peut s'assimiler à l'édition d'une base de données de décisions de justice, soit l'information elle-même, le retrait des noms et prénoms des personnes visées par la décision vidant l'article de tout intérêt, soit d'en restreindre l'accès en modifiant le

référencement habituel, excèdent, ainsi que l'a estimé le tribunal, les restrictions qui peuvent être apportées à la liberté de la presse ».

Au niveau européen, dans une décision du 16 juin 2013, la Cour européenne des droits de l'homme (CEDH), a rejeté la demande de deux avocats polonais de supprimer un article, reconnu diffamatoire par la justice polonaise, mais qui demeurait accessible sur le site internet du journal. Cherchant un équilibre entre le droit à la réputation et le droit à l'information, la CEDH déclarait que le retrait du contenu en question « constituerait une censure et équivaudrait à réécrire l'histoire ».

Ces décisions apportent des précisions bienvenues sur la portée qui doit être donnée à l'exception journalistique. En effet, les dispositions relatives à la protection des données personnelles ne sauraient limiter la liberté d'expression. Aussi doivent-elles demeurer inapplicables pour l'ensemble des contenus éditoriaux et toute information d'intérêt public.

Face aux velléités des États membres de l'Union européenne de faire suite à l'arrêt de la CJUE en renforçant considérablement la portée des droits à l'oubli et à l'effacement, il importe de limiter ces derniers pour protéger la liberté d'expression. Le règlement doit être amendé afin de renforcer l'exception journalistique en l'étendant à tous les contenus éditoriaux et autres informations d'intérêt public.

Une fois cette clarification législative actée, la conciliation du droit à la vie privée et de la liberté d'expression pourra se faire de manière équilibrée sous l'empire du droit national et international et la jurisprudence afférente (par exemple, en France, l'article 9 du code civil ou les articles 226-1 et 226-2 du code pénal), tout en respectant le cas échéant les garanties existantes en matière de liberté d'expression (notamment celles contenues dans la loi sur la presse de 1881).

RECOMMANDATIONS

• L'arbitrage entre droit à la vie privée et la liberté d'expression doit se fonder sur les dispositions de droit commun et, le cas échéant, dans le respect des garanties applicables au droit de la presse, et non sur le droit spécial des données personnelles.

• Dans le cadre des négociations en cours sur le règlement européen sur les données personnelles, élargir l'exception journalistique à l'ensemble des contenus éditoriaux et informations d'intérêt public et limiter le champ d'application du droit à l'oubli prévu à l'article 17 aux données personnelles mises en ligne par la personne elle-même.

• Dans l'attente de l'adoption du règlement européen, instaurer un moratoire sur les mesures fondées sur ce droit spécial qui restreignent la liberté d'expression et le droit à l'information. À défaut, adopter des mesures transitoires pleinement respectueuses de la liberté d'expression.

• Au niveau de l'Union Européenne, réfléchir à l'opportunité de compléter les règles en matière de protection de la vie privée en adoptant un cadre protecteur de la liberté d'expression, notamment pour concilier ces deux droits fondamentaux.

2. SUR LE RÔLE DES MOTEURS DE RECHERCHE DANS L'ACCÈS À L'INFORMATION

En retenant une conception large de la notion de « responsable du traitement de données personnelles », la Cour de justice de l'Union européennne a donné compétence à une entreprise privée pour traiter les demandes de déréférencement en soumettant les moteurs de recherche aux obligations auxquelles sont soumis les responsables de traitement de données personnelles.

Le raisonnement de la CJUE semble résulter d'une vision conservatrice et erronée de l'Internet et du rôle des moteurs de recherche dans la communication. En effet, à aucun moment la Cour ne précise le rôle des moteurs de recherche dans la collecte d'information et leur contribution à l'exercice de la liberté d'expression, la Cour se contentant de souligner les risques plus grands induits par Internet « en raison du rôle important que jouent Internet et les moteurs de recherche dans la société moderne, lesquels confèrent aux informations contenues dans une telle liste de résultats un caractère ubiquitaire ».

Or, si Internet et les moteurs de recherche peuvent effectivement accroître les risques pour la protection de la vie privée, ils jouent symétriquement un rôle positif du point de vue de la liberté d'expression. Ainsi, le 4 avril 2012, le Comité des ministres du Conseil de l'Europe adoptait une recommandation sur la protection des droits de l'homme dans le contexte des moteurs de recherche (Comité des ministres, 4 avril 2012, recommandation sur la protection des droits de l'homme dans le contexte des moteurs de recherche). Il y souligne que « les moteurs de recherche permettent au public du monde entier de rechercher, de recevoir et de communiquer des informations, des idées et d'autres contenus, en particulier, d'avoir accès au savoir, de prendre part à des débats et de participer aux processus démocratiques. »

Dans un récent rapport, le Conseil d'État juge encore que « le déréférencement affecte la liberté d'expression de l'éditeur du site en rendant l'information publiée moins accessible et en le ramenant ainsi à la situation antérieure à Internet » (Conseil d'Etat, Étude annuelle 2014, Le numérique et les droits fondamentaux, p. 188). En raison de leur rôle de facilitateur d'accès à des contenus éditoriaux ou des informations d'intérêt public présents dans l'espace public, il y a donc un risque important à considérer les moteurs de recherche comme des responsables de traitement de données personnelles. Cela encouragerait en effet l'extrajudiciarisation de mesures affectant directement la liberté d'expression et le droit à l'information permis par Internet et ne permettrait pas une prise en compte suffisante des différents intérêts et droits en présence.

En outre, comme l'a constaté l'avocat général Jääskinen dans ses conclusions dans l'affaire Google Spain, considérer l'activité des moteurs de recherche en tant que telle comme relevant du traitement de données à caractère personnel serait proprement « absurde ». En effet, selon lui, « si les fournisseurs de services de moteur de recherche sur Internet étaient considérés comme des responsables du traitement de données à caractère personnel sur des pages

web source de tiers et que figuraient sur ces pages des "catégories particulières de données", telles que visées à l'article 8 de la directive (c'est-à-dire des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que des données relatives à la santé et à la vie sexuelle), l'activité du fournisseur de services de moteur de recherche sur Internet deviendrait automatiquement illégale, dès lors que les conditions strictes prévues dans cet article pour le traitement de telles données ne seraient pas remplies. »

Notamment pour cette raison, y compris dans les cas de liens vers des contenus non-éditoriaux ou ne relevant pas de l'intérêt public, l'activité des moteurs de recherche ne doit pas relever du statut de responsable de traitement de données à caractère personnel. Dans de tels cas, c'est à la source qu'il faut agir, en exigeant du responsable du traitement de données personnelles de retirer ou de corriger les informations qu'il diffuse sur Internet et qui ont par la suite été indexées par le moteur de recherche. Il serait toutefois opportun de donner aux autorités de protection des données un pouvoir d'injonction sur les moteurs de recherche pour qu'ils mettent à jour leurs résultats de recherche : suite à l'exercice de leur droit d'opposition ou de rectification auprès du responsable de traitement, les utilisateurs pourraient saisir leur autorité nationale pour qu'elle ordonne aux moteurs de recherche la correction ou la suppression d'informations contenues dans les extraits de copies de pages web ou dans leur cache (à l'image des décisions de justice qui ordonnent le déréférencement de liens pointant vers des contenus illicites).

RECOMMANDATIONS

• Amender le règlement européen sur les données personnelles pour considérer que, en tant qu'ils sont essentiels à l'exercice du droit à l'information et dès lors qu'ils fournissent des liens vers des contenus éditoriaux et des informations d'intérêt public, les moteurs de recherche et autres intermédiaires « facilitateurs d'accès à l'information » fournissant des liens vers de tels contenus doivent être couverts par l'exception journalistique élargie et ne pas relever de la qualification de responsable de traitement de données à caractère personnel.

• En cas de fourniture de liens vers des traitements de données personnelles ne relevant pas de contenus éditoriaux ou d'informations d'intérêt public, donner aux autorités de protection des données la compétence d'enjoindre aux moteurs de recherche la mise à jour des informations présentées dans les résultats de recherche, sans pour autant les considérer comme des responsables de traitement.

3. SUR LES DROITS DE LA DÉFENSE ET LES PROCÉDURES ADÉQUATES

Dans un État de droit, il n'appartient ni à des acteurs privés, ni même aux CNIL européennes de déterminer l'équilibre entre la protection de la vie privée et la liberté d'expression.

S'agissant du retrait de contenus par des acteurs privés, le Conseil constitutionnel avait relevé en marge de sa décision de 2004 sur la Loi pour la confiance dans l'économie numérique que « la caractérisation d'un message illicite peut se

révéler délicate, même pour un juriste » (Les Cahiers du Conseil constitutionnel, Commentaire de la décision n° 2004-496 DC du 10 juin 2004, Cahiers du Conseil constitutionnel, n° 17, p. 4). Une observation qui, par analogie, vaut également pour les mesures de déréférencement mises en œuvre par les moteurs de recherche en ce que dans la mesure où ces dernières restreignent la liberté d'expression et le droit à l'information. Le droit au procès équitable pour les auteurs et éditeurs de contenus déréférencés ne peut être honoré si l'examen des demandes est confié à un acteur privé.

De même, les autorités de protection des données personnelles n'ont ni la compétence, ni la légitimité pour procéder à l'examen de ces demandes et déterminer les limites de la liberté d'expression. Comme l'a précisé le Conseil Constitutionnel dans sa décision du 10 juin 2009 relative à l'HADOPI, le législateur ne peut confier à une autorité administrative, fusse-t-elle indépendante, le pouvoir de restreindre l'exercice du droit de s'exprimer librement.
S'agissant de la mise en balance de droits fondamentaux, c'est donc au juge judiciaire, garant des libertés individuelles, que revient la tâche de trancher un litige, garantissant ainsi pleinement le droit au procès équitable.

Le cas échéant, l'intervention du juge judiciaire pourrait survenir en aval d'une procédure de médiation permettant un règlement à l'amiable des litiges afférent au droit à l'oubli entre les différents parties en présence (c'est-à-dire, d'une part, le plaignant qui dénonce une atteinte à sa vie privée et, de l'autre, l'éditeur du contenu litigieux). Celle ci devrait permettre a minima le respect d'un principe contradictoire ainsi qu'un recours à un conseil juridique pour les personnes concernées.

Enfin, au cas où serait reconnu un abus de liberté d'expression attentatoire à la vie privée, plusieurs types de mesures doivent être envisagés. En effet, si dans l'arrêt de la CJUE, il est seulement question du déréférencement, l'actualisation, l'effacement de certaines informations, l'anonymisation ou la pseudonymisation des publications litigieuses peuvent être plus adaptés et proportionnés, selon les cas d'espèce.

RECOMMANDATIONS

- En cohérence avec le principe d'une protection judiciaire de la liberté d'expression, garantir la compétence exclusive du juge judiciaire pour concilier la liberté d'expression et le respect de la vie privée.

- Réfléchir à la création d'une instance de médiation multipartite, permettant aux parties au litige de parvenir à un règlement à l'amiable (le recours au juge judiciaire devra évidemment rester possible en cas de non-accord entre les parties).

- Rappeler que le déréférencement de liens dans les moteurs de recherche constitue l'une des multiples mesures possible pour concilier la liberté d'expression et le droit à la vie privée (selon les cas, l'actualisation, le retrait, l'anonymisation, la pseudonymisation à la source du contenu litigieux peuvent s'avérer plus adaptés).

LE PARTAGE DE LA CULTURE ET DES CONNAISSANCES

Internet permet à chacun de partager librement l'information numérique. La réappropriation et la modification des œuvres (remix) devient en outre une pratique d'expression pour toute une génération. Aussi, les droits intellectuels sur l'information, quelle qu'elle soit, doivent s'adapter à cette nouvelle donne afin d'encourager l'accès à la culture et à la connaissance. Cela suppose de mettre un terme à la guerre contre le partage d'œuvres culturelles, et d'adopter des politiques permettant la réappropriation de la culture et de la connaissance par le public.

Afin que chacun d'entre nous puisse bénéficier des possibilités offertes par l'ère numérique, il est nécessaire de réformer le droit d'auteur et le copyright. La plateforme de propositions de La Quadrature du Net (VOIR P. xx) fournit une analyse détaillée des enjeux de cette réforme, et un ensemble de propositions portant sur le droit d'auteur et le copyright, mais aussi sur les politiques liées en matière de culture et de médias.

RECONNAÎTRE LE PARTAGE EN DROIT ET EN FAIT

• Il faut reconnaître la légitimité du partage d'œuvres culturelles entre individus sans but de profit en le plaçant hors du champ d'application du droit d'auteur, par exemple par la création d'une nouvelle exception.

• Les verrous numériques et autres dispositifs anti-copie devraient être abandonnés. Ils doivent être déclarés illégaux lorsqu'ils empêchent des usages licites.

• Les outils de partage, tels que les logiciels peer-to-peer, doivent pouvoir se développer en toute sécurité juridique.

Pour plus d'information :
– lire le point consacré au partage non marchand sur notre plateforme de propositions,
– Sharing Culture and the Economy in the Internet Age (1er février 2012) et Internet et Création (2008) de Philippe Aigrain, ainsi que son article sur la légitimité du partage,
– la réponse de La Quadrature à la consultation européenne sur le futur de l'économie culturelle,
– sur l'interdiction des DRM abusifs, voir enfin l'ancien projet de loi de réforme du droit d'auteur au Brésil.

NOUVEAUX MODÈLES DE FINANCEMENT DE LA CRÉATION, DE L'INFORMATION ET DES MÉDIAS

• Il est grand temps de créer une « contribution créative » pour le financement de la création et de l'expression publique à l'ère numérique, mutualisée entre tous les usagers et contributeurs d'Internet.

• Un observatoire indépendant et rendant compte au public analysera des données fournies volontairement par les utilisateurs pour définir les clés de répartition.

• Les ressources dégagées par la contribution créative récompenseront les auteurs et créateurs (y compris bien sûr pour les œuvres sous licences libres), et serviront à financer de nouvelles productions.

• Il faut enfin créer les conditions pour le développement de modèles économiques innovants, en facilitant l'accès à l'exploitation commerciale des droits d'auteur sur Internet.

Pour en savoir plus
– nos propositions de nouveaux modèles de financement de la culture numérique sont détaillées sur notre plateforme de propositions,
– mais aussi dans Sharing: Culture and the Economy in the Internet Age et Internet et Création,
– vous pouvez également visionner l'intervention au Sénat de Philippe Aigrain dans les auditions sur « Comment concilier liberté de l'Internet et rémunération des créateurs ? »,
– ainsi que le guide du Free Culture Forum.

RENFORCER LE DOMAINE PUBLIC ET LIBÉRER LE PATRIMOINE NUMÉRIQUE

• Après des années d'une politique infondée en la matière, il est nécessaire de revenir à une durée raisonnable des droits d'auteur et des droits voisins.

• Les pouvoirs publics doivent s'engager dans une politique ambitieuse en faveur des données publiques ouvertes.

• Il faut repenser les stratégies de numérisation du patrimoine, et encourager un modèle distribué permettant le concours de chacun à ces politiques culturelles.

Pour plus d'informations :
– voir notre plateforme de propositions,
– le Manifeste pour le domaine public,
– la réponse de La Quadrature du Net sur la numérisation du patrimoine culturel européen,
– sur l'ouverture des données, voir les travaux de Regard Citoyens.