NATURALISER L'ACCÈS À INTERNET L'assemblage de l'adresse IP aux normes communautaires et constitutionnelles

Le troisième chapitre de la partie de la thèse consacrée aux publics, porte, après les SPRD et la mission Olivennes, sur les collectifs de militants anti-hadopi et leur entrée en scène. À la question classique de Robert Dahl (1971) « Qui gouverne ? », ces collectifs illustrent et documentent un cas intéressant de « coalition de cause » théorisée par Paul Sabatier et Jenkins-Smith (1993) dans ses contributions au renouvellement des études de politiques publiques dans les années 90 avec la notion d'*Advocay Coalition Framework*. Ce chapitre s'intéresse ainsi aux modalités du blocage de l'action législative par une partie des acteurs des controverses générées par le projet de loi HADOPI qui ont obtenu de l'instance supérieure de contrôle de constitutionnalité la censure de l'ensemble du dispositif répressif de la loi en juin 2009. Il s'agit d'un processus original qui est parvenu à naturaliser un élément technique – l'adresse IP – maillon essentiel de l'accès au réseau des réseaux, en le faisant entrer dans le champ du droit constitutionnel. En déclarant que l'accès à internet constitue une des possibilités, désormais notable, d'exercer la liberté d'expression et d'information, le Conseil constitutionnel acclimate la thématique de l'accès à l'ordonnancement constitutionnel érigé sur les droits naturels. La notion de droits naturels irrigue en effet le préambule de la Constitution française de 1958 qui expose «les droits naturels, inaliénables et sacrés de l'homme, afin que cette déclaration, constamment présente à tous les membres du corps social, leur rappelle sans cesse leurs droits et leurs devoirs ; afin que les actes du pouvoir législatif et ceux du pouvoir exécutif, pouvant être à tout instant comparés avec le but de toute institution politique, en soient plus respectés ; afin que les réclamations des citoyens, fondées désormais sur les principes simples et incontestables, tournent toujours au maintien de la Constitution et au bonheur de tous.»[121]. Pour comprendre comment une série d'acteurs a réussi ce tour de force, nous rappelons en

[121]Voir aussi l'article 2 de cette Déclaration, «le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression » et l'article 4 de cette Déclaration, « la liberté consiste à pouvoir faire tout ce qui ne nuit pas à

premier lieu la définition de l'adresse IP, sa dimension matérielle et son administration comme preuve en droit pénal. Cette description des relations entre humains et non-humains s'inscrit dans le sillage des concepts relevant des *Science and Technology Studies* appliqués au numérique et des travaux de Janet Abbate (2010: 170-180) ou Niva Elkin-Koren (2006). La seconde partie du chapitre explique comment la riposte graduée contenue dans la loi HADOPI a pu concourir à l'hypothèse d'une clarification du statut juridique contradictoire de l'adresse IP au regard du concept de donnée personnelle. La troisième partie détaille le cheminement d'un amendement du parlement européen en parallèle des débats parlementaires qui, de l'extérieur, parviendra à infléchir le cours du débat français. Enfin, la dernière partie du chapitre porte sur l'étape ultime de la saisine et de la décision du Conseil constitutionnel dont l'un des considérants dispose qu'*« en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, [la libre communication des pensées et des opinions] implique la liberté d'accéder à ces services ».* La naturalisation déterminante de l'accès à internet dans le droit constitutionnel suit donc plusieurs étapes et canaux : construction de l'association juridique entre IP et données personnelles, matérialité de la preuve, amendement au niveau européen, et *in fine* saisine et décision du Conseil constitutionnel. Par l'entrée en scène et en action de collectifs de militants – en réalité une poignée d'individus - l'accès à internet parvient à se frayer un passage et à s'arrimer au droit constitutionnel. Cette naturalisation d'un dispositif socio-technique dans la norme juridique supérieure constitue une étape essentielle, quoique déstabilisante pour les artisans des lois HADOPI, du désir de « civiliser internet ».

autrui : ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la loi ».

I – La matérialité de l'adresse IP

L'adressage IP, maillon essentiel du réseau des réseaux.

Le courant des *Sciences and Technology Studies (STS)* affirme depuis les années 80 que les architectures techniques ne sont pas, comme l'a montré pour internet Barbara Van Schewik (2010), de simples artefacts « pertinents seulement pour les ingénieurs »[122] mais performent et sont performées par des dynamiques économiques, politiques, juridiques et sociales. Le courant des STS a souligné, à travers la théorie de l'acteur-réseau (Hård et Jamison (2005), Callon, Latour (2005)), que les préférences et les objectifs humains sont ancrés dans les artefacts techniques. L'agentivité n'est pas propre à l'être humain mais appartient collectivement à une association ou un réseau d'acteurs humains et non-humains où s'entremêlent les agentivités des personnes et des moyens technologiques. La recherche multidisciplinaire récente sur l'Internet a pu faire référence aux travaux de Winner (1980: 121-136) pour analyser les politiques incorporées dans ce medium. Lawrence Lessig (1999), pour sa part, a examiné dans *Code is law* la manière dont la conception des infrastructures et des services logiciels peut limiter le droit constitutionnel de l'utilisateur à la vie privée et à la liberté d'expression. En dépassant un simple déterminisme technologique, Lessig souligne que les acteurs humains à l'origine du code produisent une interchangeabilité du code avec d'autres formes culturelles de régulations comme le droit, les marchés et les normes sociales. Dans cette perspective et pour mieux saisir un agencement entre un objet technique (l'adresse IP) et une norme juridique de haut niveau (le droit constitutionnel), rappelons en premier lieu dans ce chapitre les principales étapes historiques, les notions fondamentales et les grandes définitions techniques du protocole TCP/IP (Transmission Control Protocol/Internet Protocol) qui sous-tend toutes les transmissions de données numériques sur internet.

[122]Cité par Musiani et Schafer (2011 : 62-71).

Notions essentielles

La notion de *protocole de communication* désigne une spécification d'un ensemble de règles lié à un type de communication particulier. Ces règles permettent à deux machines de communiquer en transformant des données en informations, non seulement en parlant un langage commun mais en s'accordant sur des règles minimales d'émission et de réception des données. Une notion essentielle connexe à celle de protocole de communication est celle de *couche de protocole*. Le principe d'un protocole de communication est de pouvoir interconnecter deux machines quelles qu'elles soient. Les protocoles sont composés de plusieurs modules effectuant chacun une opération. Ces opérations étant effectuées dans un ordre précis et de manière contiguë, on parle alors d'un modèle en couches. Les données qui transitent dans le réseau sont traitées successivement par chaque couche du protocole en émission comme en réception. Chaque couche du protocole va ajouter un élément d'information aux données sous la forme d'un en-tête aux données transmis à la couche suivante par un principe de concaténation. Sur un plan logique, un modèle en couches permet de séparer le problème en différentes parties selon leur niveau d'abstraction.

La transmission des données s'appuie sur le principe cardinal de *commutation par paquets*. C'est une innovation essentielle bien qu'ancienne qui désigne un processus d'acheminement des données dans lequel les messages sont découpés « en paquets » de petite taille informatique. Chaque paquet est doté d'un en-tête contenant les informations nécessaires à son transit par les nœuds du réseau. Une fois arrivés à destination, les messages sont reconstitués à partir des paquets reçus et des informations des en-têtes. Les paquets peuvent être acheminés selon deux modes : un « circuit virtuel » (un chemin est construit entre le nœud entrant et le nœud sortant, tous les paquets suivant dans l'ordre ce même circuit) ; ou selon le principe du « datagramme » (chaque paquet est traité indépendamment en fonction des ressources de transit disponibles, les paquets arrivent donc dans le désordre et doivent être remis en séquence au moment de leur arrivée au destinataire). Ce principe simple permet d'optimiser fortement la réservation des ressources nécessaires à la transmission des données. A l'inverse, en effet, la commutation de circuits – le modèle historique du réseau téléphonique - nécessite durant toute la durée de la transmission des données la réservation du circuit complet à débit constant entre deux machines, y compris pendant les

nombreux silences d'une communication informatique. La commutation par paquets optimise ainsi fortement les ressources de communication par une utilisation uniquement pendant la durée effective de transmission du paquet.

Deux dernières notions essentielles, qui vont heurter dans les années 70 la rationalité des normalisateurs historiques des télécommunications, caractérisent le protocole TCP/IP. En premier lieu, il s'agit du concept de *« best-effort delivery »* qui concerne un réseau n'offrant pas de garantie sur la qualité de service, notamment en matière de débit et de durée de transmission des données. La seule garantie est que les intermédiaires vont fournir le meilleur effort, à l'image du courrier postal dont la durée de transmission n'est pas garantie, les ressources n'étant pas allouées à l'avance, comme pour la commutation par paquets. Une autre notion liée à la précédente et au design d'internet concerne le « *principe de bout-en-bout* » (*end-to-end arguments*). Cet autre concept central de l'architecture du réseau internet (Bärwolff 2010) pose comme principe de repousser aux marges du réseau la couche applicative, « l'intelligence », diront certains. L'intérêt de cette idée permet de préserver la flexibilité et l'ouverture d'internet notamment en réduisant la complexité du cœur du réseau et les coûts induits de maintenance. Cette simplification du centre permet aussi d'accroître les chances que de nouvelles applications puissent être ajoutées sans risque pour le cœur du réseau. Symétriquement, les applications sont fiables puisqu'elles ne souffrent pas des modifications des couches inférieures du réseau. Dans cette perspective, le réseau doit transporter des paquets sans privilégier ni une adresse, ni un protocole, ni porter atteinte au contenu transmis.

Bref historique du protocole TCP/IP

Le protocole TCP/IP est en fait une « pile » de protocoles, puisqu'il associe deux protocoles différents aux opérations complémentaires dont nous proposons de retracer brièvement les principales étapes historiques. En 1969, l'agence américaine DARPA[123], rattachée au ministère de la défense, lance un projet expérimental d'étude de technologies de la communication basé sur la commutation de paquets

[123]Defense Advanced Research Projects Agency, http://www.darpa.mil

(ARPANET). Parallèlement en France, en 1972, le projet « Cyclades » basé lui aussi sur cette architecture et l'usage de datagrammes, est initié par Louis Pouzin mais se heurtera à la fin des années 70 à des choix politiques divergents sous la pression de l'opérateur national historique. L'expérience ARPANET est si concluante que les différentes entités rattachées à la DARPA l'utilisent quotidiennement. Elle passe officiellement du statut expérimental au statut opérationnel en 1975. ARPANET ne fonctionne pas encore avec le protocole TCP/IP, les arènes de normalisation des protocoles sont plurielles et hétérogènes, à ceci prêt que chacune d'entre elles a conscience qu'il ne sera pas possible de concevoir des réseaux monopolisés par un seul constructeur et qu'il est indispensable de créer un protocole ouvert capable de connecter toutes sortes de machines hétérogènes sur le plan de leur fonctionnement interne. En 1977, l'Organisation Internationale de Standardisation (ISO) se lance avec enthousiasme dans un vaste programme de normalisation d'interconnexion de systèmes ouverts (OSI : *Open Systems Interconnection*). L'OSI qui stabilise le principe des protocoles en couches empilables n'est publié qu'en 1984. La visée « babélique » de l'entreprise de l'ISO, sa lenteur, sa complexité et la prolifération de normes transitoires – comme la définition de l'IP en 1978-1981 par Jon Postel - ont abouti à un échec opérationnel. Pendant sa laborieuse conception au sein de comités techniques de l'ISO, la norme TCP/IP est parvenue à s'imposer *de facto*. Son processus d'innovation, fondamentalement opposé à l'élaboration classique d'une standardisation internationale opérée par les arcanes de l'ISO, s'est construit sur la mise en place par Stephen Crocker en 1969, d'un système original de documentation technique et de réflexion collective : les *Requests For Comments*. Cette méthode permet une participation large et informelle de collectifs d'ingénieurs à l'élaboration des protocoles. Une démarche souple et réactive, particulièrement adaptée à l'objet technique recherché qui a pu contourner le processus politique de normalisation de l'ISO et pris de vitesse l'effort multilatéral pour produire le protocole TCP/IP. Le milieu universitaire américain (l'Université de Berkeley en tête) et la « National Science Foundation », saisissent l'intérêt majeur de l'interconnexion des réseaux informatiques de recherche par le biais du protocole TCP/IP et allouent d'importants financements à son développement. Dès lors, le protocole TCP/IP a envahi l'intégralité du réseau des réseaux, y compris les réseaux locaux eux-mêmes, en raison de l'intérêt d'utiliser les mêmes protocoles pour l'interconnexion des machines au sein des réseaux locaux et pour l'interconnexion des réseaux locaux entre eux.

Pour atteindre ce degré de transparence pour l'utilisateur et acquérir cette robustesse d'utilisation planétaire, le design du protocole TCP/IP s'appuie sur quatre caractéristiques : 1/ il s'agit d'un protocole ouvert dont le code source est disponible gratuitement, développé indépendamment d'une architecture, d'un système d'exploitation, d'une structure commerciale particulière. Il est en outre transportable sur n'importe quel type de plate-forme, 2/ il est indépendant du support physique du réseau et de la technologie utilisée (câble, liaison radio, fibre optique, laser...) 3/ Le mode d'adressage est commun à tous les utilisateurs quelle que soit la plate-forme. Si l'unicité de l'adresse IP est respectée les communications aboutissent 4/ Les protocoles de haut niveau sont standardisés, rendant des développements inter-opérables sur tous types de machines.

Concernant sa structure en couches, le protocole TCP/IP simplifie le protocole OSI en ne comportant que quatre couches au lieu de sept.

Couche 4 Application	Applications standard du réseau (HTTP, SMTP, FTP, DNS ...)
Couche 3 Transport (TCP)	Assure l'acheminement des données et les mécanismes permettant de connaître l'état de la transmission
Couche 2 Internet (IP)	Fournit le paquet de données (datagramme)
Couche 1 Accès réseau	Spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé

L'adressage IP

Internet est donc un réseau virtuel qui interconnecte des réseaux physiques hétérogènes via des passerelles. Pour assurer l'homogénéité et rendre transparents les détails physiques des réseaux locaux, le principe de l'adressage est essentiel pour permettre la mise en relation d'un hôte avec n'importe quel autre. Pour assurer cette fonction cruciale, il est absolument nécessaire de parvenir à une unicité du principe général d'identification des machines connectées. Intuitivement, comme pour se rendre chez une personne physique, trois informations sont nécessaires : son nom, son adresse et la route à suivre pour s'y rendre. C'est exactement ce que permet l'adresse IP. A la différence près que, si les humains

utilisent des mots pour ces différentes informations, le processeurs d'une machine informatique va utiliser des nombres au format binaire. Les adresses IP sont standardisées sous la forme d'un nombre de 32 bits permettant de connaître deux informations fondamentales : l'identification de chaque hôte et le réseau physique auquel il appartient. Le choix des nombres constituant une adresse IP est essentiel pour assurer les opérations de routage, c'est à dire pour définir la route à emprunter par les paquets de données. La combinaison de l'adresse du réseau d'appartenance et de l'adresse de l'hôte au sein de ce réseau permet de désigner de manière unique une machine et une seule sur internet. Les adresses IP sont données aux abonnés par les Fournisseurs d'Accès (FAI), adresses qu'ils ont eux mêmes reçues de l'organisme chargé de définir les procédures d'attribution et de résolution de conflits : l'ICANN (*Internet Corporation for Assigned and Numbers*), société à but non lucratif fonctionnant grâce à un *memorandum* du Département du commerce américain et de ses structures régionales et locales. Par sa capacité à coordonner la distribution des adresses IP, le pouvoir de cet organisme est entier sur internet.

L'efficacité de l'ouverture du protocole TCP/IP et son design par couches le rendant indépendant des supports physiques du réseau et du type de machine utilisée sont conditionnés par un seul point de passage obligé: l'unicité de l'adressage IP. Ce point pratique, loin d'être dénué d'enjeu socio-politique, constitue le maillon essentiel pour réaliser le projet d'interconnexion potentiel de n'importe quelle machine avec n'importe quelle autre à l'échelle globale. L'architecture distribuée que permet entre autres le protocole originel TCP/IP est porteuse d'une vision politique, notamment à l'œuvre dans les échanges pair-à-pair qui « façonnent différemment les frontières entre l'usager et le réseau, mettent à disposition des utilisateurs un outillage techno-juridique pour se protéger, échanger, construire la légitimité de connaissances communes : avec le déploiement de ces dynamiques, sont en jeu l'attribution, la reconnaissance, la modification et l'équilibre des droits d'utilisateurs et fournisseurs au sein des services » (Musiani 2012: 315). Comme le montre Niva Elkin-Koren (Elkin-Koren et Salzberger 2012) dans ses travaux, le droit n'est pas simplement une réponse aux nouveaux problèmes posés par la technologie, dans bien des cas c'est aussi le droit qui façonne les technologies et en influence la conception. La co-construction entre ordre technologique et ordre juridique, explorée par des auteurs comme Séverine Dussollier (2012: 297-317), Danièle Bourcier (2010) ou Mélanie Dulong de Rosnay (2007), trouve ici un terrain particulièrement intéressant d'articulation entre l'objet technologique constitué par l'adresse IP

et les concepts juridiques de délit, d'infraction, d'identité et de preuve. En attribuant une adresse IP et une seule à une machine donnée, le protocole TCP/IP offre la possibilité de déterminer quelle machine a été utilisée pour commettre une infraction au droit. En matière d'instruction de la preuve à l'occasion d'un délit pénal, la notion de « preuve électronique » a progressivement constitué, comme nous allons le voir, un premier agencement entre l'objet technique qu'est l'adresse IP et l'ordre juridique.

Preuve et identité électroniques

La collecte de la preuve numérique en matière pénale

Il faut ici rappeler que tout mode de preuve est recevable en matière pénale. Tel est donc aussi le cas pour le téléchargement illicite qui entre dans la catégorie d'un délit de contrefaçon. Mais, si la matérialité des preuves est réelle dans l'univers numérique, elle s'avère difficile à rapporter et demeure facilement corruptible par les délinquants. Difficulté aggravée par l'ubiquité des données et leur localisation hors du territoire juridictionnel du droit national.

C'est pourquoi, grâce à sa flexibilité inhérente, le droit a pu et su s'adapter pour permettre aux autorités de police judiciaire de pouvoir appréhender des infractions qui paraissaient mettre le droit en échec par leur apparente dématérialisation et leur dimension transnationale. La loi pour la confiance dans l'économie numérique (LCEN, 21 juin 2004), élargit ainsi la notion de perquisition en disposant qu'il « [...] est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition ». Si une copie a été réalisée, il peut être procédé sur ordre du juge d'instruction, « à l'effacement définitif sur le support physique qui n'a pas été placé sous main de justice, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens »[124]. Au niveau européen, une procédure standard de collecte de preuves numériques a été établie sous le nom de *Cybertools online search evidence* (CTOSE). Entre autres

[124] Loi du 21 juin 2004, art. 41 et 43 - c. pr. pén., art. 97.

dispositions législatives récentes, on notera la loi du 23 janvier 2006 sur la lutte contre le terrorisme[125] qui introduit l'obligation de conservation des données de connexion des opérateurs de communications électroniques.

La particularité de l'évolution de la collecte des preuves numériques réside dans le rôle de plus en plus important des auxiliaires de justice et des acteurs privés. Plusieurs décisions ont ainsi écarté les constats établis à l'initiative du demandeur et contribué à préciser progressivement les contraintes de l'établissement de preuves sur internet. Les huissiers ont ainsi vu leurs procédures clarifiées. Les agents agréés par le ministère de la culture, qui nous intéressent au premier chef, ont eux-aussi vu leur compétence dans ce domaine renforcée par des décisions importantes qui nous détaillons ci-après. Les experts, dont le rôle est incontournable pour ces dossiers de procédure très techniques, ont aussi vu leur contribution stabilisée dans la collecte de la preuve numérique[126], ainsi que les fournisseurs d'accès qui se sont volontairement organisés à travers le réseau *InHope*[127] en vue de coordonner la lutte contre la pédopornographie de concert avec les autorités judiciaires.

Le mode de collecte de la preuve s'est donc adapté pour répondre à l'instabilité du domaine des échanges numériques en élargissant le spectre des acteurs et en dotant d'assise juridique leur action, à condition de respecter la définition canonique de la preuve du droit pénal qui en raison de son caractère nécessairement répressif et attentatoire aux libertés, oblige au respect des principes de loyauté, de proportionnalité et du contradictoire. Mais comme toujours, si le juge nourrit un doute sur les techniques probatoires utilisées, il peut en toute souveraineté écarter ces éléments de la procédure.

L'identité numérique : entre matérialité et présomption

La notion d'identité préside aux relations de l'individu avec les droits et permet aux institutions publiques de définir la titularité des droits et devoirs (élections, impôts…). Une identité se définit comme un

[125] Articles L. 34-1-1 du code des postes et des communications électroniques et 6 II bis de la loi du 21 juin 2004.
[126] Article 156 du nouveau code de procédure civile, « toute juridiction, d'instruction et de jugement, dans le cas où se pose une question d'ordre technique, peut, soit à la demande du ministère public, soit d'office, soit à la demande des parties, ordonner une expertise ».
[127] http://www.inhope.org/gns/home.aspx

ensemble de données, elle est souvent accompagnée d'un qualificatif (civile, génétique, biométrique, numérique…) qui permet de caractériser le régime juridique applicable à travers un réseau de temps, de lieux et de filiation. La loi LOPPSI 2 (Loi d'orientation et de programmation pour la performance de la sécurité intérieure, du 14 mars 2011) a étendu l'infraction d'usurpation d'identité « punie des mêmes peines lorsqu'elle est commisse sur un réseau de communication au public en ligne ». Cet article admet donc que l'identité peut être établie selon des éléments de nature numérique.

Dans l'économie du cadre processuel, la fiabilité de l'identité repose sur deux types d'éléments qui sont : soit des données considérées comme faisant intrinsèquement partie de la personne (données génétiques ou biométriques) qui relèvent de son unicité ; soit des éléments détachables de l'individu (n° de sécurité sociale, matricule…). L'identité numérique ressort de cette catégorie. L'identité numérique « n'a aucun lien naturel ni institutionnel avec la personne de sorte qu'elle peut aisément être partagée, prêtée, échangée ou usurpée » (Deharo 2011: 87-102). L'administration de la preuve se trouve donc plus difficile à réaliser pour des éléments comme l'adresse IP qui présentent des liens très faibles avec l'unicité d'un individu.

Il importe de remarquer que les codes de procédure civile et pénale utilisent avec parcimonie le terme « d'identité » mais privilégient les éléments qui la composent (nom, date et lieu de naissance…). Il est également paradoxal de constater que le système numérique qui génère de vastes incertitudes sur les éléments de l'identité des individus est en revanche capable de tracer la relation entre les systèmes et machines informatiques qui ont servi aux échanges. L'établissement de connexions informatiques laisse toujours des traces et l'anonymat des machines utilisées est en principe impossible, puisque précisément l'adressage des machines, à elle et elle seule, permet l'établissement des flux de données. L'identité numérique produit un effet limité en matière d'identification car elle est dépourvue de signification propre attachée à la personne. En raison de ces effets limités, les juges font toujours preuve d'une grande prudence quant à son instrumentalisation possible. La jurisprudence enseigne donc que l'identité numérique est une identité incomplète qui doit être corroborée par d'autres éléments, comme nous le verrons ultérieurement dans les controverses autour du traitement de l'adresse IP par les agents assermentés des Sociétés de Perception et de Répartition des Droits (SPRD).

L'identité numérique matérialisée notamment par l'adresse IP présente donc des liens très faibles d'attachement à l'identité civile d'une personne. Si elle permet la traçabilité des échanges de données entre des machines informatiques, elle échoue à remplir les critères complets d'une identification au sens juridique du terme. Il est néanmoins possible, comme la jurisprudence l'a montré, de surmonter ces carences par le mécanisme classique de la présomption « qui existe uniquement lorsqu'un fait, c'est-à-dire un événement de la vie quotidienne qui n'a pas été réalisé dans le seul but de la préconstitution d'une preuve, permet d'établir un second fait jusqu'alors difficile, voire impossible à prouver » (Quétand-Finet 2013: 143).

II – Le rôle de l'adresse IP dans le concept de riposte graduée

Jusqu'au milieu des années 2000, l'adresse IP permettait certes une traçabilité des échanges, mais difficilement, à elle seule, une identité. Sa qualification comme « donnée personnelle » demeurait très instable sur le plan juridique. Les innovations en matière préventive et répressive du projet de loi DADVSI puis HADOPI reposent sur le concept de « riposte/réponse graduée ». Cette idée originale prévoit, dans un souci initial de prévention, de pouvoir adresser à l'internaute en infraction un ou plusieurs avertissements par mel et courrier avant de déclencher des mesures de répression proprement dites comme, ultimement, la coupure de l'accès à internet. Nous détaillons ici les prémices de cette idée et leurs implications dans le domaine de la clarification du statut juridique de l'adresse IP. Dans un second temps, nous examinons une controverse portant sur la nature juridique du mécanisme de traduction d'une adresse IP en donnée personnelle qui opposa la CNIL et les SPRD autour des constats de leurs agents assermentés. Dans un dernier paragraphe, une analyse des débats parlementaires concernant la fiction de la sécurisation de l'accès à internet souligne une certaine contradiction à admettre – d'un côté – que l'adresse IP échappe à la supervision de la CNIL parce qu'elle ne serait pas une donnée personnelle, et à affirmer – de l'autre – que cette même adresse IP est suffisamment personnalisée pour identifier et sanctionner l'internaute (Teller 2009: 2001) et qu'il faille en assurer l'inviolabilité par des procédés techniques dont les spécifications sont renvoyées aux décrets d'application de la loi.

La riposte graduée : une chance de clarification du statut juridique de l'adresse IP

« La charte musique » du 28 juillet 2004

Signée par Nicolas Sarkozy, Ministre de l'économie, des finances et de l'industrie, Renaud Donnedieu de Vabres, Ministre de la culture et de la communication, Patrick Devedjian, Ministre délégué à l'industrie, cette charte constitue le premier engagement symbolique mais effectif des pouvoirs publics dans la lutte contre le téléchargement illicite de biens culturels. La méthode qui consiste à obliger des parties à s'asseoir autour d'une table de négociation pour leur faire signer un document d'engagement réciproque pour éviter de passer par la phase réglementaire ou législative est à souligner car elle sera rééditée dans la phase préliminaire à HADOPI[128]. Cette charte vise en premier lieu à régler le contentieux entre fournisseurs d'accès et filière musicale concernant l'abus des campagnes publicitaires des FAI qui ont bâti le consentement à payer des abonnés à l'ADSL sur la promesse implicite d'accès gratuit mais illicite à des œuvres soumises au droit d'auteur. Les FAI s'engagent donc à « ne plus initier de campagnes publicitaires vantant le téléchargement illégal ou encourageant les échanges de fichiers musicaux protégés ». Autre point important, la charte, certes de manière un peu péremptoire, commence à introduire l'idée d'un « processus automatisé mis en œuvre en coopération avec les ayants droit permettant d'adresser, à la demande de ces derniers dans des délais les plus courts possibles […] un message personnalisé à tout abonné offrant ou téléchargeant illégalement des fichiers protégés, d'ici la fin de l'année 2004 ». Le texte glisse aussi l'idée d'une suspension de l'abonnement en demandant de « poursuivre les efforts entrepris contre la violation des droits de propriété littéraire et artistique dans les clauses de résiliation ou de suspension de l'abonnement figurant dans leurs conditions contractuelles avec les abonnés ». Les FAI se sont en outre engagés à ne référencer que les offres de musique légale sur leurs portails et à procéder au dé-référencement, sur demande des ayants droit, de sites violant les droits d'auteur. Pour leur part, les ayants droit s'engagent « avant la fin de l'année 2004 à mener des actions civiles et pénales ciblées à l'encontre de pirates et à donner à ces actions la visibilité nécessaire pour

[128]Voir chapitre 4.

atteindre l'objectif de sensibilisation voulu par les signataires de la présente charte ». Ils s'engagent par ailleurs à accroître l'offre licite de musique en ligne et à accorder de manière non discriminatoire et transparente l'autorisation d'exploiter leur répertoire aux exploitants de service en ligne. Enfin, avec les pouvoirs publics, les signataires annoncent étudier la mise en place d'instruments de mesure de la contrefaçon et aussi vouloir expérimenter des solutions de filtrage. Les pouvoirs publics, quant à eux, s'engagent « à faire de la lutte contre la piraterie sur internet une priorité de l'action politique, policière et judiciaire en étudiant en particulier les possibilités de renforcer les moyens des ayants droit pour agir contre la piraterie en ligne ». Enfin, FAI et ayants droit s'engagent « à s'abstenir de se mettre publiquement et réciproquement en cause sur le sujet ».

Cette charte tranche nettement avec les rapports et avis policés du CSPLA. Là où le Conseil tente d'approfondir avec des autorités académiques les enjeux juridiques très complexes et s'efforce de rendre des avis et recommandations équilibrés, la charte est un véritable texte de combat. En annonçant brutalement, et sans en mesurer les risques juridiques, l'avènement d'accords entre FAI et ayants droit pour mener des opérations d'envoi de messages auprès d'internautes supposés coupables de téléchargement illicite (qui reste un délit) , en suggérant la suspension de l'abonnement, en prônant le dé-référencement, en envisageant l'expérimentation du filtrage et en annonçant une vague de procédures civiles et pénales pour l'exemple, le tout co-signé par trois ministres, la charte aura surtout pour effet d'attirer l'attention des associations de défense des libertés sur internet et de laisser transparaître une certaine « panique » de la filière musicale.

Prémices de « l'approche graduée » au Conseil Supérieur de la Propriété Littéraire et Artistique

Le Conseil Supérieur de la Propriété Littéraire et Artistique (CSPLA) est la première instance publique créée avec l'objectif explicite de conseiller l'exécutif face à l'évolution des échanges de biens culturels à l'ère numérique, notamment dans leur dimension juridique. Cette arène va donc être déterminante pour forger les positions politiques vis-à-vis de ce défi à la fois technologique, économique et juridique dès le début de la décennie 2000. Ses membres, ses avis et recommandations, ses relations avec les autres grands

acteurs des controverses vont progressivement dessiner les contours de la mise en politique des problèmes posés par l'extension des échanges de biens culturels numérisés, en particulier entre 2003 et 2005, c'est à dire dans la période qui précède la première tentative d'élaboration législative, la loi sur le droit d'auteur et les droits voisins dans la société de l'information (DAVDSI) du 1er août 2006. Cette instance consultative a pour origine le rapport « Désir de France » du député PS de la 7ème circonscription de Paris, Patrick Bloche[129]. Un nom à retenir puisqu'il sera un des principaux ténors de l'opposition au moment des débats sur la loi HADOPI. Ce rapport, remis au premier Ministre de l'époque Lionel Jospin en décembre 1999, porte sur « la présence internationale de la France et de la francophonie dans la société de l'information ». Son auteur y prône la constitution d'une instance consultative indépendante chargée de la médiation pour les questions de propriété intellectuelle liées « à la société de l'information et plus particulièrement à l'internet ».

C'est chose faite par un arrêté conjoint du ministère de la culture et de la communication et du Garde des Sceaux du 10 juillet 2000 qui institue auprès du ministre chargé de la culture le CSPLA pour une durée de six ans. Son existence sera par la suite pérennisée par l'article 17 de la loi du 1er août 2006, dite DAVDSI. Le CSPLA, stipule l'arrêté de création, a pour but de conseiller le ministre de la culture sur les questions de propriété littéraire et artistique, de remplir une fonction d'observatoire de l'exercice et du respect des droits d'auteur et droits voisins et de suivi de l'évolution des pratiques et des marchés à l'exception des questions de concurrence qui relèvent du Conseil de la concurrence. Il peut aussi aider à la résolution des différends relatifs à l'application de la législation sur des sujets qui mettent en cause les intérêts collectifs des professions. Son objectif est donc « de concilier les intérêts légitimes des professionnels des industries culturelles et l'intérêt général de la création et de l'accès à la culture ». Sa présidence est assurée par un conseiller d'État et sa vice-présidence par un conseiller à la Cour de cassation. Le nombre de ses membres titulaires est assez important puisqu'il atteint la cinquantaine. Le CSPLA comprend plusieurs catégories de membres : des membres de droit de l'administration centrale[130],

[129]On retrouve aussi parmi les contributeurs, David Kessler, conseiller médias et culture du Président de la République depuis mai 2012 et Jean Noël Tronc, Directeur général de la SACEM depuis septembre 2012.

[130]Le directeur de cabinet du Ministre de la culture, le directeur de l'administration générale assisté du sous-directeur des affaires juridiques et du chef du bureau de la propriété littéraire et artistique qui assurent le secrétariat du CSPLA. Le directeur du service juridique et technique de l'information et de la communication, le directeur des affaires civiles et du sceau au ministère de la justice, un représentant du ministère de l'éducation nationale et de la recherche, un représentant du ministère de l'économie, des finances et de l'industrie, un représentant du ministère des affaires étrangères.

trente deux membres représentant les professionnels[131], et huit personnalités qualifiées en matière de propriété littéraire et artistique nommées par le Ministre de la culture dont trois professeurs d'université et deux avocats à la Cour. Cette structure fait donc qualitativement et quantitativement une place presque exclusive aux professionnels des industries culturelles. Les opérateurs des Télécoms sont pratiquement absents et les usagers marginalisés. En revanche, la structure techno-étatique encadre fortement l'ensemble, tant sur le plan de la présidence et de la vice-présidence que pour le secrétariat. L'arrêté précise aussi que la création des commissions spécialisées est décidée par le président et les rapporteurs désignés par ce dernier de manière privilégiée au sein du Conseil d'État, de la Cour des comptes ou de l'ordre judiciaire. Selon le règlement intérieur, les séances du CSPLA ne sont pas publiques et les membres et experts sont tenus à l'obligation de discrétion.

L'avis 2005-2 du CSPLA cible les échanges pair-à-pair et surtout la « licence globale » ; il évoque étrangement, au détour d'un paragraphe et pour la première fois, le concept de « l'approche graduée » qui consiste à assurer en aval d'un téléchargement illicite la mise en place de mécanismes prévoyant des actions de sensibilisation et de responsabilisation et, le cas échéant, des sanctions appropriées. Mais la commission du CSPLA chargée de la rédaction du rapport et de l'avis en question déclare ne pas avoir étudié cette voie, puisqu'elle a été, écrit-elle, élaborée « en parallèle » par les représentants de la filière cinématographique[132] et les FAI membres de l'Association des Fournisseurs d'Accès (AFA). Le CSPLA précise, pour semble-t-il se démarquer de cette initiative, que « les travaux visant à finaliser ce projet se poursuivent entre les parties intéressées ». Ces mentions laconiques attestent de la constitution de regroupements d'acteurs hors du CSPLA qui cherchent à rendre effectif le droit d'auteur sur les réseaux numériques. A la différence du CSPLA, très encadré sur le plan technocratique par le ministère de la culture, d'autres acteurs ont choisi une méthode plus pragmatique en approchant, directement comme le précise l'avis du CSPLA, « les cabinets des ministres ». Clairement, plusieurs acteurs cherchent à se libérer d'une tutelle ministérielle pour s'adresser directement aux membres de l'exécutif. D'autre part, les ministères approchés ne se limitent pas au seul ministère de la culture et de la communication, qui bien

[131]10 représentants des auteurs, et à chaque fois deux représentants des auteurs et éditeurs de logiciels, des artistes-interprètes, des producteurs de phonogrammes, des éditeurs de presse, des éditeurs de livre, des producteurs audio-visuels, des producteurs de cinéma, des radiodiffuseurs, des éditeurs de services en ligne, des consommateurs.

[132]ALPA, ARP, BLIC, BLOC, PROCIREP, SACD.

que prestigieux, ne dispose pas d'une administration aussi organisée, nombreuse et puissante que ceux des finances et de l'industrie, structurée par de grands corps comme les inspecteurs des finances ou les corps techniques, notamment celui des Télécoms. Si le ministère de la culture compte bien dans son périmètre la communication, au sens classique du terme, tout le secteur des Télécoms et des fournisseurs d'accès à internet échappe à ses prérogatives. Ainsi, « parallèlement » au CSPLA, les fournisseurs d'accès et la filière cinématographique vont entamer des discussions afin de proposer, non plus des avis, mais des ébauches d'« opérations » susceptibles de résoudre cette perte d'efficacité du droit dans l'univers numérique. Le rapport du CSPLA qui s'en fait publiquement l'écho, indique deux souhaits fondamentaux des parties aux négociations, très importants pour comprendre la suite des événements et les positions profondes des parties prenantes. En premier lieu « la solution législative retenue ne devra entraîner aucune confusion avec le champ actuel de la contrefaçon » ; en second lieu, cette solution devra être « véritablement efficace ».

Nous avons ici une étape clé du processus qui se propose d'établir un droit spécial de lutte contre le téléchargement illicite visant « à créer un outil de lutte contre les actes des abonnés permettant des échanges illégaux d'œuvres cinématographiques commis de manière ponctuelle par des non professionnels dans un but non lucratif. Il se distingue des actions en responsabilité délictuelle que les ayants droit de cette filière se réservent d'engager à l'encontre de la piraterie réalisée à titre onéreux, des actes de téléchargement massif ou encore des actes de première mise à disposition sur les réseaux ». Cette « approche graduée » comporterait trois étapes, indique le rapport du CSPLA. Les FAI transmettraient en premier lieu par courrier électronique à leurs abonnés un message d'avertissement relayant les constatations faites par les agents assermentés des ayants droit[133]; un courrier en recommandé serait adressé à l'abonné en cas d'absence de modification de son comportement ; un troisième niveau consisterait à sanctionner financièrement l'abonné toujours récalcitrant. L'importance réside dans le degré suffisamment dissuasif de la sanction financière et son application effective. Le but général de « l'approche graduée » est de faire changer les comportements avant les poursuites judiciaires, sans toutefois abaisser le niveau de protection du droit d'auteur.

Le CSPLA conclut son compte rendu de cette initiative parallèle en émettant des réserves sur le plan

[133]Au titre des dispositions des art. L. 331-2 du CPI

juridique en raison, notamment, de l'inachèvement de la réflexion entre parties aux négociations. Les ayants droit du secteur musical, membres du CSPLA, soulignent par ailleurs que n'ayant pas été associés aux travaux, ils « réservent leur position ». Réserve d'autant plus prudente qu'eux aussi ont mené des actions importantes débouchant sur la signature par trois ministres, la filière musicale et les fournisseurs d'accès d'une « charte d'engagement pour le développement de l'offre légale de musique en ligne » près d'un an plus tôt.

Le principe de l'approche graduée, appelée successivement « riposte » puis « réponse » graduée au fil du processus HADOPI, fait de l'adresse IP, élément matériel de l'accès d'une machine au réseau, la pierre angulaire de la lutte contre le téléchargement illicite. La commission Olivennes de novembre 2007 recommande ainsi de « mettre en place soit une politique ciblée de poursuite, soit un mécanisme d'avertissement et de sanction allant jusqu'à la suspension et la résiliation du contrat d'abonnement, ce mécanisme s'appliquant à tous les fournisseurs d'accès ». Idée « inscrite dans le marbre » des Accords de l'Élysée qui stipulent, en engageant *ex-ante* la représentation nationale, que les pouvoirs publics s'engagent « à proposer au Parlement les textes législatifs et à prendre les mesures réglementaires permettant de mettre en œuvre un mécanisme d'avertissement et de sanction visant à « désinciter » l'atteinte portée aux droits de propriété intellectuelle sur les réseaux numériques. Ce mécanisme devrait porter sur le principe de responsabilité de l'abonné du fait de l'utilisation frauduleuse de son accès [...] ». Cette perspective n'est pas sans réjouir par avance les juristes qui voient dans la notion hybride d'approche graduée, volontairement à la fois pédagogique et répressive, une occasion de clarifier la qualification juridique de l'adresse IP. En premier lieu, l'opération induite par l'approche graduée doit conduire à une clarification du statut de l'adresse IP vis-à-vis de la notion cardinale de donnée personnelle inscrite dans la grande loi « Informatique et libertés» de 1978. Cette question est conditionnée par le type de « traitement » subi par les données brutes des adresses IP – automatisé ou non – et par l'agent de ce traitement – humain ou non-humain. En outre, les données numériques ainsi traitées doivent à un certain moment de la procédure être traduites en données nominatives pour identifier le titulaire de l'abonnement mis en cause. La stabilisation du cadre juridique et procédural de la réconciliation entre données collectées et traitées et identification nominative est à la fois une condition d'opérationnalité de la mesure « d'approche graduée » et, plus largement, un moment essentiel et attendu

pour l'assemblage du concept d'accès à internet avec l'ordre juridique. Un arrêt du 13 janvier 2009 de la chambre criminelle de la Cour de cassation illustre dans les faits sur le plan de la jurisprudence les controverses entremêlées de la matérialité de l'adresse IP dans l'instruction d'un délit pour contrefaçon, et l'hésitation entre traitement humain et non-humain de cette donnée pour lui conférer ou non un statut direct ou indirect de donnée personnelle à caractère nominatif.

Le rôle du traitement de l'adresse IP dans sa traduction en donnée personnelle

(arrêts de la Chambre criminelle, Cour de cassation du 13 janvier 2009, n° 08-84.088 et du 16 juin 2009, n° 08-88.560).

L'extension du pouvoir d'enquête des agents assermentés des Sociétés de Perception et de Redistribution des Droits (SPRD) aux réseaux numériques est une condition essentielle pour la lutte contre le téléchargement illicite[134]. C'est l'étendue de ce pouvoir et son appréciation progressive par les différentes instances judiciaires qui vont permettre de stabiliser le statut et la qualification de l'adresse IP au regard notamment du droit au respect de la vie privée et plus largement dans l'articulation de cette notion à la norme suprême de la Constitution et aux normes communautaires supra-nationales, comme nous le verrons ultérieurement avec l'amendement 138 dit Bono/Cohn Bendit et la saisine du Conseil constitutionnel après le vote de la première loi HADOPI.

Avant cela, examinons deux arrêts de janvier et juin 2009 de la Chambre criminelle de la Cour de cassation qui vont participer à un début de clarification du statut juridique de l'adresse IP en fonction de la nature de son traitement. Cette sous-controverse liée à l'instabilité entre matérialité de l'adresse IP et donnée personnelle à travers le traitement automatisé ou humain de ces données constitue un cas exemplaire d'articulation entre humains et non-humains chère à l'anthropologie des sciences et des techniques de Michel Callon et Bruno Latour. Les faits à l'origine du premier arrêt remontent au 4 janvier 2005, lorsque qu'un agent assermenté de la SACEM et de la SPRD entame une procédure de constatation d'actes de contrefaçon d'œuvres musicales, conformément à l'article L. 331-2 du Code de la

[134]Voir chapitre 3.

propriété intellectuelle[135]. L'arrêt de la Chambre criminelle de la Cour de cassation relate avec précision les étapes techniques qui ont permis d'engager les poursuites :

> *« […] en se livrant à des opérations que tout internaute peut effectuer, après avoir ouvert une session sur un logiciel de pair à pair et s'être connecté à un réseau, l'agent verbalisateur a lancé, sur Internet, une requête portant sur une œuvre musicale du répertoire de la SACEM avant de sélectionner, dans la liste des nombreux résultats affichés, l'offre émanant d'un internaute puis de lire, dans la rubrique « parcourir l'hôte », son adresse IP (Internet Protocol) qui s'est affichée spontanément ainsi que le nombre total d'œuvres musicales mises à disposition des autres internautes dans le dossier de partage de l'internaute concerné ; que l'agent a, ensuite, procédé, à titre d'échantillon, au téléchargement de dix-neuf de ces œuvres musicales, encodées au format Mp3, avant de déterminer les coordonnées du fournisseur d'accès correspondant à l'adresse IP susvisée et de s'assurer de l'exactitude de cette adresse ; que, sur la base du procès-verbal ensuite dressé, la SACEM a porté plainte auprès des services de gendarmerie ; que ces services ont, après autorisation du Parquet, adressé une réquisition au fournisseur d'accès pour identifier l'abonné utilisant l'adresse IP relevée par l'agent assermenté ; que les vérifications effectuées ont révélé que l'ordinateur portable de cet abonné était utilisé par C. S. qui a reconnu qu'il avait procédé au téléchargement de nombreuses œuvres musicales avant de les mettre à disposition d'autres internautes ».*

Cyrille S., l'internaute incriminé, sera condamné en première instance pour contrefaçon à 2000 euros d'amende dont 1000 avec sursis, en plus de la confiscation de ses CD et de son ordinateur, ainsi qu'à 3000 euros de dommages et intérêts au profit de la SACEM et de la SDRM. Faisant appel de ce jugement, Cyrille S. voit la Cour d'appel de Rennes annuler en mai 2008 toute la procédure au motif que le traitement effectué par l'agent assermenté tombe sous le coup de la loi Informatique et Libertés qui requiert une autorisation de la CNIL – que l'agent n'avait pas sollicitée – pour procéder à l'établissement de tous fichiers de données indirectement nominatives, même si l'article 9-4 de la loi en question autorise les SPRD à rassembler des informations relatives au téléchargement illicite sur les

[135] *« Outre les procès-verbaux des officiers ou agents de police judiciaire, la preuve de la matérialité de toute infraction aux dispositions des livres Ier, II et III du présent code peut résulter des constatations d'agents assermentés désignés selon les cas par le Centre national du cinéma et de l'image animée, par les organismes de défense professionnelle visés à l'article L. 331-1 et par les sociétés mentionnées au titre II du présent livre. Ces agents sont agréés par le ministre chargé de la culture dans les conditions prévues par un décret en Conseil d'État ».*

réseaux pair-à-pair[136]. Cette affaire survient alors que les ayants droit intensifient le recours aux constats de leurs agents assermentés et que leur validité est fréquemment mise en cause, empêchant de prouver la matérialité du délit de contrefaçon. La loi Informatique et Libertés entre en effet en conflit avec le Code de propriété intellectuelle au sujet de la constitution de fichiers d'adresses IP, de la nature du traitement conféré à ces données et de la nature juridique de l'adresse IP comme donnée personnelle, nominative ou indirectement nominative. La cour d'appel de Rennes conclut ainsi : « *en l'absence d'autorisation préalable de la CNIL pour procéder à ces opérations, les constatations relevées par l'agent et ayant pour finalité la constatation du délit de contrefaçon, commis via les réseaux d'échange de fichiers "peer-to-peer", portent atteinte aux droits et garanties des libertés individuelles que la loi du 6 janvier 1978 a pour but de protéger et aux intérêts du prévenu.* ». Face à cette jurisprudence qui remet en cause le pouvoir d'enquête par la fragilité de la validité des constats, les SPRD décident de se pourvoir en cassation. La question posée à la chambre criminelle de la Cour de cassation est simple et cruciale : les constatations de l'agent assermenté peuvent-elles être ou non qualifiées de traitement de données personnelles soumis à déclaration auprès de la CNIL car portant sur des infractions ? La Cour de cassation répond par la négative en décidant que les constatations de l'agent assermenté « ne constituent pas un traitement de données à caractère personnel relatives à ces infractions ».

Pour parvenir à cette conclusion audacieuse qui vise à mettre un terme à un conflit de lois entre le Code de la propriété intellectuelle et la loi Informatique et Libertés, la Haute juridiction va concentrer en premier lieu son analyse sur le type de traitement effectué par l'agent assermenté. Pour échapper à toute obligation de déclaration préalable à la CNIL, l'arrêt va souligner que le traitement n'est pas, en l'espèce, automatisé. L'agent assermenté ayant accédé « manuellement » aux œuvres, son comportement n'est pas automatisé mais bien le résultat d'une activité humaine. Dans ce cas le « traitement automatisé de

[136]Cour d'appel de Rennes, 3ème chambre, le 22 mai 2008, Monsieur S C c/ SACEM, SDRM et Ministère Public :

« (…) Il s'ensuit, que si l'article 9-4° de la loi [Informatique et Libertés], permet à la SACEM, dans le cadre de la lutte contre les atteintes à la propriété littéraire et artistique, de rassembler des informations relatives à l'utilisation des réseaux d'échange « peer-to-peer » pour le téléchargement illicite des œuvres protégées et de constituer ainsi des fichiers de données indirectement nominatives, la mise en œuvre de ces traitements reste soumise en raison de leur nature, à autorisation préalable de la CNIL (…)

En l'absence d'autorisation préalable de la CNIL pour procéder à ces opérations, les constatations relevées par l'agent et ayant pour finalité la constatation du délit de contrefaçon, commis via les réseaux d'échange de fichiers «peer-to-peer», portent atteinte aux droits et garanties des libertés individuelles que la loi du 6 janvier 1978 a pour but de protéger et aux intérêts du prévenu. (…)

données à caractère personnel » n'est pas recevable, l'autorisation de la CNIL est sans objet et le constat qui apporte la preuve de la matérialité du délit ne peut donc être déclaré nul. Mais, l'article 2 de la loi Informatique et Libertés vise aussi des « *traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers* ». Le comportement de l'agent assermenté entre de plain pied dans la définition générale donnée par la loi Informatique et libertés du traitement de données à caractère personnel : « *constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* ». Donc, si la Cour de cassation affirme que les faits examinés « ne constituent pas un traitement de données à caractère personnel relatives à ces infractions », soit il n'y a pas eu « traitement » – ce qui est difficile à soutenir, vu la définition très large admise par la loi Informatique et libertés –, soit les données ne sont pas « à caractère personnel ».

Si l'on suit le syllogisme de l'arrêt, des commentateurs concluent que « si le traitement non automatisé n'est pas soumis à autorisation préalable de la CNIL, c'est parce qu'il ne porte pas sur des « données à caractère personnel » » (Caron 2009). Ces arguments apparemment contradictoires et sibyllins soulignent en fait que la traduction factuelle de l'adresse IP en donnée à caractère personnel est un processus. L'adresse IP n'est pas, en soit, une donnée à caractère personnel au moment où elle est collectée par l'agent. La Cour de cassation tente d'introduire une nuance entre la matérialité de l'adresse IP au moment de sa collecte (une suite de chiffres) et ce qu'elle peut révéler ultérieurement dans le cadre d'une réquisition du Parquet à un fournisseur d'accès (l'identité de l'abonné). L'arrêt fait donc sortir du domaine d'application de la loi Informatique et libertés les constats manuels des agents qui se contentent de collecter des adresses IP, qui, à cet instant, ne relèvent pas de la définition de donnée personnelle. Les agents assermentés peuvent donc réaliser ces constatations sans obtenir préalablement l'autorisation de la CNIL et sans craindre leur nullité dans le cadre d'une procédure.

Cet arrêt de la plus haute juridiction de l'ordre judiciaire français qui, de ce fait, revêt un caractère normatif très puissant va jeter un trouble considérable sur le plan juridique et médiatique : la Cour de

cassation a-t-elle décidé de contredire frontalement la position de la CNIL qui a toujours affirmé que l'adresse IP était une donnée personnelle ? Voire de faire dissidence avec les autorités communautaires et la directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[137] qui institue dans son article 29, un groupe de travail constitué des autorités de protection des données de chaque pays membre de l'Union européenne. Groupe de travail qui a conclu sans ambiguïté que les adresses IP sont des données à caractère personnel. En réalité, la Cour de cassation se garde de trancher et de qualifier l'adresse IP de donnée intrinsèquement nominative. C'est l'action humaine sur cette donnée matérielle qui est au cœur de l'arrêt. Comme le traitement de la donnée a été manuel et non automatique, la Cour distingue selon les moyens utilisés par l'agent pour collecter les informations et dont un certain type – dans le cas d'une automatisation du traitement – aurait dû donné lieu à une déclaration auprès de la CNIL. Mais cette décision feint d'ignorer que, quelle que soit la nature du procédé et les moyens mis en œuvre, l'autorisation préalable de la CNIL est nécessaire dès lors qu'il s'agit d'une donnée à caractère personnel (Teller 2009: 1988). En conclusion, la fragilité de cet arrêt permet de progresser quelque peu sur le chemin étroit de l'assemblage de l'adresse IP avec la norme juridique. Sans avoir définitivement stabilisé la controverse, il est simplement possible d'affirmer avec certitude que « l'adresse IP constitue un des éléments du faisceau d'indices permettant d'identifier l'internaute » (Teller 2009: 1988).

Les règles de l'identité juridique ne semblent pas transposables dans l'univers numérique. Nous avons vu en effet que la jurisprudence de la Cour de cassation ne permet pas de manière catégorique de conclure que l'adresse n'est pas une donnée à caractère personnel. Cette fragilité est sans doute à considérer comme un moyen de faciliter l'administration de la preuve qui demeure toujours délicate en matière de contrefaçon sur les réseaux pair-à-pair. Pourtant, signale Marina Teller, pour la Cour de Justice de l'Union Européenne la protection de la propriété intellectuelle « ne peut pas préjudicier aux exigences liées à la protection des données à caractère personnel […]. Dans le cadre d'une action relative à une atteinte à un droit de propriété intellectuelle et en réponse à une demande justifiée et proportionnée du requérant, les autorités judiciaires compétentes [peuvent] ordonner que des informations sur l'origine

[137]Directive 95/46/CE du Parlement européen et du Conseil du 24 oct. 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE L 281 du 23 nov. 1995, p. 31.

ainsi que sur les réseaux de distribution des marchandises ou des services qui portent atteinte à un droit de propriété intellectuelle soient fournies»[138]. La CJUE s'appuie sur un principe de proportionnalité à la charge des législateurs nationaux en vue de concilier droits et intérêts.

L'arrêt de la Cour de cassation inscrit la matérialité de l'adresse IP dans un faisceau d'indices qui, corroborés mutuellement, permettent *in fine* l'identification d'un internaute. Il faut notamment y intégrer les circonstances et la possibilité matérielle qu'a un internaute mis en cause de s'être connecté à internet au moment de la commission de l'infraction[139]. Il faut aussi considérer que l'usurpation d'adresse IP (spoofing) est à la fois très fréquente et très difficile à prévenir et que les perspectives de généralisation de la riposte graduée risquent d'accroître ces pratiques d'usurpation d'identité numérique. Concernant la riposte graduée, il y a bien *une certaine contradiction à admettre, d'un côté, que l'adresse IP échappe à la supervision de la CNIL parce qu'elle ne serait pas une donnée personnelle et à affirmer, de l'autre, que cette même adresse IP est suffisamment personnalisée pour identifier et sanctionner l'internaute* (Teller 2009: 2001). Mais la jurisprudence évoquée ici à travers l'arrêt symptomatique de la Cour de cassation de janvier 2009 s'inscrit dans un courant favorable à la lutte contre les actes de téléchargement illicite dont les lois HADOPI seront l'aboutissement. L'efficacité de cette orientation repose sur le rassemblement probant d'éléments de preuve par les agents assermentés des SPRD, comme c'est le cas pour d'autres Autorités Administratives Indépendantes comme la HALDE, le CSA ou encore l'Autorité des Marchés Financiers (AMF).

Le caractère hybride de l'adresse IP et le principe de symétrie entre matérialité technique et signification juridique présentent donc un cas intéressant de la nécessité de dépasser la dichotomie « des choses entre elles » et des « acteurs eux mêmes » et d'interroger une vision essentialiste et explicative du naturel et du social au profit de réseaux de médiations peuplés de collectifs nature-culture. Selon Jean-Marc Weller (1997 : 94-101), « le principe de symétrie et la considération des hybrides interdisent de réduire les échanges entre les humains au social et montrent comment la possibilité même d'une interaction dépend également des objets qui la peuplent ». Ainsi, la description de cette situation ne peut faire sens sans la

[138]CJCE 29 janv. 2008, op. cit. V. C. Caron, Appréciation de l'obligation de communiquer des données à caractère personnel dans le cadre d'une procédure civile, JCP E 2008. 1270.
[139]Dans le cas des auditions de la Commission de Protection des Droits, un internaute a pu ainsi invoquer une raison valable qui le disculpait d'une infraction de contrefaçon, bien que titulaire de l'abonnement : il était en effet incarcéré au moment des faits.

prise en compte de l'hybridation capable d'établir des associations entre des matériaux si divers. Mais, pour trancher entre deux visions du monde, celle de la CNIL qui interdit sans son consentement l'inscription d'un individu dans un fichier informatique et celle des SPRD qui n'y voit que la seule prise possible pour faire respecter ses droits de propriété, la Cour de cassation, pour élaborer son jugement et le justifier, a dû, certes mobiliser des objets, mais aussi intégrer des contraintes de cohérence, de justification, de pertinence, de logique ou de sens. Les arrêts rendus par la Chambre criminelle en 2009 ont pu ainsi faire craindre un certain « laxisme » au regard de la loi Informatique et Libertés. « Il semble plutôt que c'est dans un souci de compromis et de réalisme – ne pas désarmer la répression par des protections excessives – que ces solutions ont été retenues. » (Francillon 2010: 173).

La coupure de l'accès – et la fiction technique de sa « sécurisation » –, mère des controverses

Le véritable point de fixation, au-delà de la difficulté pratique à qualifier juridiquement l'adresse IP, est le projet de procéder à la coupure de l'accès à internet de l'internaute récalcitrant qui aurait bravé un avertissement par mel doublé d'un courrier recommandé. Cette menace ultime va, à elle seule, cristalliser les passions en raison de la portée symbolique de l'atteinte à la liberté d'un individu de se connecter à internet entravant par là même l'expression de certaines libertés fondamentales comme la liberté d'expression et d'information. Si l'on peut comprendre que les victimes du téléchargement illicite souhaitent brandir une menace d'autant plus grande que le délit de contrefaçon est complexe à définir et à appréhender, il est étonnant de constater que ses promoteurs n'ont pas mesuré les conséquences symboliques, constitutionnelles, procédurales et pratiques de cette idée. La prise ainsi offerte aux opposants à la lutte contre le téléchargement illicite va générer une large controverse centrée sur la désignation de l'autorité judiciaire capable de décider de la suspension de l'accès à internet. Une sous-controverse toute aussi florissante va prospérer sur l'effectivité technique de la décision juridique de la suspension et, corrélativement, sur la possibilité de sécuriser un accès internet par l'internaute.

Une controverse technique, et non des moindres, va donc être soulevée à propos des moyens de sécurisation des connections, de leur fiabilité et de l'absence, au moment de la discussion, des

spécifications techniques de ces logiciels laissant entrevoir des risques notables en matière de respect de la vie privée. Ces mesures sont résumées par le court article Art. L. 331-30 : *« La Haute Autorité établit la liste de moyens de sécurisation regardés comme efficaces pour prévenir les manquements à l'obligation mentionnée à l'article L. 336-3* [140]*»*. Lors des débats parlementaires , l'amendement 451[141] des députés Brard et Billard, va amener cette question avec l'exposé des motifs suivants : *« Il est inacceptable d'obliger les internautes à faire l'acquisition de logiciels commerciaux privés de « sécurisation », ce qui s'apparente à l'obligation de recourir aux services d'une société privée de vigiles, adaptée à l'Internet »*. Les discussions de cet amendement sont symptomatiques des tensions entre des mesures apparemment simples et la réalité des faits en matière de sécurité informatique.

> *Mme Martine Billard. […] « Par l'amendement 451, nous proposons de supprimer ces dispositions, sur lesquelles il vaut la peine de se pencher plus longuement. L'utilisation des ces moyens de sécurisation est censée exonérer les utilisateurs d'Internet de la responsabilité que cette loi va leur faire porter. […] Puisque c'est l'utilisation de tels dispositifs qui exonère le titulaire de l'accès de sa responsabilité, comme le précise l'article L. 336-3, chaque abonné à Internet se trouvera obligé d'en installer, ce qui constitue à nos yeux une réduction arbitraire de son droit à l'information, à la communication et au respect de la vie privée. [...]*
>
> *Imposer une telle obligation est inadmissible. On peut discuter de la philosophie de la riposte graduée. Mais comment justifier qu'on oblige à sécuriser ainsi un poste de travail, alors qu'on ne demande pas la même sécurisation pour d'autres fonctions de l'Internet ? Rappelons que l'accès à des contenus ou applications sur internet ne peut être limité que suite à une décision de l'autorité judiciaire. […] Ajoutons qu'obliger à l'utilisation de ces techniques peut poser un problème de respect de la libre concurrence.*

[140] Art. L. 336-3. - Le titulaire d'un accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'oeuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.

« Le fait, pour la personne titulaire d'un accès à des services de communication au public en ligne, de manquer à l'obligation définie au premier alinéa peut donner lieu à sanction, dans les conditions définies par l'article L. 331-25.

[141] http://www.assemblee-nationale.fr/13/amendements/1240/124000451.asp

[…] Selon une étude parue récemment dans une revue de sécurité, dans les 5e et 13e arrondissements de Paris, sur 31 000 points d'accès à Internet étudiés, plus de 2 000 étaient totalement ouverts et plus de 40 % utilisaient le protocole WEP notoirement inefficace, puisqu'il peut être cassé en moins de quatre minutes. En résumé, je suis totalement opposée à ce dispositif pour des raisons de fond ; au demeurant, il est irréaliste, inapplicable et donc inefficace.

M. le président. Quel est l'avis de la commission ?

M. Franck Riester, rapporteur. Avis défavorable. Il vaut la peine de disposer, dans la palette de sanctions, de cette possibilité d'adresser au titulaire d'un accès Internet une injonction de le sécuriser. L'article L. 331-30 prévoit d'établir une liste des spécifications nécessaires pour que la sécurisation soit effective, mais ne désigne pas les logiciels de telle ou telle société. C'est tout à la fois transparent et efficace. Qui plus est, la procédure d'évaluation et de labellisation des moyens de sécurisation sera fixée par décret.

M. le président. Quel est l'avis du Gouvernement ?

Mme Christine Albanel, ministre de la culture. Avis défavorable. Nous souhaitons encourager l'utilisation la plus systématique possible de ces logiciels de sécurisation, car il y a là également une dimension pédagogique. De même, il faut encourager l'activation des codes de sécurité de la Wi-Fi par les particuliers. L'abonné à Internet n'a pas d'obligation de se doter de ces moyens de sécurisation. Mais celui qui fait cet effort est présumé s'être ainsi acquitté de son obligation de surveillance et dégagé de toute responsabilité. Des logiciels de ce type sont sur le marché, et ils fonctionnent. Il y a des pare-feux, des logiciels de contrôle parental.

M. Lionel Tardy. Mais non, cela ne marche pas !

Mme Christine Albanel, ministre de la culture. […] La liste des moyens de sécurisation parmi lesquels l'abonné choisira librement sera établie, aux termes de l'article L. 331-30 du code de la propriété intellectuelle, sur la base de spécifications fonctionnelles objectives. Figureront donc sur cette liste tous les dispositifs qui remplissent les fonctions jugées

nécessaires pour empêcher le renouvellement du manquement. La Haute autorité, en établissant cette liste, ne donnera en aucun cas la préférence à tel dispositif, propriétaire ou non, et se bornera à vérifier que les dispositifs présentés par le fabricant en vue de leur inscription remplissent bien les fonctionnalités nécessaires.

Mme Martine Billard. Je ne sais si nous allons finir par arriver au bout de ce débat : il est tout de même surprenant ! Je souhaite bien du plaisir à la HADOPI pour parvenir à établir la liste des « spécifications nécessaires fonctionnelles objectives » dont parlait Mme la ministre. Monsieur Riester, il suffit de lire les pages de votre rapport consacrées aux problèmes que cela pose pour constater que les choses ne sont pas si simples. »

À elle seule, la question de la sécurisation de l'accès à internet et notamment de la connexion sans fil ouvre une quantité de problèmes en plus de la fragilité intrinsèque de la sécurité en matière informatique : comment imposer de telles contraintes aux usagers alors que même les professionnels ne sont pas capables de garantir la sécurité des réseaux ? Quelles seront les spécifications techniques et dans quels délais seront-elles disponibles pour que le marché s'en saisisse ? Comment arguer que la simple déclaration d'installation d'un logiciel de sécurisation dédouane l'usager s'il peut le désactiver facilement ? Dans le cas contraire, si la désactivation du logiciel est transmise automatiquement à la HADOPI, la Haute Autorité prend le risque juridique d'établir, de fait, la surveillance des réseaux. À l'issue de ces discussions très techniques et beaucoup plus développées que lors de la lecture au Sénat, plusieurs points importants sont à souligner. Très peu de députés ont réellement pris part à la discussion, quatre de l'opposition (Patrick Bloche, Christian Paul, Jean-Pierre Brard et Martine Billard) et deux pour la majorité (Lionel Tardy et Jean Dionis du Séjour). Ils ont dénoncé les obstacles techniques risquant de rendre le projet de loi inapplicable. Les défenseurs, au delà des invectives sans contre-arguments techniques, n'étaient représentés que par la Ministre de la culture Christine Albanel et surtout le député Franck Riester qui vivait son « baptême du feu » en tant que rapporteur d'un projet de loi.

Les quatre principaux blocages techniques abondamment développés au cours des débats semblent rendre le projet de loi objectivement déconnecté de la réalité des contraintes techniques qui pèsent sur les échanges numériques et la matérialité des réseaux de communications électroniques. Plutôt que de