REVUE LAMY

Droit de l'immatériel

MAI 2009

INFORMATIQUE | MÉDIAS | COMMUNICATION

Collection LAMY DROIT DE L'IMMATÉRIEL

49

Lamy
une marque Wolters Kluwer

Les dernières évolutions jurisprudentielle et légales intervenues en la matière sont nombreuses et génèrent des questions dont la résolution s'avère délicate. Aussi, les éléments de clarifications apportés Mes Florence Chafiol-Chaumont et Antoine Bonnier sont-ils les bienvenus.

L'identification des « pirates du Web » à partir de leurs adresses IP

De la qualification du constat probatoire de l'agent assermenté mandaté par la SACEM au projet de loi « HADOPI »

Par Florence CHAFIOL-CHAUMONT
Avocat Associé
August & Debouzy

Par Antoine BONNIER
Avocat
August & Debouzy
Membre du Cerdi

Depuis quelques années, l'engouement général provoqué par la possibilité de pouvoir télécharger et posséder gratuitement (mais illégalement, faut-il le rappeler) des œuvres protégées *via* les réseaux *peer to peer*, a poussé les ayants droit de l'industrie culturelle à réagir à la vue de l'effondrement de leur système économique. Ces derniers ont notamment engagé des actions judiciaires à l'encontre des pirates du web, après les avoir identifiés sur internet au moyen de leur adresse IP. Mais la mise en place de « *surveillances numériques* » et d'identifications ont soulevé de nombreuses problématiques juridiques et sociologiques (liées notamment au respect du droit à la vie privée) qui ne cessent d'alimenter encore aujourd'hui les débats « passionnels » entre ayants droit, internautes, autorités administratives, judiciaires et exécutives.

En effet, comme l'a très récemment rappelé la Cour de justice des Communautés européennes dans deux affaires portant sur ce thème (1), la protection des droits de propriété intellectuelle, le droit fondamental à une protection juridictionnelle et effective de ces droits et la protection des données à caractère personnel et donc de la vie privée, constituent tous des principes généraux du droit communautaire. En conséquence, il revient aux États membres de trouver un juste équilibre entre le respect de chacun de ces droits, sans en privilégier un au profit d'un autre.

En France, la lutte contre la contrefaçon sur internet s'est déroulée en deux temps : Dans un premier temps, les Sociétés de perception et de répartition des droits (ci-après les « SPRD ») ont, tout d'abord, souhaité poursuivre en justice les contrefacteurs. Cette volonté a toutefois très vite été confrontée à des problématiques de preuve. En effet, comment démontrer de manière certaine le téléchargement illicite d'un fichier informatique incorporant un contenu protégé par un droit de propriété intellectuelle ?

La contrefaçon est un fait : la preuve de sa matérialité peut donc être rapportée par tous moyens. Néanmoins, si tous les modes de preuve sont admis en justice pour démontrer la survenance d'un fait juridique, leur force probante n'en demeure pas moins différente et variable. Afin de minimiser les difficultés de preuve auxquelles elles se trouvaient confrontées, les SPRD ont alors imaginé une procédure selon laquelle : (i) elles faisaient appel à des agents assermentés chargés de repérer les adresses IP des personnes s'adonnant au téléchargement illicite d'œuvres protégées, (ii) ces derniers dressaient des procès-verbaux faisant mention des adresses IP relevées, (iii) elles portaient, ensuite, plainte devant les autorités judiciaires concernées en se fondant sur le procès-verbal ainsi réalisé.

Toutefois, les internautes poursuivis n'en sont pas restés là et ont argué de la nullité de ces constats au regard de la loi du 6 janvier 1978 (2) (ci-après la « loi Informatique et libertés »). Ils se sont, en effet, fondés sur le fait que l'accord de la Commission nationale de l'informatique et des libertés (ci-après, la « CNIL ») n'avait pas été préalablement sollicité alors qu'il s'agissait selon eux d'une obligation conformément aux articles 2 et 25 de la loi « Informatique et libertés ».

Le constat probatoire de l'agent assermenté : traitement de données personnelles nécessitant l'autorisation préalable de la CNIL ou simple relevé d'adresses IP non soumis à une quelconque formalité ? L'enjeu de la réponse était de taille pour les ayants droit car l'ensemble des procé-

(1) CJCE, 19 févr. 2009, aff. C-557-07, *LSG c/ Tele2 Telecommunication* ; CJCE, 29 janv. 2008, aff. C-275/06, *Promusicae c/ Telefónica de España*. (2) L. n° 78-17, 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés.

dures encourues était fondé sur des procès-verbaux potentiellement nuls pour ne pas avoir obtenu l'aval de la CNIL.
Finalement, la Cour de cassation a tranché, par un arrêt du 13 janvier 2009, et s'est prononcée en faveur de la seconde alternative, considérant qu'aucune formalité préalable n'était requise et ce, pour le plus grand bonheur des SPRD (I).
Dans un second temps cependant, les actions judiciaires à l'encontre d'internautes étant très mal perçues par une majorité de justiciables, les SPRD ont alors imaginé la mise en place d'un nouveau procédé plus pédagogique, consistant à réaliser des messages personnalisés d'avertissement envoyés *via* les fournisseurs d'accès à internet à ceux des internautes ayant été identifiés comme téléchargeant des contenus illicites.
Avec la mise en œuvre de ces procédures judiciaires, les SPRD souhaitaient créer une prise de conscience générale sur les enjeux juridiques liés au *peer to peer* et attirer l'attention des internautes sur les conséquences économiques du piratage pour l'industrie culturelle.
Cette disposition est finalement devenue l'axe principal du projet de loi dit « HADOPI », « *favorisant la diffusion et la protection de la création sur internet* » (II).

I. – LA LUTTE CONTRE LA CONTREFAÇON DES ŒUVRES SUR INTERNET *VIA* LE CONSTAT PROBATOIRE D'UN AGENT ASSERMENTÉ : LA COUR DE CASSATION SE PRONONCE ENFIN SUR LA NATURE DU CONSTAT

Jusqu'à cet arrêt rendu par la chambre criminelle de la Cour de cassation, le 13 janvier 2009, la jurisprudence était incertaine quant au régime applicable aux constatations visuelles effectuées par des agents assermentés.
Ces constats étaient réalisés sur le fondement de l'article L. 331-2 (3) du Code de la propriété intellectuelle qui prévoit que « *la preuve de la matérialité de toute infraction* (…) *relative aux droits d'auteur* (…) *peut résulter des constatations d'agents assermentés désignés selon les cas par le Centre national de la cinématographie, 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 constatations, effectuées sur internet, permettaient de recueillir un certain nombre de renseignements à partir des adresses IP des internautes qui téléchargeaient du contenu illicite sur internet.
En reconnaissant la validité de ces constats probatoires effectués sans l'autorisation préalable de la CNIL, la Cour de cassation met fin à une longue incertitude juridique (B).

> Jusqu'à l'arrêt rendu par la chambre criminelle de la Cour de cassation, le 13 janvier 2009, la jurisprudence était incertaine quant au régime applicable aux constatations visuelles effectuées par des agents assermentés.

Il est à noter que cet arrêt de Cour de cassation était grandement attendu par un ensemble de praticiens imaginant que celle-ci réglerait la question de savoir si une adresse IP devait ou non être considérée comme étant une donnée à caractère personnel, question ayant déjà donné lieu à de nombreux arrêts rendus par différentes Cours d'appel. Cependant, la Cour de cassation s'est bien gardée de se prononcer sur ce point et a rendu un arrêt pour le moins sibyllin (A).
Or, la question de savoir si l'adresse IP est ou non une donnée à caractère personnel aurait notamment permis de connaître avec certitude les conditions devant, le cas échéant, être préalablement remplies pour que des constats sur les adresses IP des internautes contrefacteurs soient valablement dressés par des agents assermentés.

A. – L'adresse IP : une donnée à caractère personnel ? Un débat clos ?

Pour rappel, l'adresse IP (pour *Internet Protocol*) est un numéro unique correspondant à l'adresse d'un ordinateur connecté à l'internet. Cette adresse IP est constituée de quatre nombres, chacun compris entre 0 et 255.
Conformément à la loi « Informatique et libertés » qui se calque, même si les termes employés sont différents, sur les dispositions de la directive 95/46/CE du 14 octobre 1995 (4), la notion de donnée à caractère personnel est extrêmement large. En effet, « *constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement* ou indirectement, par référence à un numéro d'identification *ou à un ou plusieurs éléments qui lui sont propres* » (5).
C'est notamment pour cette raison que la CNIL (6) et le groupe dit de « l'article 29 » (7) qualifient l'adresse IP de donnée à caractère personnel en estimant logiquement que cette donnée est *indirectement personnelle* puisqu'elle permet *in fine*, à l'instar d'une plaque d'immatriculation, de remonter jusqu'au contrefacteur, à tout le moins jusqu'au titulaire de la connexion.
Toutefois, du point de vue de la jurisprudence, la qualification retenue est bien plus nuancée, notamment depuis les arrêts de la Cour d'appel de Paris rendus en 2007.
En effet, selon les juridictions parisiennes, l'adresse IP est rattachée par essence à une machine et non à une personne et rien ne saurait permettre de déterminer l'identification de la personne à l'origine de la contrefaçon : « *cette série de chiffre en effet ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon* » (8).
Dans le même sens, une autre section de la Cour d'appel de Paris a affirmé que « l'adresse IP ne permet pas d'identifier la ou les personnes qui ont utilisé cet ordinateur *puisque seule l'autorité légitime* >

(3) C. propr. intell., art. L. 331-2 : « *la preuve de la matérialité de toute infraction aux dispositions des livres Ier, II et III du présent code et de l'article 52 de la loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle peut résulter des constatations d'agents assermentés désignés selon les cas par le Centre national de la cinématographie, 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* ». (4) Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 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. Selon l'article 2a) de cette directive, constitue une donnée à caractère personnel « *toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ». (5) Loi « Informatique et libertés », art. 2, al. 2. (6) Communiqué officiel, 2 août 2007 : « *L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes* », <www.cnil.fr>. (7) Avis n° 4/2007 du 20 juin 2007 sur le concept de données à caractère personnel du groupe dit « article 29 », groupe établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE. (8) CA Paris, 13e ch., sect. A, 15 mai 2007, *Henri S. c/ SCPP*, <www.legalis.net>.

pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur d'accès l'identité de l'utilisateur » (9).

À l'inverse, la troisième chambre de la Cour d'appel de Rennes annulait à deux reprises (dans des arrêts des 22 mai et 23 juin 2008) des procès-verbaux d'agents assermentés qui avaient collecté des adresses IP sans obtenir préalablement l'autorisation de la CNIL, en estimant notamment que « *l'adresse IP de l'internaute, constitue une donnée indirectement nominative* » (10). En effet, l'article 25-I 3° de la loi « Informatique et libertés » prévoit que tout traitement de données à caractère personnel relatif aux infractions, condamnations et mesures de sûreté doit être soumis à l'autorisation préalable de la CNIL.

Au vu des différents enjeux économiques et juridiques nés de la contrefaçon, et de l'incertitude jurisprudentielle chronique quant à cette question, la position de la Cour de cassation sur ce sujet, suite au pourvoi formé à l'issue de la décision rendue le 22 mai 2008 par la Cour d'appel de Rennes, était très attendue. Mais en vain !

En effet, la Cour de cassation, dans son arrêt rendu le 13 janvier 2009, a confirmé la position des juges parisiens et cassé l'arrêt de la Cour d'appel de Rennes du 22 mai 2008, mais seulement sur la question du régime applicable aux constats de l'article L. 331-2 du Code de la propriété intellectuelle. En revanche, alors que les différentes juridictions saisies de ces questions s'étaient préalablement prononcées sur la nature de l'adresse IP, la Cour de cassation a décidé d'évincer la question…

Cette absence de positionnement clair des magistrats de la Haute Cour sur une question aussi essentielle est d'autant plus regrettable que l'adresse IP est, à ce jour, l'une des données existantes les plus sensibles dont la collecte sans contrôle effectif pourrait être nuisible au respect de la vie privée.

En effet, cette question renvoie de manière plus générale à celle de la valeur des traces informatiques que les internautes laissent ici et là en surfant sur internet.

Si l'adresse IP devait ne pas être définitivement considérée comme une donnée à caractère personnel (même indirectement personnelle), cela signifierait donc qu'elle pourrait être collectée par toute personne, pour une durée indéterminée et surtout pour n'importe quel type de finalité. On comprend aisément les risques de dérives que cela pourrait entraîner.

Dès lors, une confirmation par la Cour de cassation de l'existence d'un cadre légal destiné à régir le traitement de l'adresse IP n'aurait pas été inutile. De fait, le débat sur sa nature et sur sa qualification reste ouvert.

B. – La collecte de l'adresse IP par un agent assermenté : l'autorisation préalable de la CNIL n'est pas requise

Dans l'arrêt rendu par la Cour de cassation, le 13 janvier 2009, un agent assermenté désigné par la SACEM avait utilisé un logiciel de *peer to peer* afin de procéder à la constatation d'actes de contrefaçon d'œuvres musicales commis sur internet.

Pour sa défense, l'internaute avait soulevé l'exception de nullité du constat sur la base de la loi « Informatique et libertés » en soutenant que la SACEM n'avait pas respecté les dispositions de l'article 25-I 3° de la loi « Informatique et libertés » qui requiert l'autorisation préalable de la CNIL avant d'effectuer un constat.

> Une confirmation par la Cour de cassation de l'existence d'un cadre légal destiné à régir le traitement de l'adresse IP n'aurait pas été inutile.

Pour affirmer que ces constats constituaient un traitement de données à caractère personnel et rejeter, en conséquence, l'action de la SACEM en raison de la nullité du procès-verbal, la Cour d'appel de Rennes (11) avait notamment estimé que l'adresse IP devant être considérée comme une donnée personnelle et le traitement mis en place étant automatisé, l'autorisation préalable de la CNL aurait dû être sollicitée.

Même si la décision était critiquable sur l'automaticité supposée du traitement – la démonstration de la Cour était très lacunaire – le raisonnement des magistrats d'appel quant à la nature de l'adresse IP était, en revanche, tout à fait conforme aux positions de la CNIL, du groupe dit de l'« article 29 » (12) et de la définition de la loi.

Mais c'était sans compter sur le positionnement de la Cour de cassation qui, pour casser cette décision et rejeter l'idée même de l'existence d'un traitement de données à caractère personnel, s'est fondée exclusivement sur le mode opératoire mis en œuvre par l'agent assermenté, sans se prononcer expressément sur la nature de l'adresse IP.

1°/ Traitement automatisé ou manuel : l'incidence du procédé

Dans son attendu de principe, la Cour de cassation affirme, en visant notamment les articles 2, 9, 25 et 50 de la loi « Informatique et libertés », que « *constitue un traitement de données à caractère personnel relatives aux infractions toute opération* automatisée *ou tout ensemble d'opérations automatisées portant sur de telles données ainsi que toute opération* non automatisée *ou tout ensemble d'opérations non automatisées portant sur de telles données contenues ou* appelées à figurer dans des fichiers ».

Autrement dit, peut être uniquement qualifié de traitement de données à caractère personnel portant sur des infractions :

- le traitement *automatisé* de telles données ; et
- le traitement *non automatisé* de telles données contenues ou appelées à *figurer dans des fichiers*. Rappelons que conformément à l'article 2, alinéa 4, de la loi « Informatique et libertés » : constitue un fichier « *tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés* ».

Autrement dit, pour écarter l'application de la loi « Informatique et libertés » à la collecte de données à caractère personnel portant sur des infractions, il conviendra, tout d'abord, de vérifier que le traitement n'est pas automatisé et, le cas échéant, de s'assurer que les données collectées ne sont pas destinées à figurer dans un fichier.

En l'espèce, pour écarter l'application de ladite loi au constat probatoire effectué par l'agent assermenté, la Cour de cassation souligne, en premier lieu, que le recueil d'informations avait été effectué sans recourir à un « *traitement préalable de surveillance automatisé* ». L'arrêt mentionne, ensuite, que l'agent accédait manuellement à la liste des œuvres proposées irrégulièrement, en se contentant simplement de relever les adresses IP qui s'affichaient à son écran.

Le caractère manuel du traitement (donc non automatisé) étant établi, restait alors à vérifier la présence ou non d'un fichier struc-

(9) CA Paris, 13e ch., sect. B, 27 avr. 2007, *M. G.A c/ SCPP*, <www.legalis.net>. (10) CA Rennes, 3e ch. crim., 22 mai 2008, *SACEM, SDRM et Ministère Public c/ Cyrille S.* (11) Précité. (12) Organe consultatif européen indépendant sur la protection des données et de la vie privée établi en vertu de l'article 29 de la directive 95/46/CE.

turé destiné à recevoir les données à caractère personnel relatives aux infractions. Or, après avoir détaillé l'ensemble du mode opératoire de l'agent assermenté, la Cour de cassation se contente simplement d'en conclure que ce procédé ne constitue pas un traitement au sens de la loi, sans se prononcer sur la présence ou non d'un tel fichier.
Partant, doit-on en déduire, à la seule lecture de l'arrêt, que les adresses IP relevées ne figureraient pas dans un fichier ? Si tel étais le cas, cela serait problématique car, en pratique, chaque adresse IP collectée par l'agent assermenté n'est-elle pas nécessairement classée dans un fichier en fonction de la date du constat, des œuvres contrefaites, etc. ? À défaut, le sérieux du constat ne pourrait-il pas être remis en cause par les internautes ?
Sinon, deuxième option, doit-on en déduire que les magistrats considèrent implicitement que l'adresse IP ne constitue pas en soi une donnée à caractère personnel (13) ? Dans ce cas précis, la loi « Informatique et libertés » serait inapplicable au cas d'espèce, non pas en vertu de l'absence de fichier structuré et donc de la nature du procédé, mais simplement en raison de la nature même des données collectées.
Toutefois, si tel était le cas, pourquoi la Cour de cassation aurait-elle pris la peine de décrire l'ensemble du mode opératoire de l'agent assermenté et d'insister sur le caractère manuel de la collecte ? Il lui aurait simplement suffit de statuer sur la nature de la donnée collectée pour arriver à la même solution.
On le voit, cet arrêt de cassation laisse de nombreuses zones d'ombre. Les décisions ultérieures, et notamment celle de la Cour d'appel de Paris désignée en l'espèce comme cour de renvoi par la chambre criminelle, seront donc très éclairantes sur ces points.

2°/ L'incidence de la personne du « collectant » sur la nature de l'adresse IP

Le pourvoi formé par la SACEM à l'issue de l'arrêt rendu par la Cour d'appel de Rennes, le 22 mai 2008, arguait également que l'obtention de l'identité de l'internaute à partir de son adresse IP ne pouvait être requise auprès du fournisseur d'accès que par l'autorité judiciaire. Ainsi, elle affirmait que ces données ne présentaient donc pas, en elles-mêmes, de caractère personnel, puisque seul le juge pouvait faire le rapprochement entre la donnée chiffrée et l'identité de la personne.
Comme nous l'avons préalablement envisagé, cet argument avait été accueilli favorablement par les deux arrêts de la Cour d'appel de Paris de 2007 et avait été confirmé plus récemment par la 3e chambre de l'instruction de la même cour le 28 mai 2008 (14).
Également, la Cour de cassation semble implicitement faire référence à cette notion de personne du « *collectant* ». Elle affirme, en effet, que l'adresse IP est relevée par l'agent « *pour pouvoir localiser son fournisseur d'accès* [à internet] *en vue de la découverte* ultérieure *de l'auteur de la contrefaçon* ».
Toutefois, cet argument ne saurait, selon nous, être recevable au regard de la loi « Informatique et libertés ». S'il est vrai qu'en soi, l'adresse IP ne permet pas d'identifier directement une personne, il est incontestable que cette donnée est indirectement personnelle en ce qu'elle permet *in fine* de remonter jusqu'à la personne étant titulaire de la connexion internet ayant permis, à partir d'un poste informatique donné, de se livrer à des actes de contrefaçon sur internet. Et s'il devait s'avérer que ce n'est pas le titulaire de la connexion internet qui est à l'origine de la contrefaçon, il lui appartiendra alors d'indiquer aux autorités judiciaires l'identifié de la personne ayant effectivement commis l'infraction (à l'instar des procès-verbaux adressés au propriétaire d'un véhicule à qui il appartient, s'il n'est pas à l'origine de l'infraction routière, d'indiquer aux autorités l'identité de la personne étant à l'origine de l'infraction). La plaque d'immatriculation des véhicules ayant depuis longtemps été reconnue comme constituant une donnée indirectement personnelle, il paraît dès lors étrange que des débats interviennent sur l'adresse IP qui se trouve être dans une configuration similaire à celle de la plaque d'immatriculation automobile.

> L'inefficacité constatée des procédures judiciaires intentées contre les internautes contrefacteurs a contraint les SPRD à se tourner vers un procédé plus pédagogique.

Dès lors, l'incidence de la personne du « collectant » sur la nature de cette information doit être écartée.
En outre, les risques liés à la collecte de données sensibles sont d'autant plus élevés que les données à caractère personnel sont désormais numériques et font l'objet, en pratique, d'un commerce très lucratif. Elles sont, en effet, revendues, transférées, échangées entre commerçants, passant ainsi de main en main dans une transparence toute relative.
Partant, il serait bien trop risqué, car incertain, de considérer que la qualification d'une telle donnée dépend de la qualité de la personne même du collectant ou de l'instant ou celle-ci est collectée. En conséquence, l'adresse IP doit, dès son origine, sa création, être qualifiée de donnée à caractère personnel.
En tout état de cause, cet argument de la SACEM n'a pas été retenu ni traité par la Haute Cour. En effet, plutôt que de se prononcer sur la qualification de l'adresse IP au regard de la définition de la donnée à caractère personnel prévue à l'article 2, alinéa 2, de la loi « Informatique et libertés », la Cour de cassation s'est limitée à l'alinéa 1er de ce même article qui n'envisage que le champ d'application de ladite loi.

II. – LA LUTTE CONTRE LA CONTREFAÇON *VIA* LA COLLECTE ET LE TRAITEMENT D'ADRESSES IP

Comme nous le rappelions en introduction, l'inefficacité constatée des procédures judiciaires intentées contre les internautes contrefacteurs a contraint les SPRD à se tourner vers un procédé plus pédagogique.
Celui-ci consistait à collecter les adresses IP des contrefacteurs, à réaliser des messages personnalisés d'avertissement et à les envoyer *via* leur fournisseur d'accès à internet. À terme, les SPRD devaient décider ou non des poursuites à donner contre les « récidivistes ».
Toutefois, cette volonté des SPRD relative à la mise en place de tels procédés s'est heurtée dès l'origine à l'opposition de la CNIL (A) en raison notamment de la possibilité de pouvoir identifier une personne physique à partir de son adresse IP, sans aucun contrôle de l'autorité judiciaire.
Cette crainte semble en partie avoir été entendue par le législateur *via* le projet de loi *favorisant la diffusion et la protection de la création sur internet*, qui prévoit d'accorder des nouvelles prérogati- >

(13) Pour une interprétation en ce sens : Caron Ch., *in* Comm. com. électr. 2009, n° 4, comm. 31. **(14)** CA Paris, 3e ch. instr., 28 mai 2008, n° 2007-01064.

ves à l'Autorité de régulation des mesures techniques (ARMT) (15) qui sera désormais dénommée Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI), pour garantir le respect de ces différents droits fondamentaux (B).

A. – Retour sur le contentieux ayant opposé la CNIL aux SPRD

Selon la nature des données collectées, un traitement de données à caractère personnel peut être mis en œuvre (i) après une simple déclaration effectuée auprès de la CNIL (16) ou (ii) après l'obtention d'une autorisation de celle-ci (17).
En l'espèce, la CNIL considérait que la collecte d'adresses IP afin de lutter contre la contrefaçon était assimilable à la collecte de données relatives aux infractions, condamnations et mesures de sûreté (18). Ainsi, les SPRD ne pouvaient entreprendre ce combat sans l'autorisation préalable de la CNIL.
En outre, les SPRD se heurtaient à une difficulté supplémentaire en ce que la collecte de telles données ne peut être mise en œuvre que par des personnes expressément et limitativement visées par la loi (19) ; liste dont elles ne faisaient pas partie et pour laquelle elles ont dû manifester leur besoin auprès du législateur.
Finalement, cette volonté des SPRD d'être intégrée à la liste de l'article 9 de la loi « Informatique et libertés » a été validée par le Conseil constitutionnel dans une décision du 29 juillet 2004 (20).
Celui-ci déclarait alors que, compte tenu du contrôle de ce traitement par la CNIL et de la mise à disposition de ces informations au juge, seul autorisé à effectuer le rapprochement entre l'adresse IP et le nom de l'internaute, « *ce traitement est de nature à assurer, entre le respect de la vie privée et les autres droits et libertés, une conciliation qui n'est pas manifestement déséquilibrée* ».
Cela s'est traduit *in fine* par la confirmation de l'intégration, en vertu de la loi du 6 août 2004 (21), d'une nouvelle disposition à l'article 9 de loi « Informatique et libertés » (22).
Suite à l'entrée en vigueur de cette loi, les SACEM (23), SDRM (24), SCPP (25) et SPPF (26) ont alors formulé des demandes auprès de la CNIL afin d'obtenir l'autorisation de mettre en œuvre de tels traitements.
Ces sociétés voulaient notamment pouvoir (i) repérer les internautes pratiquant l'« *upload* » (la mise à disposition de contenu au profit des tiers sur internet) ; (ii) réaliser un message personnalisé d'avertissement ; (iii) transmettre ce message ainsi que l'adresse IP concernée au fournisseur d'accès à internet ; et (iv) permettre au fournisseur d'accès à internet d'identifier l'abonné à partir de l'adresse IP communiquée afin qu'il lui envoie directement le message par courrier électronique.

> Selon la nature des données collectées, un traitement de données à caractère personnel peut être mis en œuvre après une simple déclaration effectuée auprès de la CNIL ou après l'obtention d'une autorisation de celle-ci.

Mais le 18 octobre 2005 (27), malgré les nombreuses discussions entreprises entre les différents acteurs, la CNIL a refusé d'autoriser ces quatre sociétés d'auteurs et de producteurs de musique à mettre en œuvre ces dispositifs. Pour justifier sa décision de refus, la CNIL avait notamment considéré que :
– la décision du Conseil constitutionnel du 29 juillet 2004 affirmait que les données collectées à l'occasion des traitements portant sur des infractions aux droits d'auteur « *ne pourront acquérir un caractère nominatif que dans le cadre d'une procédure judiciaire* » (alors que le dispositif proposé par les SPRD prévoyait une identification par le fournisseur d'accès à internet) ;
– les dispositifs présentés n'étaient pas proportionnés à la finalité poursuivie.
Toutefois, les différentes SPRD n'en sont pas restées là et ont décidé de faire appel de ces décisions devant le Conseil d'État. Le 23 mai 2007, le Conseil d'État a finalement fait droit aux demandes des SPRD et décidé d'annuler ces décisions en considérant que le traitement de données issu de la surveillance des réseaux n'était pas disproportionné au but légitime qui était poursuivi par ces sociétés, notamment en vertu de « *l'importance de la pratique des échanges de fichiers musicaux sur "internet"* » (28), contrairement à ce qu'estimait la CNIL.
Les SPRD ont alors formulé de nouvelles demandes auprès de la CNIL. Par deux décisions des 8 et 22 novembre 2007 (29), celle-ci a finalement autorisé les SACEM, SDRM et SCPP à mettre en œuvre ce traitement de données à caractère personnel, puis le 10 janvier 2008 (30), il en a été de même pour la SPPF.
Il convient de souligner qu'à cette même époque, le rapport « Olivennes » (31) a été remis au ministre de la Culture. Celui-ci invitait également la CNIL à « *tirer les conséquences de l'arrêt du 23 mai 2007 du Conseil d'État annulant sa décision du 18 octobre 2005 refusant à diverses sociétés d'auteur l'autorisation nécessaire à la mise en place d'un fichier permettant la recherche et la constatation des actes de contrefaçon sur internet* » (32). En plus de l'arrêt du Conseil d'État, il est probable que la CNIL ait pris sa décision en considération de cette « invitation ».
La remise de ce rapport a finalement débouché, le 23 novembre 2007 sur la signature de *l'accord pour le développement et la protection des œuvres et programmes culturels sur les nouveaux réseaux* (33), par l'ensemble des acteurs du secteur de l'industrie culturelle et des prestataires d'internet. C'est ce texte qui a véritablement posé les bases du projet de loi « HADOPI » tel qu'on le connaît aujourd'hui.

B. – La collecte d'adresses IP selon le projet de loi « HADOPI » garantit-elle la protection des droits des personnes à la vie privée ?

Outre la mise en place de la riposte dite « *graduée* », sur laquelle nous ne revien-

---

(15) L'Autorité de régulation des mesures techniques (ARMT) est une autorité administrative indépendante instituée par la loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information. **(16)** Loi « Informatique et libertés », art. 23 et 24. **(17)** Loi « Informatique et libertés », art. 25. **(18)** Conformément à l'article 25-I 3° de la loi « Informatique et libertés ». **(19)** Loi « Informatique et libertés », art. 9. **(20)** Déc. n° 2004-499 DC, 29 juill. 2004. **(21)** L. n°2004-801, 6 août 2004, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. **(22)** Loi « Informatique et libertés », art. 9 : « *Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par :* (...) *4° les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du Code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits* ». **(23)** Société des auteurs, compositeurs et éditeurs de musique. **(24)** Société pour l'administration du droit de reproduction mécanique des auteurs, compositeurs et éditeurs. **(25)** Société civile des producteurs phonographiques. **(26)** Société civile des producteurs de phonogrammes en France. **(27)** Délib. n° 2005-235, n° 2005-236, n° 2005-237 et n° 2005-238, 18 oct. 2005. **(28)** CE, 23 mai 2007, Caron Ch., Vers la traque des internautes contrefacteurs, Comm. com. électr. 2007, comm. 90. **(29)** Délib. CNIL n° 2007-334, 8 nov. 2007 et n° 2007-348, 22 nov. 2007. **(30)** Délib. CNIL n° 200.87-006, 10 janv. 2008. **(31)** Rapport au ministre de la Culture et de la Communication, nov. 2007 : Le développement et la protection des œuvres culturelles sur les nouveaux réseaux. **(32)** 12e recommandation du rapport Olivennes, p. 25. **(33)** <http://www.culture.gouv.fr/culture/actualites/index-olivennes231107.htm>.

drons pas ici, la collecte de l'adresse IP est au cœur du mécanisme prévu par le projet de loi « HADOPI » pour lutter contre le piratage d'œuvres protégées par un droit de propriété intellectuelle.
Désormais, selon le futur article L. 331-22 du Code de la propriété intellectuelle, il appartiendra aux agents assermentés désignés notamment par les SPRD et les organismes de défense professionnelle, de saisir la commission de protection des droits de l'HADOPI sur la base des informations recueillies sur la toile.
Autrement dit, les SPRD seront au cœur du dispositif de lutte contre la contrefaçon. Celles-ci pourront collecter les adresses IP des internautes sur le même modèle que celui soumis à la CNIL depuis 2005, processus que nous avons rappelé ci-avant.
Toutefois, seuls les agents assermentés habilités par le président de l'HADOPI et la commission de protection des droits de l'HADOPI pourront obtenir l'identité de l'internaute dont l'adresse IP a été collectée, auprès des opérateurs de communications électroniques (34).
Cette précision est d'importance au regard des différentes critiques formulées ici et là par les nombreux opposants à ce texte. En effet, ceux-ci insistent justement sur l'absence de l'intervention de l'autorité judiciaire au moment de l'identification des internautes à partir de leur adresse IP, absence qui serait néfaste à la protection du droit à la vie privée.
Or selon nous, cet argument est inopérant en tant que tel.
En effet, précisons, tout d'abord, que la commission de protection des droits sera exclusivement composée de trois membres en activité (35) au sein de la Cour de cassation, du Conseil d'État et de la Cour des comptes (36). Également, faut-il le rappeler, les décisions prises par l'HADOPI pourront en tout état de cause être contestées devant le juge administratif.
En outre, l'HADOPI est une autorité administrative indépendante au même titre que l'AMF et l'ARCEP, autorités dont le sérieux et la légitimité ne sont pas remis en cause aussi vivement.
En définitive, plutôt que d'axer le débat autour de questions posées de telle sorte qu'elles desservent la réelle nature du texte et décrédibilisent, par voie de dommages collatéraux, d'autres institutions comme les autorités administratives indépendantes, nous pensons qu'il est essentiel de replacer le débat autour de la lutte contre la contrefaçon commise sur le réseau internet, véritable enjeu pour la pérennité de la création en France.

Il est réellement souhaitable, selon nous, que le législateur intervienne dans le sens d'une protection réelle et définitive de l'adresse IP (...).

À noter enfin que le Parlement européen, à l'occasion des discussions relatives au « paquet télécoms » (37), a voté le 6 mai 2009 à une très large majorité un amendement indiquant qu'« *aucune restriction ne peut être imposée aux droits et libertés fondamentaux des utilisateurs finaux (d'internet) sans décision préalable des autorités judiciaires* ». Dès lors, le devenir du projet de loi « HADOPI » et son application en droit interne restent à ce jour encore très incertains.

CONCLUSION

L'évolution des modes de commission des actes de contrefaçon va de pair avec l'évolution des modes de consommation et d'accès à la culture. Par exemple, le système du *peer to peer* est déjà largement dépassé par les sites internet de *streaming* (consommation en flux continu sans téléchargement définitif de l'œuvre). Il paraît être d'un autre âge à l'échelle d'internet.
Désormais, la possession physique et définitive d'une œuvre n'est plus requise pour pouvoir en jouir. Le constat probatoire, tel qu'effectué par l'agent assermenté mandaté par la SACEM dans l'arrêt de la Cour de cassation du 13 janvier 2009, n'a probablement plus d'avenir.
Est-ce à dire pour autant que la problématique liée à la collecte d'adresses IP pour lutter contre la contrefaçon va disparaître ? Nous pouvons en douter si l'on combine, en effet, (i) le fait que le numérique a banalisé le principe même de la copie « clone », qu'elle soit licite ou illicite, (ii) qu'internet permet la diffusion de ces copies à grande échelle et (iii) que l'adresse IP reste, jusqu'à présent, la seule véritable donnée permettant de remonter de manière effective jusqu'au titulaire d'une connexion internet.
En conséquence, il est réellement souhaitable, selon nous, que le législateur intervienne dans le sens d'une protection réelle et définitive de l'adresse IP tout en assurant le respect des différents droits que sont la propriété intellectuelle, la protection juridictionnelle et effective de ces droits, et la protection du droit à la vie privée, comme l'a rappelé la CJCE (38).
Une solution pourrait consister en la création d'un régime spécial, applicable exclusivement à l'adresse IP sur le même modèle que les données sensibles de l'article 8 de la loi « Informatique et libertés », qui concilierait respect de la vie privée et droit de la propriété intellectuelle. ◆

(34) Objet du futur article L. 331-20 du Code de la propriété intellectuelle issu du projet de loi « HADOPI ». **(35)** Les membres sont nommés par décret pour un mandat de 6 ans qui est ni renouvelable ni révocable. **(36)** Objet du futur article L. 331-16 du Code de la propriété intellectuelle issu du projet de loi « HADOPI ». **(37)** Il s'agit d'un paquet législatif comportant plusieurs directives et règlement. **(38)** CJCE, 19 févr. 2009, aff. C-557-07, *LSG c/ Tele2 Telecommunication* ; CJCE, 29 janv. 2008, aff. C-275/06, *Promusicae c/ Telefónica de España*.