Tribunal de grande instance – Saint-Brieuc

6 septembre 2007

Ministère public, Scpp, Sacem / J. P.

Sources :

Références de publication :
- http://www.legalis.net/

La décision :

FAITS

Le 29 novembre 2004, Jean Yves Salaun, agent assermenté de la Sacem/Sdrm, ouvrait une session, via le réseau internet, sur le logiciel d'échange dit P2P (peer to peer), dénommé "Soulseek".

Il constatait qu'un internaute, sous le pseudonyme "La Plume", mettait à disposition du public, 147 318 fichiers essentiellement constitués d'œuvres musicales pour la plupart protégées par le droit d'auteur.

Le 14 décembre 2004, J. P. après avoir ouvert une session sur ce même logiciel constatait, après avoir lancé une recherche de fichiers d'enregistrements phonographiques de l'artiste Jean Jacques Goldman qu'un internaute, sous le pseudonyme "La Plume" proposait un fichier audio de cet artiste, et, après clic droit de souris pour ajouter ce pseudonyme dans la liste des utilisateurs, constatait qu'il était affiché que cet utilisateur mettait à disposition 149 632 fichiers.

Par ailleurs des consignes étaient données par cet internaute pour accéder au téléchargement des fichiers qu'il mettait à disposition, règles limitant à un CD ou 1 livre à la fois et autorisant 3 téléchargements de fichiers, ces limites ne s'appliquant pas à ses amis.

Le 16 décembre 2004, l'agent assermenté, lors d'une nouvelle session lançait l'application "Kerio personnel firewall" laquelle faisait apparaître l'adresse IP (Internet Protocole). A l'aide du logiciel Visuel Route, il établissait que cette adresse IP avait été attribuée par le fournisseur d'accès Wanadoo.france et que la connexion se faisait plus précisément par le bloc localisé à Rennes.

Le 25 février monsieur Anthony Sibton, agissant pour le compte de la Sacem/Sdrm, déposait plainte contre X auprès de la section de recherche de gendarmerie de Rennes, faisant valoir que selon ses constatations les 149 632 fichiers mis à disposition reproduisaient des œuvres protégées, et qu'il en résultait ainsi un préjudice important à la Sacem/Sdrm.

Les officiers de police judiciaires identifiaient auprès du fournisseur d'accès Wanadoo, centre de Rennes l'internaute disposant de cette adresse IP à savoir J. P.

Dans le cadre de l'enquête diligentée par la gendarmerie, il était saisi au domicile de J. P. deux ordinateurs et des DR-room gravés. Sur les disques durs, il était découvert l'existence de 22 547 fichiers musicaux au format MP3, 948 fichiers musicaux au format piste audio CD et 35 films au format Divx. Tous ces fichiers apparaissaient avoir été chargé par l'intermédiaire des logiciels de peer to peer Emule et Soulseek. En outre à la date des constations réalisées les options de partage de ces deux logiciels étaient actives pour les relations définies par J. P. soit une liste d'une trentaine de pseudonymes.

Lors de son audition J. P. ne contestait pas les constatations faites par l'agent de la Sacem ni celles faites par les enquêteurs. Il reconnaissait avoir téléchargé sur internet les fichiers puis les avoir partagés avec les deux logiciels Emule et Soulseek. Il précisait qu'il ne contestait pas le chiffre de 149 632 fichiers mais expliquait qu'il était redescendu, au moment de la perquisition, à 28 000 fichiers, la musique représentant 24 000 titres.

Il admettait que le logiciel Soulseek était ouvert en permanence et son partage accessible sauf aux personnes "qui viennent chercher et ne partagent pas".

Il précisait concernant les consignes apparaissant dans la fonction "Browse Files" qu'il avait trois connexions possibles pour les inconnus et cinq pour des amis, rencontrés sur le "chat" mais jamais physiquement.

A la suite de cette enquête J. P. était cité devant ce tribunal à la diligence du ministère public pour avoir représenté ou diffusé des œuvres en violation des droits des auteurs, infraction prévue et réprimée par les articles L 335-2 et L 335-3 du code de la propriété intellectuelle.

Il était également cité directement par la Scpp, société civile des producteurs phonographiques, du chef de mise à disposition du public de phonogrammes et de reproduction de phonogrammes réalisés sans l'autorisation de leurs producteurs légitimes et du délit de recel de fichiers musicaux illicites faits prévus et réprimés par les articles L 335-4 et L 335-6 du code de la propriété intellectuelle et 321-1 du code pénal.

Sur l'exception de nullité du procès verbal de l'agent assermenté de la Sacem au regard des dispositions de la loi du 6 janvier 1978 dite "informatique et libertés"

J. P. soutient que le procès verbal établi par l'agent assermenté est nul car celui-ci, pour l'établir, a procédé à un traitement illicite de données à caractère personnel relatives à des infractions sans obtenir l'autorisation de la Cnil.

Il fait valoir que l'adresse IP est une donnée à caractère personnel au sens de l'article 2 de la loi susvisée car elle identifie un ordinateur précis et indirectement son utilisateur, comme un numéro de téléphone ou une adresse électronique.

Il fait valoir, en second lieu, que pour obtenir cette adresse IP l'agent assermenté a effectué plusieurs traitements automatiques.

Le traitement peut consister, selon la loi, dans le simple ciblage ou la simple sélection d'une donnée personnelle, même sans enregistrement.

En l'espèce, l'agent a extrait les données de connexion à l'aide d'un logiciel espion "Kerio Personnal Firewall" et les a traitées pour obtenir l'adresse du fournisseur d'accès. Ces données ont été ensuite organisées et consignées dans un procès verbal informatique lequel est conservé dans un fichier informatique avec les autres procès verbaux similaires. Il y a bien un traitement automatisé s'agissant de l'utilisation d'un programme informatique.

En troisième lieu et à titre subsidiaire, J. P., soutient, à supposer que les traitements en question ne soient pas considérés comme des traitements automatisés de donnés à caractère personnel, que les données personnelles recueillies par la Sacem concernent en réalité quelques 200 internautes qu'elle a décidé de poursuivre. Il n'est pas douteux que ces informations nominatives ont été collectées par des agents assermentés et collectés dans des fichiers structurés au sens de l'article 2 de la loi "informatique et libertés".

J. P. estime donc que les données recueillies sur lui par l'agent assermenté relèvent de cette loi.

Il expose qu'aux termes de l'article 4-9 les traitements de données à caractère personnel relatives aux infractions ne peuvent être mises en œuvres notamment que par les personnes morales mentionnées aux articles L 321-1 et L 331-1 du code de la propriété intellectuelle agissant aux titres des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus par le code aux fins d'assurer la défense de ces droits.

Aux termes de l'article 25 de cette même loi des traitements automatisés ou non portant sur des données relatives aux infractions, condamnations ou mesures de sûreté ne peuvent être mis en oeuvre qu'après autorisation de la Cnil sauf ceux qui sont mis en oeuvre par les auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées.

En l'espèce, affirme J. P. l'agent assermenté de la Sacem/Sdrm ne peut exciper d'aucune autorisation de la Cnil pour les traitements auxquels il a procédé.

Il souligne en outre que de tels agissements tombent sous le coup de la loi pénale.

J. P. estime que le procès verbal dressé par Jean Yves Salaun est entaché de nullité car il y a eu, s'agissant du non respect d'une obligation visant à assurer la protection d'une liberté fondamentale et en conséquence ne peut que lui faire grief au sens de l'article 802 du code de procédure pénale.

J. P. soutient que cette nullité entraîne nécessairement la nullité des actes subséquents à savoir la procédure établie par les officiers de police judiciaire car ceux-ci se sont contentés de rechercher auprès du fournisseur d'accès le titulaire de l'adresse IP qui avait été relevée par l'agent assermenté. Ils n'ont fait aucune recherche indépendante supplémentaire.

Les parties civiles contestent cette argumentation.

Elles font valoir que les agents assermentés tiennent leur compétence de la loi en application de l'article L 331-2 du code de la propriété intellectuelle.

Ce n'est pas la Sacem/Sdrm qui a fait le constat mais un agent assermenté qui n'avait nulle obligation d'obtenir au préalable l'autorisation de la Cnil.

Par cette assermentation l'agent a rang d'officier public et de plus un texte de loi contenu dans un code spécifique n'a pas à être conditionné par l'agrément d'une autorité administrative elle-même crée par la loi et relevant d'un domaine distinct.

Elles soutiennent encore que le constat n'est pas une base de données et qu'il ne traite rien, c'est seulement une preuve pénale.

Elles font valoir que les constatations de l'agent assermenté ne constitue nullement un traitement automatisé de données à caractère personnel au sens de l'article 2 de la loi du 6 juillet 1978.

En effet, il convient de ne pas confondre collecte automatisée d'adresses IP et la collecte ponctuelle d'une telle donnée. En l'espèce, l'agent n'a fait que ce que tout internaute peut faire à savoir se connecter sur un logiciel de "peer to peer", lancer une requête sur un nom d'artiste, visualiser les résultats, sélectionner un des pseudonymes d'internaute mettant les oeuvres à disposition, faire des constatations sur le nombre de dossiers de partage proposés par cet internaute, lire dans l'application "Kerio personnal firewall" l'adresse IP de l'ordinateur correspondant à ce pseudonyme avec lequel il se trouvait connecté puis à l'aide du logiciel "Visual Route" constater que le fournisseur d'accès en l'espèce était Wanadoo.

La collecte de l'adresse IP ne résulte nullement d'un processus automatisé mais a bien nécessité une intervention humaine. Il s'agit d'une collecte ponctuelle effectuée par un agent assermenté et non d'une collecte automatisée effectuée par une machine. Le matériel informatique n'a été utilisé que pour retranscrire les informations recueillies sur internet pour les besoins de ses constatations.

Les parties civiles soulignent que l'adresse IP a été obtenue non avec un logiciel spécifique destiné à la collecte automatisée de telles adresses mais au moyen d'un logiciel pare-feu qui a pour objet de protéger un ordinateur contre des intrusions extérieures.

Ce qui tombe sous le coup de la loi c'est le caractère automatisé du traitement, non le caractère automatisé du procédé qui permet de commettre des infractions, en l'espèce le logiciel "peer to peer", contrairement à ce que soutient la Cnil qui considère que l'utilisation d'un tel logiciel en tant que telle pour procéder aux fins de constatation d'une infraction constitue un traitement automatisé de données à caractère personnel.

Les parties civiles soutiennent enfin qu'il ne peut être reproché à l'agent d'avoir procédé à un traitement automatisé de données à caractère personnel destinées à figurer dans un fichier au sens de la loi "informatique et libertés".

En aucun cas les "prétendus" dossiers correspondant aux affaires de piraterie dans lesquelles la Sacem intervient ne constituent un ensemble structuré et stable de telles données accessibles selon des critères déterminés.

DISCUSSION

La loi du 6 janvier 1978 dans sa rédaction applicable à l'espèce dispose en son article 2 al. 1 qu'elle s'applique aux traitements automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles.

L'alinéa 2 du même article dispose que 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. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peuvent avoir accès le responsable du traitement ou toute autre personne.

En l'espèce, il apparaît que J. P. a été identifié, et donc son nom révélé grâce à l'adresse IP et au nom du fournisseur d'accès (FAI), toutes informations recueillies par l'agent assermenté lors de ses sessions sur internet.

Certes ce sont les enquêterus de la section de recherche de la gendarmerie, officers de police judiciaire, qui ont requis Wanadoo, le fournisseur d'accès, de leur donner l'identité de l'utilisateur de l'adresse IP que leur avait fourni le procès verbal de l'agent assermenté.

L'adresse IP, est, au sens strict, un identifiant d'une machine lorsque celle-ci se connecte sur l'internet et non d'une personne. Mais au même titre qu'un numéro de téléphone n'est, au sens strict, que celui d'une ligne déterminée mais pour laquelle un abonnement a été souscrit par une personne déterminée, un numéro IP associé à un fournisseur d'accès correspond nécessairement à la connexion d'un ordinateur pour lequel une personne déterminée a souscrit un abonnement auprès de ce fournisseur d'accès. L'adresse IP de la connexion associée au fournisseur d'accès constituent un ensemble de moyens permettant de connaître le nom de l'utilisateur.

En l'espèce, il n'est pas contestable que les informations recueillies par l'agent assermenté, Jean Yves Salaun, à savoir l'adresse IP de la connexion du 16 décembre 2004 de l'internaute utilisant le pseudonyme "La Plume", puis le nom du fournisseur ayant attribué cette adresse à savoir wanadoo.france et plus précisément le bloc situé à Rennes constituaient des données à caractère personnel ayant indirectement permis l'identification de J. P. par les officiers de police judiciaire qui n'ont eu qu'à contacter le fournisseur d'accès wanadoo pour avoir son identité.

L'article 2 sus-visé dispose encore que constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant que 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 tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Il apparaît que l'agent assermenté, pour obtenir les éléments permettant d'identifier l'internaute proposant des fichiers à l'échange sous le pseudonyme "La Plume" a eu recours à deux logiciels spécifiques qui seuls lui ont permis d'obtenir et l'adresse IP de l'ordinateur connecté lors de sa navigation sur "Soulseek" à savoir le pare feu "Kerion personnel Firewall" et le logiciel "Visuel Route".

L'obtention de ces informations a donc nécessité aux moins deux opérations spécifiques pour collecter et extraire des données électroniques celles correspondantes à ces informations et pour les consulter.

Ce n'est pas le seul fait de l'utilisation du logiciel "Soulseek" qui constitue un traitement de données à caractère personnel mais cette utilisation associée à des logiciels permettant d'obtenir les données nominatives à caractère personnel associées aux internautes proposant des fichiers de partage sur ce logiciel de "peer to peer".

La loi n'impose aucune caractéristique particulière autre à la nature des traitements qu'elle spécifie. Dès lors le fait que des outils, tels ceux utilisés par l'agent assermenté, soient en ligne sur le réseau à disposition de n'importe quel internaute ne saurait avoir pour effet de faire perdre aux opérations qu'ils permettent le caractère de "traitement" au sens de l'article 2 sus-visé.

Il doit être constaté que la loi ne définit pas ce qu'elle entend par "automatisé". Il peut toutefois être considéré, s'agissant d'une loi relative à l'informatique, qu'est visé par ce terme un processus informatique qui par nature est constitué d'une suite d'actions de nature électronique enchaînant les uns les autres sans intervention manuelle conduisant à un résultat. Un programme informatique qui comporte une suite d'instructions s'exécutant par enchaînements successifs jusqu'au terme prévu est un processus automatisé.

Il est soutenu par les parties civiles qu'il y aurait lieu de distinguer entre procédé et traitement et que seul peut être qualifié d'automatisé un traitement informatique de données nominatives à caractère personnel à savoir l'utilisation d'un programme informatique permettant d'effectuer sans intervention humaine et donc de manière automatique l'une des opérations visées à l'article 2. Par contre ne serait pas un traitement "automatisé", le fait d'utiliser l'outil informatique pour recueillir l'adresse IP dès lors que ce recueil est effectué par l'utilisation des fonctionnalités à disposition de l'internaute dans le cadre d'une session sur le réseau internet ce qui suppose l'intervention, à chaque étape, de celui-ci : ouverture de la session, connexion au réseau puis au logiciel de partage, activation des fonctionnalités de celui-ci, puis de celles du pare-feu, lancement du logiciel "Visual Route" et au final transcription dans le procès verbal des informations ainsi obtenues.

Une telle interprétation ne peut être retenue. D'une part tout programme informatique suppose néanmoins, à un moment ou à un autre l'intervention humaine (démarrage par exemple). D'autre part le texte de l'article 2 lui-même à propos des "opérations" précise : "quelque soit le procédé utilisé". C'est donc qu'elle inclut la notion de procédé dans celle de traitement.

Doit donc être qualifié "d'automatique" l'utilisation d'un programme informatique permettant l'une des opérations telles que définies à l'alinéa 3 de l'article 2 de la loi du 6 janvier 1978.

Tel est bien le cas en l'espèce concernant le recueil des données à caractère personnel concernant J. P. par l'agent assermenté Jean Yves Salaun.

Il apparaît donc que ces opérations entrent dans le champ d'application de la loi sus-visée.

L'article 9 de la loi du 6 janvier 1978 tel que modifié par la loi du 6 août 2004 dispose que les traitements de données à caractère personnel relatives aux infractions , condamnations et mesures de sûreté ne peuvent être mis en œuvre que par :

1° les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;

2° les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leurs sont confiées par la loi ;

3° 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 II et III du même code aux fins d'assurer la défense de ces droits.

Il résulte de ces dispositions que les personnes morales telle la Sacem ou la Scpp peuvent donc procéder à des traitements, automatisés ou non, de données à caractère personnel dans le cadre de la recherche d'infractions telles que celles visées à la présente procédure.

Toutefois, cette mise en œuvre ne peut intervenir que dans le respect des formalités prévues à cette fin par les dispositions du chapitre IV intitulé : "Formalités préalables à la mise en œuvre des traitements".

L'article 25 de la loi dispose que sont mis en oeuvre après autorisation de la CNIL, à l'exclusion de ceux mentionnés aux articles 26 et 27 :
...

3° les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûretés, sauf ceux qui sont mis en oeuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées.

En l'espèce, il n'est pas contestable que les traitements automatisés effectués par l'agent assermenté de la Sacem portaient sur des données à caractère personnel relatives à des infractions au code de la propriété intellectuelle.

Si aux termes de l'article L331-2 du code de la propriété intellectuelle la preuve de la matérialité des infractions aux dispositions des livres Ier, II et III, peut résulter des constatations d'agents assermentés désignés selon les cas ... par les organismes professionnels d'auteurs et par les sociétés mentionnées au titre II du présent livre, il n'apparaît pas qu'un tel agent assermenté puisse être considéré comme un auxiliaire de justice au sens de l'article 25 précité de la loi informatique et libertés.

En effet, le terme d'auxiliaire de justice désigne les membres de professions, le cas échéant réglementées, qui concourent à l'administration de la justice où interviennent dans les procédures au soutien ou en représentation, d'une partie ainsi qu'il résulte notamment des dispositions de l'article 25 de la loi du 10 juillet 1991 aux termes desquelles sont considérés comme des auxiliaires de justice les avocats et les officiers publics et ministériels.

Les experts sont également considérés, à raison du concours qu'ils apportent à l'œuvre de justice, comme des auxiliaires de justice.

L'auxiliaire de justice intervient au soutien d'une partie, effectue des actes de procédure au profit d'une partie ou encore apporte son concours à l'office du juge.

Il en résulte notamment que le juge exerce un contrôle sur la rémunération des auxiliaires de justice.

Un agent ou un officier de police judiciaire ne saurait être qualifié d'auxiliaire de justice car son activité ne rentre dans aucune de celles-ci dessus définies.

Le pouvoir de constatation des infractions que l'agent assermenté tient des dispositions de l'article L331-2 sus-visé du code de la propriété intellectuelle l'assimile sur ce point à un agent ou un officier de police judiciaire. Il ne peut donc être qualifié d'auxiliaire de justice.

Dès lors, il ne peut être excipé de cette qualité pour l'agent assermenté aux fins d'échapper à la condition d'autorisation préalable de la CNIL pour mettre en oeuvre les traitements automatisés de données à caractère personnel auxquels il a procédé en l'espèce pour établir son procès-verbal.

Il ne peut être non plus soutenu les dispositions de l'article L 331-2, antérieures à la loi du 6 janvier 1978 constitueraient les dispositions spéciales auxquelles les dispositions générales de celles-ci ne pourraient déroger.

En effet, il ne s'agit aucunement de dispositions traitant de la même matière mais de dispositions sans lien les unes avec les autres puisque le premier texte ne vise qu'à permettre de dresser procès verbal, celui-ci devant par ailleurs, comme tout procès verbal, respecter les dispositions légales susceptibles de s'appliquer aux moyens utilisés pour le constat et aux conditions de son établissement, alors que le second vise à définir les conditions dans lesquelles peuvent intervenir, notamment le traitement de données à caractère personnel. Si tel était le cas il en résulterait que l'agent assermenté, dès lors qu'il se contente de dresser un procès verbal pourrait à cette fin avoir recours à un traitement quel qu'il soit de données à caractère personnel.

Aux termes de l'article 802 du code de procédure pénale en cas de violation des formes prescrites par la loi à peine de nullité ou d'inobservation des formalités substantielles la nullité ne peut être prononcée que si elle a eu pour effet de porter atteinte aux intérêts de la partie qu'elle concerne.

En l'espèce il est établi que l'agent assermenté a procédé, pour dresser son procès verbal, à des traitements automatisés de données à caractère personnel sans qu'une autorisation préalable de la Cnil ait été obtenue.

Cette autorisation, dans le domaine aussi sensible de la protection des droits et libertés individuelles au regard de la puissance de l'outil informatique, est à l'évidence une garantie expressément voulue par le législateur pour assurer une protection effective de ces droits.

Le fait que n'ait pas été respectée cette formalité constitue donc nécessairement une atteinte aux intérêts de J. P., partie poursuivie.

II y a donc lieu de prononcer la nullité du procès-verbal de constat dressé le 17 décembre 2004 par l'agent assermenté de la Sacem Jean Yves Salaun.

Du fait même de cette nullité le procès verbal ne peut dès lors être produit comme simple élément de preuve obtenu irrégulièrement au titre de la liberté de preuve telle que prévue à l'article 427 du code de procédure pénale .

En outre, cette nullité entraîne la nullité de la totalité de la procédure subséquente dans la mesure où le procès verbal de l'agent assermenté apparaît comme le soutien nécessaire de la procédure diligenté par la section de recherche de Rennes de la gendarmerie et des actes de poursuites diligentés par le ministère public et par la Scpp.

En effet, les investigations diligentés par les officiers de police judiciaire n'ont eu pour effet d'une part que d'obtenir du fournisseur d'accès le nom de l'utilisateur sur la base des constatations contenues dans le procès verbal de l'agent assermenté et d'autre part de procéder ensuite à son interpellation, à une perquisition à son domicile et à son audition portant sur les constatations faites par l'agent assermenté.

La procédure d'enquête est donc atteinte de nullité dans son ensemble et par voie de conséquence les actes de poursuites fondés sur cette procédure sont nuls, à savoir ceux du Ministère Public et de la partie civile, le Scpp dans le cadre de sa citation directe. Dès lors il y a lieu de constater la nullité de l'ensemble de la procédure et de renvoyer J. P. des fins des poursuites.

Sur l'action civile

En raison de la nullité encourue de l'ensemble de la procédure les constitutions de parties civiles de la Sacem et de la Scpp ne peuvent qu'être rejetées.

DECISION

Statuant publiquement et en premier ressort, contradictoirement à l'égard de J. P. ;

Sur l'action publique

. Prononce la nullité de l'ensemble de la procédure et en conséquence revoie J. P. des fins de la poursuite ;

Sur l'action civile

. Déclare les constitutions de parties civiles de la Scpp et de la Sacem irrecevables ;

Le tout en application des articles 406 et suivants et 485 du code de procédure pénale et des textes susvisés.