



# Concurrences

Revue des droits de la concurrence

Saisies informatiques : Le régime français à l'épreuve des impératifs de conformité et de cohérence

**Doctrines** | *Concurrences* N° 2-2009 – pp. 69-77

---

**Nathalie JALABERT-DOURY**

[jalabert-doury@cbr-law.com](mailto:jalabert-doury@cbr-law.com)

■ Avocat à la Cour, Paris



eux-mêmes ou les principes fondamentaux. Ce contentieux est peu fourni et largement confidentiel : il s'exerçait jusqu'à présent devant des Juges des libertés dont les ordonnances ne sont pas publiées, dans des délais stricts, avec une possibilité de pourvoi devant la Cour de cassation rarement mise en œuvre<sup>6</sup>.

7. Or, les pratiques des deux "corps" concernés sont pour l'heure assez différentes par nature. L'Autorité de concurrence est membre d'un Réseau européen de la concurrence, elle s'attache depuis de nombreuses années à faire œuvre de transparence et elle a amélioré à bien des égards les droits de la défense dans ses procédures. Les Rapporteurs qui exerceront désormais les pouvoirs d'enquête sont par ailleurs en charge de l'instruction complète du dossier, de l'enquête jusqu'à la séance en passant par l'accès au dossier et le débat contradictoire, ce qui est susceptible de modifier leur perspective sur les modalités ou les pratiques d'enquête tenables dans les suites de la procédure.

8. Certaines de ces différences de méthode sont bien connues. Ainsi, dans le cadre des auditions, les enquêteurs de la DNE ont pour pratique quasi-systématique de ne pas faire figurer les questions qu'ils posent dans les procès-verbaux, alors que la très grande majorité des Rapporteurs de l'Autorité les fait aujourd'hui apparaître.

9. D'autres différences ne seront perceptibles qu'au fur et à mesure du développement de l'expérience de l'Autorité sur ces sujets, mais elles pourraient bien s'avérer significatives sur des sujets où la jurisprudence française est encore en friche et où la pratique française est pour l'heure particulièrement éloignée de la pratique de nos voisins ainsi que de la Commission européenne.

10. Parmi ces sujets d'évolution possible, et selon nous souhaitable, figurent indéniablement les saisies informatiques. En la matière, la pratique française actuelle soulève de réels problèmes de conformité et elle a pour l'heure donné lieu à des jurisprudences difficilement conciliables de la part des Juges des libertés qui ont été saisis du sujet, tandis que le seul arrêt de Cour de cassation sur le sujet apporte assez peu d'enseignements<sup>7</sup>. Or, il apparaît que d'autres autorités de concurrence mettent en œuvre des modalités de saisies bien plus protectrices des droits des entreprises, et que la procédure pénale elle-même offre des mécanismes comparables.

## I. Le cadre juridique dans lequel s'opèrent les saisies informatiques est particulièrement pauvre

11. Les saisies informatiques posent des problématiques démultipliées par rapport aux saisies "papier" : chaque document papier saisi suppose une sélection, la numérotation de la pièce, la réalisation d'une photocopie pour l'entreprise et enfin une mention sur le bordereau de pièce saisie (numérotation, descriptif, nombre de pages), chacune de ces

opérations prenant un temps qui invite les enquêteurs à se concentrer sur le champ de l'enquête tel que défini par l'autorisation judiciaire obtenue au préalable, et sur l'essentiel.

12. Au contraire, les saisies informatiques permettent en quelques clics de procéder à la copie de masses de données, de dupliquer celles-ci pour l'entreprise, et d'éditer de manière automatique un inventaire des fichiers. Les données ainsi copiées peuvent être à plusieurs niveaux suivant le procédé utilisé : ainsi une copie simple de fichier permet déjà d'accéder aux métadonnées (sous Word : auteur du document, date de création et modification du document, versions antérieures etc.) ; une image numérique (copie bit à bit intégrale) permet non seulement de copier les fichiers apparents mais aussi l'ensemble des informations non apparentes stockées sur le support, notamment en vue d'une éventuelle récupération de fichiers effacés.

13. Des copies qui ne seraient pas suffisamment ciblées portent évidemment le risque de couvrir des éléments insaisissables tels que des documents hors champ d'enquête, couverts par le privilège avocat-client ou encore relevant de la vie privée. Ce risque est ici bien plus grand que s'agissant des saisies papier : on classe rarement dans un dossier client ses e-mails personnels, des échanges sensibles entre dirigeants, ou encore les échanges avec son conseil juridique. Dans une messagerie électronique, des éléments de nature très diverse sont au contraire mélangés.

14. Dans un tel contexte, on aurait pu imaginer que le législateur prenne les précautions qui s'imposaient. Or, les textes ont prévu la possibilité de saisies informatiques dans des termes à ce point flous qu'il a fallu l'intervention des juridictions pour établir que le cadre légal des saisies informatiques était au même niveau que celui des saisies papier. On sait par ailleurs que les recours *ex post* ne permettent pas de remédier adéquatement à une saisie injustifiée.

## 1. L'intervention des juridictions a été nécessaire pour que le cadre légal des saisies informatiques soit au même niveau que celui des saisies papier

15. L'article L. 450-4 du Code de commerce habilite les agents des services d'instruction de l'Autorité à procéder à des visites et saisies sur autorisation préalable du Juge des libertés et de la détention du lieu où la visite est effectuée. Ils peuvent à cette occasion saisir des documents et, depuis la loi NRE n° 2001-420 du 15 mai 2001 "tout support d'information".

16. Les termes "tout support d'information" pouvant *a priori* viser non seulement un CD ou DVD-Rom mais aussi le disque dur lui-même<sup>8</sup>, on s'est un temps interrogé sur l'applicabilité des garanties apportées par la jurisprudence s'agissant des documents papier : limitation de l'autorisation de saisie aux documents entrant dans le champ de l'enquête, insaisissabilité des documents couverts par le secret professionnel, etc.

6 Selon nos calculs, aucune ordonnance n'a été cassée depuis plus de 10 ans sur un moyen soulevé par l'entreprise concernée.

7 Crim, 12 sept. 2007, pourvoi n°06-81.907, *Sita* ; voir également Crim, 14 nov. 2007, pourvoi n°05-85.739, *Groupe Canal Plus*.

8 Sur la distinction support d'informations/document, voir Crim, 14 nov. 2007, pourvoi n°05-85.739, *Groupe Canal Plus*.

17. La jurisprudence est rapidement venue confirmer que ces garanties s'appliquaient de la même manière aux saisies informatiques<sup>9</sup>. Le contraire eût en effet été difficilement concevable dès lors que certains de ces motifs d'insaisissabilité ressortent non seulement des droits fondamentaux<sup>10</sup> et le cas échéant même de la Convention européenne des droits de l'homme : quel que soit le flou des termes employés par le législateur, la loi ne saurait en toute hypothèse y déroger.

18. L'article L. 450-4 prévoit également que "*les inventaires et mises sous scellés sont réalisés conformément à l'article 56 du Code de procédure pénale*", lequel indique que "*tous objets et documents saisis sont immédiatement inventoriés et placés sous scellés [...]. 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*".

19. Plus précisément, les saisies réalisées sur la base de l'article L. 450-4 sont pratiquées sous la forme de scellés dits "ouverts". En substance, les documents papier sont percés puis reliés par une ficelle maintenue par un lien cacheté à la cire. Ce processus a pour objet de garantir l'intégrité des pièces saisies tout en permettant leur consultation.

20. Ce processus a simplement été adapté pour les données informatiques : elles sont copiées sur un ou plusieurs DVD-Rom non réinscriptibles, et jusqu'à présent, une ou deux copies complémentaires étaient faites (pour la DGCCRF, pour l'entreprise et le cas échéant pour le Conseil).

## 2. Les recours *ex post* ne constituent pas un remède adapté en cas de saisie non conforme

21. En cas de contestation de l'entreprise sur le champ d'une saisie informatique, elle peut éventuellement solliciter les officiers de police judiciaire qui accompagnent les agents, garants des droits de la défense auxquels l'article 56 de Code de procédure pénale fait "*obligation de provoquer préalablement [à la saisie] toutes mesures utiles pour que soit assuré le respect du secret professionnel et des droits de la défense*". Ceux-ci peuvent le cas échéant se retourner vers le Juge des libertés dès lors que "*la visite et la saisie s'effectuent sous l'autorité et le contrôle*" du juge.

22. Reste que cette faculté demeure largement théorique en pratique, soit parce que le juge ne peut être contacté par les officiers de police judiciaire, soit parce que celui-ci aura quelque peine à trancher une contestation technique alors qu'il n'est pas présent sur les lieux et qu'il n'aura pas matériellement la capacité de s'y rendre. Jusqu'à présent, il renvoyait donc les parties à la possibilité de le saisir à l'issue de la visite.

23. Depuis la LME, la visite s'effectue toujours sous l'autorité et le contrôle du Juge des libertés, qui conserve la faculté de décider à tout moment la suspension ou l'arrêt de celle-ci. En revanche, sa compétence prend fin avec la clôture des opérations, le texte prévoyant désormais que "*le déroulement des opérations de visite ou saisie peut faire l'objet d'un recours devant le premier président de la Cour d'appel*". Il serait logique qu'un premier degré de juridiction existe effectivement avant que le Premier Président de la Cour d'appel ne soit amené à se prononcer. Ceci milite donc encore plus que par le passé pour une intervention du Juge des libertés en cours de visite, ce qui supposerait de lever les difficultés pratiques rencontrées jusqu'à présent.

24. À défaut d'une intervention du Juge des libertés pendant la visite, l'entreprise pourra exercer un recours devant le Premier Président de la Cour d'appel (désormais par déclaration au greffe dans un délai maximal de quinze jours). Du temps où le recours en contestation des pièces saisies s'effectuait devant le Juge des libertés ayant autorisé les visites, ce recours prenait au total de l'ordre de 6 à 8 mois (sans compter un éventuel pourvoi en cassation), pendant lesquels les scellés demeuraient physiquement entre les mains de la DGCCRF. Les durées de recours devant le Premier Président de la Cour d'appel seront vraisemblablement de même ordre.

25. Or, ce recours suppose que l'entreprise identifie les documents hors champ et/ou couverts par le privilège avocat/client afin d'établir qu'elle a fait l'objet de saisies illicites. En somme, le recours lui impose d'effectuer le travail de sélection de la DNE et de mettre en avant, dans le cadre d'un débat contradictoire avec cette dernière, les éléments dont la confidentialité aurait dû demeurer inviolée. Peu d'entreprises parvenant à s'y résoudre, elles contestent avant tout les principes, d'où l'accueil assez réservé de la majorité des Juges des libertés sur le sujet, mais elles ne disposent pas d'autre choix. Ceci démontre que le recours disponible est par nature totalement inapproprié s'agissant d'assurer le respect de ces garanties.

26. *In fine*, l'entreprise pourra le cas échéant obtenir restitution des seules pièces concernées. Elles ne pourront par la suite être utilisées à titre de preuve dans la procédure, mais elles seront restées pendant plusieurs mois entre les mains des services d'enquête, qui auront pu les exploiter, et tel est d'ailleurs le plus souvent le cas en pratique : reporter l'exploitation des données jusqu'à l'expiration des voies de recours retarderait la procédure de plusieurs mois, voire de plusieurs années.

<sup>9</sup> C'est à notre sens l'un des seuls enseignements qui peuvent être tirés de l'arrêt Crim, 12 sept. 2007, pourvoi n° 06-81.907, *Sita*.

<sup>10</sup> Qu'ils soient français, communautaires, ou plus largement partagés par la majorité des systèmes juridiques : voir à cet égard ICN, *Anticartel Enforcement Manual*, Chapter 3 Digital Evidence Gathering, April 2006.

## II. Les pratiques de saisie développées en France ne permettent pas d'assurer le respect des garanties applicables

27. Dans ce cadre déjà fragile, la pratique française pour l'heure est de procéder à des saisies informatiques nombreuses dès l'arrivée des agents sur les lieux<sup>11</sup>. Les bureaux des personnes les plus directement concernées par l'enquête sont en effet ciblés à l'arrivée des enquêteurs et les ordinateurs y sont contrôlés en priorité par les enquêteurs.

28. La méthode généralement employée consiste à procéder à une recherche (en principe par mots-clés avec les moteurs de recherche internes ou un moteur de recherche externe présent sur un ordinateur portable de la DNE) afin de déterminer si des documents entrant dans le champ de l'enquête se trouvent sur le disque dur de l'ordinateur ou sont accessibles par le réseau.

29. Lorsque tel est le cas, l'agent acte sur le procès-verbal avoir "pu constater la présence de documents entrant dans le champ de l'autorisation de visite et saisie", sans plus de précision. L'agent procède alors à la copie de tout ou partie du disque dur, y inclus des masses de fichiers n'ayant strictement aucun rapport avec l'enquête – à tel point que l'on y trouve des notes d'utilisation de Word et d'Acrobat Reader, des notes ayant trait à la vie privée, etc. – et le cas échéant des fichiers couverts par le secret des correspondances avocat/client. En cas d'organisation des documents au sein d'une arborescence de répertoires et sous-répertoires, ceux-ci sont parfois saisis intégralement.

30. S'agissant de la messagerie électronique, la méthode est encore plus expéditive et globale. Une messagerie électronique se présente en effet sous la forme d'un fichier unique ".nsf" (Lotus Notes) ou ".pst" (Microsoft Outlook) pour les deux systèmes les plus courants. Ce fichier unique regroupe l'ensemble des informations contenues dans la messagerie, à l'image d'un fichier d'archivage ou de compression. Au sein de ce fichier unique, au sens technique, figurent un grand nombre de documents distincts au sens juridique.

31. Sur cette base, les agents vérifient au préalable que la messagerie contient bien des éléments relatifs à l'enquête autorisée selon les mêmes méthodes, ils apposent sur le procès-verbal la mention qu'ils ont procédé à cette vérification, et ils saisissent l'intégralité de la messagerie.

32. Pour des données autres que celles issues des messageries, l'inventaire est généré automatiquement et permet de fournir le chemin du fichier, sa date de création, ainsi que son volume. S'agissant des messageries, l'inventaire est réalisé très simplement en recopiant le chemin du fichier de la messagerie. L'inventaire correspondant à plusieurs milliers de pages tient dès lors en une ligne.

<sup>11</sup> Voir sur l'ensemble du sujet, et en particulier sur les modalités mises en œuvre, A. Marie, "Les enquêtes de la DGCCRF en matière de pratiques anticoncurrentielles", *Revue Lamy de la Concurrence*, janvier/mars 2008, n° 14, p. 112 et s.

## 1. Les principes d'intégralité et d'insécabilité des saisies informatiques développées par l'administration ne sont guère convaincants

33. Ainsi que le reconnaissait ouvertement le directeur de la DNE dans un article récent "un certain nombre de fichiers peuvent être saisis compte tenu du principe de l'intégralité et de l'insécabilité des documents saisis. Bien sûr il peut s'agir de documents qui n'entrent pas dans le champ de l'enquête, de messageries personnelles ou de correspondances d'avocat mais, lorsque c'est le cas, l'administration est disposée à les restituer après que l'entreprise en ait fait la demande auprès du JLD et sous le contrôle de ce dernier"<sup>12</sup>. Toutes les entreprises qui ont été confrontées à de telles saisies en masse ont pu faire ce constat.

34. Nous ne pensons pas que des arguments techniques ou d'opportunité seraient à même de justifier des saisies de documents insaisissables<sup>13</sup>. Ainsi que nous le verrons ci-après, des modalités pratiques très simples peuvent être mises en œuvre pour protéger ces documents sans entraver l'enquête (voir point 3 ci-après).

35. En toute hypothèse, les arguments présentés par la DGCCRF pour justifier les principes d'intégralité et d'insécabilité en cas de recours ne nous semblent pas pertinents.

36. La DGCCRF considère d'abord qu'une messagerie électronique ou qu'un répertoire de l'arborescence constitue un seul et même document au sens juridique, cette notion s'entendant "généralement de tout support qui sert de preuve ou de renseignement" et qu'ils sont habilités à le saisir dans son intégralité dès lors que ce document est "pour partie utile" à l'enquête, selon la formule consacrée de la Cour de cassation<sup>14</sup> s'agissant des documents papier mixtes (agendas ou cahiers de notes contenant à la fois des éléments dans le champ et hors champ d'autorisation).

37. Il est exact qu'en règle générale, la messagerie électronique apparaît sous une ligne unique de fichier. Tel est notamment le cas des deux systèmes les plus couramment utilisés. Mais il ne faut pas confondre fichier au sens technique et document au sens juridique. Un fichier unique, comme une armoire d'archivage, peut contenir une multiplicité de documents. Or, il ne viendrait à personne l'idée d'affirmer que l'existence d'une armoire permet de saisir l'intégralité de son contenu sans avoir à isoler au préalable les seuls documents saisissables entrant dans le champ de l'enquête. Il en va a fortiori de même s'agissant des répertoires qui contiennent plusieurs fichiers distincts.

<sup>12</sup> J.-M. Marcellesi, "Dans une affaire récente, 98 000 fichiers informatiques ont dû être exploités", *Revue Lamy de la Concurrence*, janv./mars 2008, n° 14, p. 129 et s.

<sup>13</sup> En ce sens, TGI Nanterre, JLD, Ordonnance du 20 mars 2007, *Beiersdorf e.a.*

<sup>14</sup> Com, 12 nov. 1996, pourvois n° 94-13.944 e.a.

38. Certaines ordonnances de Juges des libertés ont pourtant validé un tel raisonnement<sup>15</sup>. La Cour de cassation a elle-même été saisie d'un cas où l'administration avait soutenu l'applicabilité à une messagerie électronique de cette jurisprudence des documents "pour partie utiles". Le rejet du moyen nous semble cependant relever plus clairement d'un renvoi au pouvoir souverain du Juge des libertés que d'une validation du principe d'insécabilité<sup>16</sup> : "si l'administration ne peut appréhender que des documents se rapportant aux agissements retenus par l'ordonnance d'autorisation de visite et saisie, il ne lui est pas interdit de saisir des pièces pour partie utiles à la preuve desdits agissements ; qu'en l'espèce le juge, qui a souverainement estimé que ces pièces n'étaient pas étrangères au but de l'autorisation accordée, a justifié sa décision"<sup>17</sup>. La Cour de cassation a d'ailleurs utilisé le terme « documents » et non « support d'informations ».

39. S'agissant des messageries, il a encore été avancé que la saisie de la messagerie dans son ensemble s'imposerait parce qu'elle serait insécable, la copie des seuls e-mails entrant dans le champ de l'enquête étant impossible. Cet argument a également été entendu par un certain nombre de Juges des libertés<sup>18</sup>.

40. Pourtant, il apparaît que le système Microsoft Outlook offre une sécabilité instantanée : un e-mail peut être copié en ouvrant la messagerie, en le sélectionnant et en le déplaçant vers le fichier de destination. Sous Lotus Notes, l'opération est à peine plus compliquée : la copie doit s'effectuer à destination d'une nouvelle messagerie Lotus Notes qui se crée en quelques clics. Une autre méthode consiste à convertir la messagerie Lotus Notes en messagerie Microsoft Outlook avec un logiciel de migration avant de procéder à l'extraction des seuls e-mails pertinents.

41. Techniquement, la copie des seuls e-mails entrant dans le champ de l'enquête est donc possible et permet aux enquêteurs de disposer d'une copie strictement identique, l'opération n'altérant à notre connaissance aucune des données contenues dans cet e-mail qu'il s'agisse de la date, de l'expéditeur, du destinataire etc.

42. Il a enfin également été soutenu que cette méthode de saisie serait protectrice des droits de l'entreprise parce qu'elle garantirait l'intégrité de la messagerie à l'occasion de sa copie, tout ajout ou altération étant ce faisant évité. Cet argument a également été soutenu par certains Juges des libertés,

notamment celui de Tours : "seule la saisie de ce fichier indissociable donne une garantie d'origine pour ne pas modifier le numéro d'identification par une entrée. À défaut de cette garantie, respectueuse des droits de la défense, la polémique naîtrait sur la source"<sup>19</sup>.

43. La préoccupation d'intégrité et de non-modification des données à l'occasion des saisies informatiques est évidemment partagée par les entreprises, et doit constituer une préoccupation de premier plan, mais nous ne comprenons pas en quoi cette préoccupation devrait légitimer une saisie sans sélection préalable. Toute erreur de manipulation peut être évitée en effectuant une copie préalable de sécurité, sous contrôle de l'occupant des lieux et/ou de son conseil.

44. Par ailleurs, là encore, l'analogie avec les documents papier est possible et elle ne conduit pas du tout à retenir le même principe : les documents papier que les enquêteurs envisagent de saisir sont consultés par l'occupant des lieux ou son conseil, et sont photocopiés avant d'être placés sous scellés, alors même que cette consultation et cette photocopie seraient susceptibles d'altérer l'original. D'autres moyens sont mis en œuvre pour réduire ce risque.

45. Enfin, des arguments de pure opportunité sont soulevés pour justifier la saisie en masse sans sélection préalable, qu'il s'agisse des messageries électroniques ou des disques durs : le temps et le nombre d'agents nécessaires à la sélection, le fait que les saisies informatiques n'auraient plus dès lors d'intérêt puisqu'il suffirait d'imprimer les documents électroniques une fois lus etc. Ces arguments – à supposer qu'ils soient fondés – seraient toutefois d'un bien faible poids face à des garanties légales de cette importance. Il existe en effet des modalités simples permettant d'assurer un meilleur équilibre entre facultés d'investigation de l'autorité sur site et hors site et les garanties légales (point 3 ci-après).

## 2. Ces principes semblent au surplus produire des conséquences difficilement tenables aux stades ultérieurs de la procédure

46. Si la messagerie ou le répertoire saisis constituent réellement un tout indissociable, tel doit rester le cas tout au long de la procédure. Or, l'expérience montre que cela produirait des conséquences difficilement tenables.

47. Tout d'abord, un tout insécable qui contiendrait un document couvert par exemple par le privilège avocat/client devrait conduire à une annulation de la saisie du scellé concerné dans sa totalité. Or, il semble que les principes d'intégralité et d'insécabilité connaissent une première exception à l'occasion des recours jusqu'ici exercés devant le Juge des libertés : le plus souvent, il est demandé à la DGCCRF de procéder à l'effacement des seuls éléments concernés<sup>20</sup>.

15 TGI Paris, JLD, Ordonnance du 27 sept. 2007, *Syngenta Agro et Syngenta France*, ou encore TFO Lille, JLD, Ordonnance du 16 déc. 2005, *Comité français du gaz et du propane*.

16 Tel n'est pas l'avis du Conseil de la concurrence qui constatait dans sa décision n° 09-D-05 précitée : « S'agissant du cas particulier des messageries électroniques, la Cour de cassation considère que, au regard des procédures de recherche des infractions aux règles de concurrence, une boîte de messagerie constitue une pièce unique, même si elle n'est que partiellement utile au dossier (voir Cass. Crim du 12 déc. 2007, n° 06-81907, *Sita Centre Ouest*) » (point 68).

17 Crim, 12 déc. 2007, pourvoi n° 06-81.907, *Sita*.

18 TGI Paris, JLD, Ordonnance du 27 sept. 2007, *Syngenta Agro et Syngenta France*, ou encore TFO Lille, JLD, Ordonnance du 16 déc. 2005, *Comité français du gaz et du propane*.

19 TGI Tours, JLD, Ordonnance du 25 oct. 2005, *Sita Centre Ouest*.

20 TGI Lille, JLD, 16 déc. 2005, *Comité français du gaz et du propane* ou encore TGI Bobigny, 12 juill. 2005, *Védiorbis e.a.*

48. Ensuite, au stade de l’instruction, se pose la question de la constitution du dossier et de l’accès des différentes parties à celui-ci : si les services d’instruction souhaitent exploiter de tels éléments au soutien des griefs, ils doivent en effet s’assurer de l’absence de secrets d’affaires.

49. À partir du moment où une messagerie électronique a été considérée comme un tout indissociable, ils ne semblent avoir d’autre choix que de continuer à la considérer comme telle et à interroger globalement l’entreprise concernée sur l’existence éventuelle de secrets d’affaires au sein de ce document unique. La réponse qui leur sera faite par l’entreprise a toutes les chances d’être tout aussi globale : l’entreprise demandera vraisemblablement la protection des secrets d’affaires pour l’ensemble de la messagerie.

50. Dans l’affaire du travail temporaire, le Conseil de la concurrence a validé une telle méthode : compte tenu de la jurisprudence selon laquelle une messagerie constitue une pièce unique, même si elle n’est que partiellement utile au dossier, “il est dès lors légitime de la traiter comme telle au titre de la protection des secrets d’affaires en la classant globalement si une demande est faite en ce sens [...]”<sup>21</sup>. Pourtant, les textes prévoient – et prévoyaient à l’époque – que les demandes de secrets d’affaires soient faites par rapport aux “documents ou parties de documents” regardés comme mettant en jeu le secret des affaires<sup>22</sup>.

51. Jusqu’ici, la cohérence est certes maintenue avec les principes d’intégralité et d’insécabilité mais ce qui semble beaucoup plus difficile à concilier est la conséquence pratique qu’en tire le Conseil lorsque l’instruction souhaite néanmoins exploiter les éventuels éléments à charge qu’elle contient. La phrase se poursuit en effet ainsi : “[...] quitte à ce qu’elle soit ensuite le cas échéant partiellement déclassée pour les besoins de la procédure ou l’exercice des droits d’une partie mise en cause”.

52. Le principe d’insécabilité n’est donc suivi qu’en première analyse. Il incombe ensuite aux services d’instruction de déterminer s’ils souhaitent exploiter des éléments à charge dans cette messagerie, auquel cas ils pourront réinterroger l’entreprise concernée sur d’éventuels secrets d’affaires au sein de ces extraits de document.

53. Le Conseil de la concurrence s’est appuyé à cet égard sur la jurisprudence de la Cour de cassation qui n’a pas remis en cause le fait que les services d’instruction puissent tirer des éléments de preuve d’un dossier pénal et ne retenir de celui-ci que les seuls éléments à charge<sup>23</sup>. La question semble cependant différente : le dossier pénal ne constitue pas un “document unique” et il contient *a priori* des éléments plus externes à l’analyse des pièces que la messagerie électronique d’une des personnes les plus directement concernées par l’enquête, d’ailleurs exploitée par les services d’instruction eux-mêmes.

54. La réponse apportée par le Conseil nous semble produire une autre conséquence difficilement justifiable : face à une telle masse documentaire, il est assez manifeste que les services d’instruction se concentreront sur les éléments à charge, non sur les éléments à décharge que cette messagerie est susceptible de contenir, à commencer par des éléments de contexte entourant l’envoi de l’e-mail litigieux.

55. Le Conseil n’y voit cependant pas de difficulté : “les droits de la défense, en ce qui concerne la recherche d’éléments à décharge, sont raisonnablement assurés par la possibilité qu’a toujours la partie qui souhaite mettre en avant de tels éléments, de les puiser dans sa propre “documentation” ou dans les informations non couvertes par la protection du secret d’affaires”<sup>24</sup>. Certes, l’entreprise qui contestait ici la méthode employée n’avait pas contesté le classement de la messagerie en secrets d’affaires et sollicité d’y avoir accès, ainsi que le prévoit l’article R. 463-15, et le Conseil n’a pas manqué de le souligner.

56. Le principe ainsi exprimé de manière générale ne nous semble toutefois pas satisfaisant. Lorsqu’un e-mail échangé entre deux personnes dont parfois aucune ne fait partie de l’entreprise appelée à exercer ses droits de la défense, la renvoyer à sa propre documentation est illusoire. Au contraire, le contexte entourant l’envoi de cet e-mail (échanges antérieurs ou postérieurs entre les mêmes personnes, échanges parallèles au même moment avec d’autres personnes etc.) est susceptible de contenir des éléments à décharge particulièrement utiles à la défense des autres entreprises.

57. Ne pas rendre accessibles ces éléments, sans autre forme de procédé, ne nous semble pas protéger adéquatement les droits de la défense. *A minima*, il nous semble qu’il incombe à l’Autorité elle-même de fournir une liste assez précise des éléments contenus dans la messagerie électronique pour permettre aux autres entreprises de déterminer s’ils sont susceptibles d’être pertinents pour leur défense<sup>25</sup>. D’ailleurs, à la faveur de la réforme de la LME, les termes de l’article R. 463-15 ont été sensiblement modifiés : désormais, le Rapporteur confronté à une demande de classement informe l’entreprise concernée lorsqu’il considère qu’une pièce ainsi classée est nécessaire “à l’exercice des droits de la défense” et non plus seulement lorsqu’il estime qu’elle est nécessaire “à la procédure”<sup>26</sup>.

58. Il est à noter que de telles questions n’auraient à aucun moment surgi si les enquêteurs s’étaient initialement saisis des seuls éléments de la messagerie entrant dans le champ de

21 Cons. Conc., décision n° 09-D-05 du 2 févr. 2009, point 68.

22 Article R. 463-13 du Code de commerce.

23 Cour d’appel de Paris, 30 janv. 2007, *Le Foll TP e.a.*, n° 06/00566.

24 Ibid., point 65.

25 En ce sens, TPICE, 15 mars 2000, aff. Jtes T-25/95 e.a., points 142 à 144, 147 et 148 : “la Commission, afin de permettre aux parties de se défendre utilement, est tenue de leur rendre accessibles l’intégralité du dossier d’instruction, à l’exception des documents contenant des secrets d’affaires d’autres entreprises et des documents internes de la Commission [...] Si la préparation de versions non confidentielles de tous les documents s’avère difficile, elle doit transmettre aux parties concernées une liste suffisamment précise des documents posant problème pour leur permettre de déterminer, en connaissance de cause, si les documents décrits sont susceptibles d’être pertinents pour leur défense”.

26 Décret n° 2009-142 du 10 févr. 2009, JORF du 11 févr. 2009.

l'enquête : la sélection des documents aurait permis un traitement document par document des questions de secret d'affaires, et sous cette réserve stricte, l'ensemble des documents auraient été versés au dossier.

59. Une autre question que soulève l'accès au dossier appliqué aux données informatiques est celle de l'utilisation éventuelle des métadonnées et des fichiers non apparents en cas de saisie par copie-image. En effet, la méthode d'organisation des dossiers et de traitement des secrets d'affaires s'effectue sur une base papier même si les données d'origine sont issues de supports informatiques. Cette méthode semble totalement inadaptée à un cas dans lequel ces données "cachées" seraient exploitées, sauf à extraire l'ensemble de ces données cachées et à les inclure au dossier, non seulement s'agissant des documents exploités par l'instruction mais aussi s'agissant d'éventuels éléments à décharge. On conviendra en outre que de telles méthodes d'investigation relèvent bien plus d'enquêtes policières liées à des infractions pénales graves que des enquêtes administratives, et nous n'avons d'ailleurs pas connaissance de cas pour l'heure.

### III. Il existe pourtant des modalités de saisies permettant de mieux respecter les garanties légales sans pour autant limiter le champ d'investigation des Autorités de concurrence

60. Au plan international, les problématiques suscitées par les saisies informatiques de concurrence ont d'ores et déjà donné lieu à un certain nombre de développements. Dès 1998, la Commission "Droit et pratiques de la concurrence" de la Chambre de commerce internationale éditait un Code pratique recommandé à l'attention des autorités de concurrence s'agissant des saisies informatiques. Ce Code pratique évoquait entre autres la problématique des données couvertes par le privilège avocat/client et recommandait aux autorités "de développer et de mettre en œuvre des procédures afin de maintenir la confidentialité des documents privilégiés et d'éviter leur divulgation"<sup>27</sup>.

61. Peu d'autorités ont suivi pour l'heure cette suggestion d'adoption et de publication d'un Code pratique. L'une d'entre elle, de longue date, est l'autorité de concurrence néerlandaise, qui disposait d'une Méthode de travail pour la recherche numérique dès 2003. La version actuelle, mise à jour en 2007, prévoit des modalités de protection des documents hors champ, couverts par le privilège avocat/client, ou encore relevant de la vie privée<sup>28</sup>. Cette Méthode apporte une

première réponse au sujet en proposant l'identification et la suppression de ces documents des données copiées au cours de l'inspection. Pour les documents qui n'auraient pu être identifiés sur site (notamment en cas de saisie par copie-image), l'entreprise dispose de dix jours pour signaler les documents concernés, pendant lesquels l'exploitation des données est suspendue.

62. Ainsi qu'il sera exposé ci-après, la Commission européenne a elle-même précisé plus avant sa pratique en la matière dans le cadre de la Note explicative systématiquement remise dans le cadre des inspections.

63. L'*International Competition Network* s'est également penché sur le sujet dans le cadre du Manuel anti-cartel, qui comporte un chapitre dédié à la recherche de preuve numérique depuis avril 2006<sup>29</sup>. S'agissant des documents couverts par le privilège ou relevant de la vie privée, ce Rapport fait état de ce que "la plupart des autorités ne sont pas autorisées à saisir ou à copier les documents couverts par le privilège ou relatifs à la vie privée" et souligne que ceci peut "restreindre en pratique la capacité de certaines autorités de procéder à des prises d'images numériques ou à des copies de supports numériques de grande taille" dont le contenu ne pourra être vérifié sur site<sup>30</sup>.

64. Le Rapport fait état de modalités retenues par certaines autorités pour assurer la protection de ces données (que la saisie soit faite par copie simple ou par copie-image) : vérification sur site en remettant une copie à l'occupant des lieux afin qu'il désigne les documents concernés, placement sous enveloppe scellée et recours en cas de contestation, examen des données après l'inspection, l'entreprise ayant préalablement désigné les documents concernés qui sont détruits, sélection par l'autorité après l'inspection et retour pur et simple des données couvertes par le privilège. Si les pratiques sont assez diverses, on doit noter que le plus grand nombre de cas cités tente de trouver un équilibre beaucoup plus satisfaisant entre garanties légales et facultés d'investigation.

65. Après examen de ces différentes modalités, le Manuel de l'ICN érige la protection des documents couverts par le privilège et privés en pratique recommandée : "Il est une bonne pratique d'avoir une approche systématique de revue, sélection et prise en charge des informations privilégiées et privées, ainsi que des informations possiblement privilégiées et privées"<sup>31</sup>.

27 ICC, "Commission on Law and Practices Relating to Competition, ICC Recommended Code of Practice for Competition Authorities on Searches and Subpoenas of Computer Records", 16 oct. 2008, <http://www.iccwbo.org/id908/index.html>.

28 NMA, Méthode de travail pour la recherche digitale, 12 déc. 2007, [http://www.nmanet.nl/nederlands/home/Actueel/Publicaties/Richtsnoeren/NMa\\_herziet\\_werkwijze\\_digitaaal\\_onderzoek.asp](http://www.nmanet.nl/nederlands/home/Actueel/Publicaties/Richtsnoeren/NMa_herziet_werkwijze_digitaaal_onderzoek.asp), traduction informelle.

29 ICN, *Anti-cartel Enforcement Manual*, Chapter 3, "Digital Evidence Gathering", avr. 2006, traduction informelle.

30 Voir p. 20-21.

31 Appendix 1, "Good Practices relating to digital evidence gathering".

## 1. La pratique développée par la Commission européenne en cas de nécessité de poursuivre la sélection ultérieurement dans ses locaux

66. La Commission européenne a développé il y a de nombreuses années une pratique d'enveloppe scellée qui n'existait pas dans les textes afin de pouvoir placer les documents soulevant une contestation dans un contenant qui ne permettait pas aux enquêteurs de consulter les documents dans l'attente d'un règlement de cette contestation par la Commission ou les juridictions communautaires. Cette pratique est notamment utilisée couramment pour les documents possiblement – mais non sûrement – couverts par le privilège avocat/client. Elle a assez naturellement été adaptée au cas des saisies informatiques.

67. En matière de saisies informatiques, la Commission européenne recherche tout d'abord à procéder à une sélection sur site. Poursuivant fréquemment son investigation deux ou trois jours, elle est en effet en mesure de dédier le temps nécessaire à un certain nombre d'opérations de sélection informatique avant de quitter les lieux. Ce n'est donc que lorsque les agents de la Commission n'ont pas matériellement la capacité de terminer la sélection des fichiers informatiques *in situ*, une copie des données non encore vérifiées est placée sous une enveloppe scellée, qui ne pourra être ouverte qu'en présence de l'entreprise afin de poursuivre la sélection dans les locaux de la Commission :

*“Si les agents, ou d'autres personnes autorisées par la Commission qui les accompagnent, le considèrent approprié, une copie intégrale d'un medium de stockage digital, telle qu'une image disque, peut également être effectuée. Ceci peut se produire, par exemple, lorsque la sélection de documents et de données sur site n'est pas achevée, ou lorsque les agents ou d'autres personnes autorisées par la Commission considèrent que cela est nécessaire pour la préservation d'informations qui pourraient être perdues ou lorsque l'accès aux données et documents sélectionnés n'est pas possible in situ. Si la sélection des documents pertinents pour l'enquête n'est pas achevée pendant l'inspection, la copie digitale (DVD, disque dur, [...]) des données encore à vérifier est placée dans une enveloppe qui est scellée in situ et emmenée par les agents. Une réplique de la copie digitale est donnée à l'entreprise. L'entreprise sera ensuite invitée par la Commission à assister à l'ouverture de l'enveloppe scellée et au processus de sélection dans les locaux de la Commission”<sup>32</sup>.*

68. Nous y voyons deux différences fondamentales avec la pratique française. Tout d'abord, la saisie en masse n'est pas envisagée *ab initio* et de manière systématique comme cela paraît fréquemment être le cas dans les enquêtes de la DNE. Elle est envisagée uniquement lorsque la sélection ne peut raisonnablement être achevée sur site ou en présence de documents cryptés ou bloqués par mots de passe. Ensuite, la

saisie sans sélection préalable est protégée de toute prise de connaissance par les enquêteurs par le placement sous enveloppe scellée jusqu'à son ouverture en présence de l'entreprise.

69. De telles modalités ne sont pas parfaites parce que la sélection qui sera réalisée dans les locaux de la Commission devra conduire à prendre une connaissance minimale des documents avant de voir reconnaître leur caractère hors champ ou privilégié<sup>33</sup>. Mais elles constituent déjà une avancée considérable par rapport à la pratique française actuelle.

70. Une troisième différence réside dans la transparence ainsi mise en œuvre par la Commission européenne sur ses méthodes d'investigation : dans une note qu'elle met régulièrement à jour et qu'elle joint aux documents remis aux entreprises faisant l'objet d'une inspection, la Commission expose un certain nombre des modalités qu'elle met en œuvre et que l'entreprise peut dès lors solliciter. Si cette Note ne traite pas de toutes les problématiques pouvant surgir en cas de saisie informatique, le sujet est néanmoins évoqué dans le prolongement de la Bonne Pratique recommandée par l'ICN. Il y a là aussi certainement matière à inspiration pour l'Autorité.

## 2. Les outils proposés par la procédure pénale française elle-même

71. La procédure pénale française – qui s'applique largement dans le cadre des visites et saisies – offre elle-même des modalités pratiques qui sont très proches de l'enveloppe scellée communautaire. Les saisies peuvent en effet être effectuées sous scellés fermés ; il s'agit même de la règle générale prévue par l'article 56 du Code de procédure pénale.

72. Il est à noter que, dans d'autres formes d'enquêtes, le législateur a prévu expressément la saisie de données informatiques sous scellés fermés dans l'attente d'un tri ultérieur en présence de l'entreprise. Ainsi, l'article 97 du Code de procédure pénale (perquisitions réalisées par les juges d'instruction) prévoit :

*“Lorsque ces scellés sont fermés, ils ne peuvent être ouverts et les documents dépouillés qu'en présence de la personne, assistée de son avocat, ou eux dûment appelés. Le tiers chez lequel la saisie a été faite est également invité à assister à cette opération”.*

73. Si la même disposition n'a pas été intégrée à l'article 56, ce dernier renvoie lui-même à la possibilité de scellés fermés ou de scellés fermés temporaires. Les agents nous semblent donc parfaitement habilités à mettre en œuvre le même mécanisme.

74. Certains Juges des libertés saisis n'ont d'ailleurs pas manqué de le souligner. Ainsi le Juge des libertés de Nanterre a annulé à plusieurs reprises des saisies informatiques dans leur intégralité aux motifs suivants :

<sup>32</sup> Notice explicative de mars 2008, <http://ec.europa.eu/competition/antitrust/legislation/legislation.html>, traduction informelle.

<sup>33</sup> TPICE, 17 sept. 2007, aff. jtes. T-125/03 e.a.



**Concurrences** est une revue trimestrielle couvrant l'ensemble des questions de droits communautaire et interne de la concurrence. Les analyses de fond sont effectuées sous forme d'articles doctrinaux, de notes de synthèse ou de tableaux jurisprudentiels. L'actualité jurisprudentielle et législative est couverte par neuf chroniques thématiques.

# CONCURRENCES

## Editorial

Elie Cohen, Laurent Cohen-Tanugi,  
Claus-Dieter Ehlermann, Ian Forrester,  
Eleanor Fox, Laurence Idot, Frédéric Jenny,  
Jean-Pierre Jouyet, Hubert Legal,  
Claude Lucas de Leyssac, Louis Vogel,  
Denis Waelbroeck...

## Interview

Sir Christopher Bellamy, Dr. Ulf Böge,  
Nadia Calvino, Frédéric Jenny, William Kovacic,  
Neelie Kroes, Christine Lagarde, Mario Monti,  
Viviane Reding, Robert Saint-Esteben, Sheridan Scott...

## Tendances

Marie-Laure Allain, Jacques Barrot, Jean-François  
Bellis, Murielle Chagny, Claire Chambolle,  
Luc Chatel, Dominique de Gramont,  
Damien Gérardin, Christophe Lemaire,  
Pierre Moscovici, Jorge Padilla, Emil Paulis,  
Joëlle Simon, Richard Whish...

## Doctrines

Guy Canivet, Emmanuel Combe, Thierry Dahan,  
Luc Gyselen, Daniel Fasquelle, Barry Hawk,  
Laurence Idot, Frédéric Jenny, Bruno Lasserre,  
Anne Perrot, Catherine Prieto, Patrick Rey,  
Didier Theophile, Joseph Vogel...

## Pratiques

Tableaux jurisprudentiels : Bilan de la pratique  
des engagements, Droit pénal et concurrence,  
*Legal privilege*, *Cartel Profiles in the EU*...

## Horizons

Allemagne, Belgique, Canada, Chine,  
Hong-Kong, Japon, Luxembourg, Suisse, USA...



## Droit et économie

Emmanuel COMBE, Philippe CHONÉ,  
Laurent FLOCHEL, Penelope PAPANDROPOULOS,  
Etienne PFISTER, Francisco ROSATI, David SPECTOR...

## Chroniques

### Ententes

Michel DEBROUX  
Laurence NICOLAS-VULLIERME  
Cyril SARRAZIN

### Pratiques unilatérales

Catherine PRIETO  
Anne-Lise SIBONY  
Anne WACHSMANN

### Pratiques restrictives et concurrence déloyale

Mireille DANY  
Daniel FASQUELLE  
Marie-Claude MITCHELL

### Concentrations

Jean-Mathieu COT  
Jérôme PHILIPPE  
Stanislas MARTIN

### Aides d'État

Jean-Yves CHÉROT  
Jacques DERENNE  
Christophe GIOLITO

### Procédures

Pascal CARDONNEL  
Christophe LEMAIRE  
Agnès MAÏTREPIERRE  
Chantal MOMÈGE

### Régulations

Denis LESCOPE  
Jean-Paul TRAN THIET  
Thierry TUOT

### Secteur public

Bertrand du MARAIS  
Stéphane RODRIGUES  
Jean-Philippe KOVAR

### Politique internationale

Frédérique DAUDRET-JOHN  
François SOUTY  
Stéphanie YON

## Revue des revues

Christelle ADJÉMIAN  
Umberto BERKANI  
Alain RONZANO

## Bibliographie

Centre de Recherches sur l'Union Européenne  
(Université Paris I – Panthéon-Sorbonne)

	<b>HT</b>	<b>TTC</b>
	<i>Without tax</i>	<i>Tax included (France only)</i>
<b>Revue Concurrences   Review Concurrences</b>		
<input type="checkbox"/> Abonnement annuel - 4 n° (version papier) <i>1 year subscription (4 issues) (print version)</i>	420 €	428,80 €
<input type="checkbox"/> Abonnement annuel - 4 n° (version électronique + accès libre aux e-archives) <i>1 year subscription (4 issues) (electronic version + free access to e-archives)</i>	510 €	609,96 €
<input type="checkbox"/> Abonnement annuel - 4 n° (versions papier & électronique accès libre aux e-archives) <i>1 year subscription (4 issues) (print &amp; electronic versions + free access to e-archives)</i>	620 €	741,52 €
<input type="checkbox"/> 1 numéro (version papier) <i>1 issue (print version)</i>	125 €	127,62 €

**Bulletin électronique e-Competitions | e-bulletin e-Competitions**

<input type="checkbox"/> Abonnement annuel + accès libre aux e-archives <i>1 year subscription + free access to e-archives</i>	560 €	669,76 €
---	-------	----------

**Revue Concurrences + bulletin e-Competitions | Review Concurrences + e-bulletin e-Competitions**

<input type="checkbox"/> Abonnement annuel revue (version électronique) + e-bulletin <i>1 year subscription to the review (online version) and to the e-bulletin</i>	730 €	873,08 €
<input type="checkbox"/> Abonnement annuel revue (versions papier & électronique) + e-bulletin <i>1 year subscription to the review (print &amp; electronic versions) + e-bulletin</i>	820 €	980,72 €

**Renseignements | Subscriber details**

Nom-Prénom | *Name-First name* : ..... e-mail : .....  
 Institution | *Institution* : .....  
 Rue | *Street* : ..... Ville | *City* : .....  
 Code postal | *Zip Code* : ..... Pays | *Country* : .....  
 N° TVA intracommunautaire/ *VAT number (EU)* : .....

**Paieement | Payment details**

Vous pouvez payer directement sur [www.concurrences.com](http://www.concurrences.com) (accès immédiat à votre commande) ou bien utiliser ce formulaire :  
*For instant access to your order, pay on-line on www.concurrences.com. Alternatively :*

- Veuillez m'adresser une facture d'un montant de ..... €  
*Please bill me for the sum of ..... €*
- Veuillez débiter ma carte MasterCard/Visa/American Express d'un montant de ..... €  
*Please debit the sum of ..... € from my MasterCard/Visa/American Express*

Numéro de carte/ *Card n°* : .....  
 Date d'expiration/ *Expiry date* : .....  
 Nom-Prénom/ *Name-First name* : .....

Signature

- J'ai transféré au compte bancaire dont références ci-dessous la somme de ..... € à la date du .....  
*I have transferred the sum of ..... € to the bank account below on ..... (date)*

IBAN (International Bank Account Number)	BIC (Bank Identifier Code)
<b>FR76 3000 4007 9900 0255 3523 060</b>	<b>BNPAFRPPPOP</b>

**Bank : BNP - Agence Opéra | 2, Place de l'Opéra - 75 002 Paris - France**

**Formulaire à retourner à | Send your order to**

**Transactive** – A ThomsonReuters subsidiary  
 1 rue Saint-Georges | 75 009 Paris – France | *contact: information@transactive.fr*

**Conditions générales (extrait) | Subscription information**

Les commandes sont fermes. L'envoi de la revue ou des articles de *Concurrences* et l'accès électronique aux bulletins ou articles de *e-Competitions* ont lieu dès réception du paiement complet. Tarifs pour licences monopostes; nous consulter pour les tarifs multipostes. Consultez les conditions d'utilisation du site sur [www.concurrences.com](http://www.concurrences.com) ("Notice légale").

*Orders are firm and payments are not refundable. Reception of Concurrences and on-line access to e-Competitions and/or Concurrences require full prepayment. Tarifs for 1 user only. Consult us for multi-users licence. For "Terms of use", see www.concurrences.com.*

**Frais d'expédition Concurrences hors France : 30 € | 30 € extra charge for sending hard copies outside France**