

# LES SAISIES INFORMATIQUES EN FRANCE APRÈS L'ÉVOLUTION DE LA MÉTHODOLOGIE DE LA COMMISSION : ENFIN UN PEU DE LUMIÈRE AU BOUT DU TUNNEL ?\*

Nathalie JALABERT-DOURY

Avocat, Mayer Brown, Paris

1. Il y a tout juste quatre ans, alors que la nouvelle Autorité de la concurrence prenait ses fonctions, nous formions le vœu d'une évolution de la méthodologie utilisée jusqu'alors par la DGCCRF s'agissant des saisies informatiques<sup>7</sup>.

18. Cette méthodologie reposait en effet sur l'utilisation du logiciel EnCase – alors également utilisé par la Commission européenne – et sur la copie de l'ensemble des fichiers contenant les mots clés définis par les enquêteurs. À l'arrivée, la masse de données informatiques saisies contenait entre autres – voire principalement – des données sans rapport avec l'objet de l'enquête, y inclus, le cas échéant, des données couvertes par le privilège des correspondances avocat-client.

19. En donnant la responsabilité première en matière d'enquêtes à l'Autorité, les articles L. 450-1 et suivants issus de la loi de modernisation de l'économie rouvraient le débat sur cette méthodologie et son évolution éventuelle pour se rapprocher de modèles plus protecteurs pratiqués par les homologues de l'Autorité de la concurrence, notamment la Commission européenne, la NMA néerlandaise ou encore le Department of Justice américain<sup>8</sup>.

20. Sur ce terrain, le bilan des quatre années écoulées depuis la création de l'Autorité de la concurrence est plutôt morose : non seulement l'Autorité a repris à son compte la méthodologie de la DGCCRF sans y apporter de modification perceptible, mais la Cour de cassation a en outre refermé une à une les perspectives d'évolution ouvertes par les juges du fond. En revanche, certaines autorités dont nous avons comparé les méthodes avec celles de l'Autorité ont franchi, dans l'intervalle, une étape supplémentaire dans la sophistication des outils et/ou dans la protection des droits des entreprises et des personnes.

21. Le régime français des saisies informatiques est donc une nouvelle fois à la croisée des chemins.

## I. Rappel des termes du débat : De la saisie limitée des documents papier à la saisie quasi illimitée des fichiers électroniques

22. Depuis la loi NRE du 15 mai 2001, l'article L. 450-4 du code de commerce dispose que les enquêteurs munis d'une ordonnance judiciaire autorisant des visites et saisies peuvent procéder "à la saisie de documents et de tout support d'information". L'article L. 450-4 renvoie également à l'article 56 du code de procédure pénale, lequel indique qu'il est "procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition". Les enquêteurs de la DGCCRF et de l'Autorité estiment sur cette base qu'ils peuvent saisir non seulement des documents "papier", mais aussi procéder à toute copie électronique, voire saisir le support lui-même (disque dur).

23. Cette lecture d'une modification législative un peu hâtive est peu contestable, mais encore faut-il que la fin puisse justifier les moyens.

24. En effet, les saisies informatiques peuvent permettre de copier une masse considérable de données dans des délais très réduits par rapport au temps nécessaire pour passer en revue puis copier des documents papier (pour l'entreprise, les originaux étant saisis par les enquêteurs).

25. Or, l'expérience montre que la méthodologie retenue conduit à des saisies massives de multiples fichiers Word, Excel ou PDF ainsi que des messageries électroniques dans leur intégralité, pour l'essentiel sans rapport avec le champ de l'enquête.

26. Ces saisies sont dès lors susceptibles de priver d'effet la limitation du champ d'investigation autorisé par l'ordonnance, considérée comme une garantie fondamentale de l'entreprise face aux mesures d'enquête arbitraires et disproportionnées, le tout pour permettre à des agents administratifs d'instruire d'éventuelles infractions au droit économique dans des conditions leur permettant de gagner du temps, voire d'économiser le coût de logiciels permettant des recherches et des copies plus ciblées.

\* Cet article est en mise à jour d'un article précédemment publié dans la revue *Concurrences*: Nathalie Jalabert-Doury, "Saisies informatiques : Le régime français à l'épreuve des impératifs de conformité et de cohérence", *Concurrences* N° 2-2009, n° 25896, pp. 69-77 sur [www.concurrences.com](http://www.concurrences.com)

<sup>7</sup> N. Jalabert-Doury, « Saisies informatiques : Le régime français à l'épreuve des impératifs de conformité et de cohérence » préc.

<sup>8</sup> N. Jalabert-Doury, Digital evidence searches in competition investigations: Best practices for effective fundamental rights, *Concurrences* n° 4-2009, p. 65.

27. S'agissant des documents papier, la jurisprudence a, de longue date, fixé les limites du pouvoir de saisie des enquêteurs :

→ seuls les documents “utiles” en rapport avec l'objet de l'enquête, tel que défini dans l'ordonnance de visite et saisie, peuvent être saisis. La jurisprudence a également validé la saisie de documents “pour partie utiles” à la preuve des pratiques lorsqu'ils traitent de plusieurs sujets et seulement en partie d'un sujet entrant dans le champ de l'autorisation judiciaire (ex. : compte rendu d'une réunion ayant traité de plusieurs sujets, qui peut néanmoins être saisi dans son intégralité)<sup>9</sup> ;

→ dans la même logique, les documents privés échappent en principe au contrôle, mais des documents mixtes contenant à la fois des annotations professionnelles et privées peuvent être saisis (ex. : agenda, qui peut également être saisi dans son intégralité)<sup>10</sup> ;

→ enfin, les documents relevant du secret professionnel entre l'avocat et son client sont insaisissables et le secret professionnel peut être opposé aux enquêteurs<sup>11</sup>.

28. La DGCCRF a transposé ces principes à sa manière aux fichiers électroniques : dès lors que la mise en œuvre des mots clés faisait apparaître un résultat positif sur un ordinateur donné, elle procédait soit à la copie-image de l'ensemble du disque dur, soit à la copie systématique de l'ensemble des fichiers ayant répondu positivement à la recherche, y inclus les fichiers de messagerie électronique qui se présentent (à tout le moins, dans certains systèmes de messagerie) comme un seul et même fichier sur le poste utilisateur concerné.

29. La DGCCRF estimait par ailleurs ne pas avoir à prendre des précautions comparables à celles mises en œuvre par un grand nombre d'autorités pour éviter toute prise de connaissance par leurs enquêteurs des documents hors champ de l'enquête et, *a fortiori*, des documents couverts par le privilège avocat-client<sup>12</sup>.

30. Les premiers recours portant sur le champ des saisies informatiques opérées ont été introduits par les entreprises au milieu des années 2000 auprès des juges des libertés, puis des magistrats délégués par les premiers présidents des cours d'appel ayant autorisé les visites et saisies.

31. Les entreprises ont mis en avant la possibilité – et donc l'obligation – pour l'administration de procéder au tri des données informatiques, comme elles l'ont toujours fait pour les documents “papier”, tandis que l'administration invoquait son droit de saisir les supports eux-mêmes aux termes de l'article L. 450-4 et le fait qu'une messagerie électronique se présente comme un seul et même fichier, qui serait d'ailleurs insécable pour des raisons d'authenticité et de traçabilité de la preuve.

32. Cette insécabilité n'est pourtant qu'un rideau de fumée :

→ sur le plan technique, tout d'abord, il existe des outils reconnus permettant de procéder à la saisie sélective de messages électroniques individuels dans des conditions d'authenticité et de traçabilité aussi satisfaisantes que celles des saisies globales de messageries<sup>13</sup> ;

→ ensuite, quelles que soient les techniques utilisées, différentes protections peuvent être conçues et mises en œuvre, à l'image de ce que font de nombreuses autorités (recours à l'enveloppe scellée, impression des messages électroniques par les enquêteurs sous contrôle de l'entreprise, revue et tri des données par des personnels indépendants des enquêteurs, etc.). L'article 56 du code de procédure pénale prévoit d'ailleurs lui-même une faculté de placer les données sous scellés fermés “jusqu'au moment de leur inventaire et de leur mise sous scellés définitifs, et ce, en présence des personnes qui ont assisté à la perquisition” qui pourrait être utilisée pour procéder au tri des données sous contrôle du juge des libertés.

33. Aucune ligne commune ne s'est véritablement dégagée de ces ordonnances assez diverses retenant, selon les cas, (i) l'insécabilité et donc la possibilité pour l'administration de procéder à la saisie complète d'une messagerie dès lors que les enquêteurs avaient vérifié la présence d'éléments entrant dans le champ de l'enquête (ii) au contraire l'obligation pour l'administration d'individualiser les messages électroniques entrant dans le champ de l'enquête et non couverts par le privilège avocat/client, ou (iii) à tout le moins de fournir aux entreprises un inventaire plus précis des éléments saisis<sup>14</sup>.

34. De son côté, l'Autorité de la concurrence a repris à son compte la méthodologie mise en place par la DGCCRF et continué, notamment, à procéder à la saisie de messageries électroniques dans leur intégralité.

## II. Le bilan de quatre années sombres de jurisprudence de la Cour de cassation

35. Les premiers signaux donnés par la Cour de cassation en 2007 puis 2009 se sont avérés peu engageants. Les opérations de saisie ont été validées, la Cour rappelant que l'administration pouvait saisir des “pièces pour partie utiles” à l'enquête et constatant que le juge avait “souverainement estimé que les supports et données saisis n'étaient ni divisibles ni étrangers au but de l'autorisation accordée”<sup>15</sup>.

9 V. par ex., Cass. Com., 12 novembre 1996, pourvoi n° 94-13.944 e.a.

10 CA Paris, 25 mars 2008, RG n° 07/04789.

11 Cass. Com., 15 décembre 1998, pourvoi n° 96-30.082.

12 N. Jalabert-Doury, Digital evidence searches in competition investigations: Best practices for effective fundamental rights, précité.

13 C'était tout l'objet de la mesure d'expertise ordonnée par la Cour d'appel de Paris, cf. point 2 ci-après. Pour ne citer que certains d'entre eux : XWays Forensics et Paraben P2 Commander.

14 Pour quelques exemples, voir TGI Paris, 27 septembre 2007, *Syngenta Agro et Syngenta France* ; TGI Paris, 12 juillet 2007, *Du Pont de Nemours* ; TGI Lille, 16 décembre 2005, *Comité Français du Gaz et du Propane* ; TGI Tours, 20 octobre 2005, *SITA Centre ouest* ; TGI Nanterre, 20 mars 2007, *Beiersdorf* ; CA Versailles, 19 février 2010, *Janssen Cilag e.a.*

15 Cass. crim., 12 décembre 2007, pourvoi n° 06-81.907 ; Cass. crim., 17 juin 2009, pourvoi n° 07-88.354.

36. Mais, à compter du 1<sup>er</sup> juillet 2009, la Cour de cassation a pris encore plus expressément position en faveur de l'analyse du fichier unique, validant implicitement la saisie de messageries complètes au motif que *“l'administration n'avait pas à individualiser sur place les seuls messages entrant dans le champ de l'autorisation judiciaire”*<sup>16</sup>, étant précisé par ailleurs que *“la confection de scellés provisoires est une faculté laissée à l'appréciation des enquêteurs”*<sup>17</sup>.

37. Un des juges des libertés saisis de ce type de recours avait cependant pris une autre voie et décidé de recourir à une expertise devant au préalable permettre de lever l'incertitude technique concernant la sécabilité. Le cas était d'autant plus notable qu'une des entreprises concernées par cette demande d'expertise avait subi d'importantes saisies informatiques, incluant la messagerie électronique de son directeur juridique contenant de nombreux messages échangés avec ses avocats, dont des échanges relatifs à d'autres affaires en cours devant l'Autorité de la concurrence. Par ordonnances du 2 novembre 2010, le magistrat délégué de la cour d'appel de Paris a indiqué que ce type de considérations pourrait peut-être commander l'annulation du procès-verbal *“s'il n'était démontré que les méthodes des enquêteurs étaient les seules qui garantissent la sécurité et l'efficacité des opérations, le délégué du premier président se réservant de vérifier ensuite leur conformité à la loi”*, justifiant le recours à l'expertise pour notamment *“évaluer techniquement la possibilité de la saisie sélective de messages dans la messagerie électronique sans compromettre l'authenticité de ceux-ci”*<sup>18</sup>.

38. Sur pourvoi de l'Autorité, dirigé contre le principe même du recours à l'expertise ou ses résultats, la réponse de la Cour de cassation a été des plus surprenantes. Celle-ci a jugé que *“seuls les faits dont dépend la solution du litige peuvent, à la demande des parties ou d'office, faire l'objet d'une mesure d'instruction”* et que *“le juge (...) ne pouvait [sans méconnaître ce principe] ordonner une mesure sans rapport concret avec le litige comme tendant à apprécier la possibilité pour les enquêteurs de procéder autrement qu'ils ne l'avaient fait”*<sup>19</sup>.

39. Les ordonnances d'expertise ont donc été annulées et, sur renvoi après cassation, le magistrat délégué de renvoi au sein de la cour d'appel de Paris a sans surprise repris à sa charge le principe d'insécabilité et n'a constaté aucune violation des droits fondamentaux dans la saisie d'échanges entre l'entreprise et son avocat dans un autre dossier en cours. L'entreprise en question a simplement été invitée à lister les éléments concernés pour en obtenir restitution de la part de l'Autorité de la concurrence après que ces éléments ont pu rester entre ses mains pendant trois ans<sup>20</sup>.

40. Dans un arrêt de 2012, la Cour de cassation reprendra même totalement à son compte la théorie de l'insécabilité en faisant référence au fait que les fichiers en cause étaient *“constitués de messageries électroniques insécables”*<sup>21</sup>.

16 Cass. crim., 1<sup>er</sup> juillet 2009, pourvoi n° 07-87.080 e.a.

17 Cass. crim., 11 janvier 2012, pourvoi n° 10-87.087.

18 CA Paris, 2 novembre 2010, RG n° 10/01894 e.a. V. égal. ordonnance du 4 janvier 2011, RG 09/13945, CSTB.

19 Cass. crim., 16 juin 2011, puis Cass. crim., 11 janvier 2012, pourvois n° 10-88.197 e.a.

20 Cour d'appel de Paris, ordonnance du 31 août 2012, RG n° 10/01894.

21 Cass. crim., 11 janvier 2012, pourvoi n° 10-87.087.

### III. Dans l'intervalle, des modèles plus avancés ont continué à faire évoluer leurs procédures

41. En août 2010, l'autorité de concurrence néerlandaise (l'une des premières à avoir formalisé une méthodologie en la matière) a tout d'abord fait évoluer significativement ses règles<sup>22</sup> sous l'impulsion de ses juridictions de contrôle<sup>23</sup>. Dans le cadre de cette nouvelle procédure, les recherches sont principalement réalisées par mots clés (communiqués à l'entreprise à la fin de l'inspection) et conduisent à séparer les données en deux séries *“within scope”* et *“possibly out-of scope”*. L'entreprise est en mesure de faire valoir le privilège avocat/client pour que les données concernées soient écartées des éléments saisis. En cas de désaccord, une procédure d'enveloppe scellée est mise en œuvre, le temps que l'entreprise puisse, le cas échéant, exercer un recours.

42. Les deux séries de données sont ensuite traitées au niveau des spécialistes informatiques de l'autorité néerlandaise pour restituer à l'entreprise les éléments qui ne seraient pas pertinents, en présence de l'entreprise si celle-ci en fait la demande. L'entreprise a elle-même la possibilité de lister les éléments non pertinents ainsi que les éléments privilégiés qui n'auraient pas été écartés pendant l'inspection pour qu'ils lui soient restitués. Durant cette procédure de tri complémentaire, les rapporteurs en charge du dossier n'ont pas accès aux données. À l'issue du processus, seules les données entrant dans le champ de l'enquête et non privilégiées sont intégrées au dossier.

43. La Commission européenne vient également de publier une version révisée de sa notice explicative relative aux inspections. Cette nouvelle version incorpore le bénéfice de sa pratique décisionnelle concernant le blocage de comptes de messagerie et plus largement le niveau de coopération attendu des entreprises concernant l'accès aux serveurs et la compréhension de l'infrastructure des réseaux. Mais le plus important n'est pas là et réside dans l'amélioration concomitante de la méthodologie utilisée par la Commission, fort utilement rendu publique par l'article de Dirk Van Erps. Si un certain nombre des précisions ainsi apportées devraient à terme trouver leur place dans la notice elle-même pour assurer toute la transparence requise en conditions d'inspection, cet article a d'ores et déjà le mérite d'exister.

44. Jusqu'à présent, la Commission avait mis au point une méthodologie de recherche sur place des éléments entrant dans le champ de l'enquête et non couverts par le privilège avocat-client. À défaut de temps suffisant, les données non exploitées étaient placées sous enveloppe scellée dans l'attente de leur tri dans les locaux de la Commission, en présence de l'entreprise et de ses conseils. Cette méthodologie avait le mérite de mieux préserver les droits des entreprises et des personnes que la méthodologie française mais avec un inconvénient sérieux : les éléments sélectionnés étaient purement et simplement imprimés.

22 Procedure in relation to the Inspection and Copying of Analog and Digital Data and Documents, 10 août 2010.

23 District Court of The Hague, 13 October 2008, LJN:BH2647.

45. Le nouvel outil NuiX devra faire ses preuves sur le terrain, mais il présente, selon la Commission, l'avantage de pouvoir relier un serveur, sur lequel les données à vérifier sont stockées, et un certain nombre de postes de revue, sur lesquels les données sont ensuite triées, afin de réaliser des copies électroniques des seuls éléments retenus avec un inventaire assez détaillé, avant qu'une procédure de nettoyage de l'ensemble des postes utilisés ne soit mise en œuvre. Nous comprenons par ailleurs que l'outil permet la copie sélective des seuls éléments entrant dans le champ de l'enquête, messages électroniques inclus. La pratique de l'enveloppe scellée pour les données qui n'ont pu être triées sur place est par ailleurs maintenue, mais elle a vocation à devenir plus exceptionnelle.

46. À l'occasion de sa conférence de mars 2010, l'International Competition Network a également mis à jour son code de bonnes pratiques relatif aux recherches électroniques de 2008<sup>24</sup>. Il s'agit d'un guide réalisé par et pour les autorités de concurrence qui composent le réseau. Il se concentre donc largement sur les questions relatives aux outils et aux méthodes, mais comporte néanmoins un point 8 relatif aux questions juridiques posées par les recherches de preuve sur informatique. L'une de ces bonnes pratiques, approuvée par la communauté internationale des autorités de concurrence, est *"d'avoir une approche systématique pour l'examen, la sélection et le traitement des données électroniques privilégiées et privées, ainsi que potentiellement privilégiées et privées"*<sup>25</sup>.

## IV. Quel avenir pour les saisies informatiques en France ?

47. Tout d'abord, le débat judiciaire nous semble loin d'être clos<sup>26</sup> parce que l'on ne peut imaginer que la Cour de cassation persiste à retenir l'insécabilité des messageries électroniques. Peut-être l'exemple de la Commission européenne sera-t-il plus parlant pour elle que toutes les démonstrations qui ont été faites par des spécialistes de la question dans les pourvois qui lui étaient soumis.

48. En outre, la Cour elle-même souligne dans la plupart de ses arrêts qu'il appartient au juge *"de vérifier concrètement, en se référant au procès-verbal et à l'inventaire des opérations la régularité de ces dernières et d'ordonner, le cas échéant, la restitution des documents qu'il estimait appréhendés irrégulièrement ou en violation des droits de la défense"*<sup>27</sup>. La faculté des juges des libertés d'annuler des opérations d'expertise informatique en présence d'irrégularités avérées est donc préservée, pour autant que les entreprises aient fait inscrire des réserves suffisantes à ce procès-verbal ou directement auprès des officiers de police judiciaire.

49. Par ailleurs, les observateurs avisés ont noté que la Cour de cassation avait pris soin, dans un de ces arrêts, de reproduire une ordonnance déférée, selon laquelle, *"dès lors que les enquêteurs soupçonnent l'existence de documents incluant des données personnelles ou couvertes par le secret des correspondances d'avocat, ou si l'occupant des lieux les alerte, ils placent les données sous scellés et il est ultérieurement procédé, sous le contrôle du juge à leur restitution"*<sup>28</sup>. Si le placement sous scellés fermés n'est qu'une faculté pour les enquêteurs en l'absence de demande particulière de l'entreprise, la Cour de cassation ne nous semble pas avoir eu pour l'heure à traiter d'un cas où l'entreprise avait formulé une telle demande auprès des enquêteurs, voire en faisant intervenir le magistrat de permanence. Sa réponse pourrait alors être différente.

50. Mais l'avenir pourrait ne pas seulement être judiciaire.

51. Tout d'abord, l'Autorité de la concurrence sollicite elle-même le renforcement de ses pouvoirs d'enquête dans le cadre du projet de loi relatif à la consommation qui devrait être introduit en juin 2013 et traite, au-delà de l'action de groupe, de plusieurs modifications aux articles L. 450-1 et suivants. Parmi les renforcements demandés, le gouvernement propose entre autres de prévoir un droit d'accès aux logiciels et données stockées dans le cadre d'enquêtes simples pour le contrôle d'opérations faisant appel à l'informatique<sup>29</sup>. Les parlementaires qui seront saisis du projet devraient, dans ces conditions, souhaiter revoir la totalité de la question de l'équilibre des moyens d'investigation informatique des agents de l'Autorité et de la DGCCRF.

52. Ensuite, à l'heure où les procédures d'enquête nationales et européennes sont plus que jamais liées (enquêtes réalisées par une autorité nationale à la demande d'une autre autorité nationale ou de la Commission européenne, transfert d'un dossier d'une autorité nationale à la Commission) il est permis de penser que l'Autorité de la concurrence et la DGCCRF auront de plus en plus de difficulté à justifier le maintien d'une méthodologie spécifique n'assurant pas le même niveau de protection des droits.

53. Il pourrait donc bien y avoir de nouveau un peu de lumière au bout du tunnel, les efforts de rapprochement entre les procédures d'enquête mises en œuvre au sein de l'Union européenne désignant une voie toute tracée à l'Autorité et à la DGCCRF pour faire évoluer leur méthodologie sans pour autant devoir envisager une réforme qui serait susceptible de remettre en cause directement les saisies opérées dans les affaires pendantes. ■

24 <http://www.internationalcompetitionnetwork.org/uploads/library/doc627.pdf>.

25 Code de bonnes pratiques précité, bonne pratique 8.3.

26 Sans compter les évolutions possibles au niveau de la Cour européenne des droits de l'homme et/ou de la Cour de justice de l'Union européenne.

27 V. par ex., Cass. crim., 11 janvier 2012, pourvoi n° 10-88.197 e.a.

28 Cass. crim., 29 juin 2011, pourvoi n° 10-85.479.

29 Article 50 de l'avant-projet de loi du 25 mars 2013.