DROIT & NOUVELLES TECHNOLOGIES

Présente :

INVESTIGATIONS JUDICIAIRES EN MATIERE D'USAGE ILLICITE DE PROGRAMMES ET/OU DE DONNEES

Par

Luc Golvers

Expert judiciaire en informatique auprès de Tribunaux

Maître de Conférences à l'Université Libre de BRUXELLES

Président du Club de la Sécurité Informatique Belge (CLUSIB Asbl).

Date de mise en ligne : 9 février 2004

INVESTIGATIONS JUDICIAIRES EN MATIERE D'USAGE ILLICITE DE PROGRAMMES ET/OU DE DONNEES

ir. Luc GOLVERS, M.B.A.

Expert judiciaire en informatique auprès de Tribunaux

Maître de Conférences à l'Université Libre de BRUXELLES

Président du Club de la Sécurité Informatique Belge (CLUSIB A.s.b.l.).

SYNTHESE

L'utilisation illicite de copies pirates de logiciels standards, la contrefaçon de logiciels et le vol de données sont des pratiques qui exposent leurs auteurs aux risques de poursuites pénales ou d'actions civiles en cessation et indemnisation du préjudice subi.

Notre étude présente les problèmes pratiques rencontrés sur le terrain lors de l'exécution de saisie-descriptions en matière de contrefaçon de logiciels et de données. Elle décrit le vécu d'un expert judiciaire en informatique dans ce type de mission et reflète donc la vue d'un technicien et non celle d'un juriste.

1. L'intentement de l'action

Le titulaire des droits intellectuels relatifs à un logiciel ou à une base de données peut être informé par une multitude de canaux d'une violation suspectée de ses droits.

Le titulaire des droits peut observer la mise sur le marché de copies plus ou moins serviles de ses produits. Il peut également être informé de ces agissements par des canaux indirects, comme les distributeurs officiels de ses produits qui constatent sur le terrain l'utilisation de copies illicites. Il arrive également que des employés, animés d'un esprit de revanche ou de ressentiment à l'égard de leur employeur, dénoncent les pratiques illicites de ce dernier.

Les éditeurs de logiciels ou les associations de lutte contre le piratage mènent des politiques actives de recherche des pratiques frauduleuses. Elles disposent d'une diversité de techniques qui leur permettent d'avoir leur attention attirée sur des pratiques illicites ou suspectes.

Dès l'instant où un acte de piratage ou de contrefaçon est soit établi, soit considéré comme très probable en raison d'éléments permettant d'avoir une suspicion fondée, il

importera de choisir la procédure judiciaire permettant éventuellement d'établir la matérialité des faits incriminés ou suspectés.

2. La voie pénale ou civile

Dans certains cas, la contrefaçon de logiciels est une infraction pénale qui expose ses auteurs à des poursuites judiciaires.

Deux voies s'offrent au titulaire des droits d'auteur sur un logiciel ou une base de données : soit la procédure civile de saisie-description, qui nécessite le recours au Juge des saisies, soit la procédure pénale, concrétisée par le dépôt d'une plainte auprès des autorités judiciaires.

Chacune de ces voies présente des avantages et des inconvénients.

La procédure civile de saisie-description permet de faire procéder dans des délais fort courts au constat de l'éventuelle utilisation abusive ou de la commercialisation de contrefaçons. Cette procédure offre en outre l'avantage de rester sous le contrôle de la partie requérante. Dans la très grande majorité des saisie-descriptions exécutées par l'auteur, les parties ont amiablement mis un terme au litige qui les opposait, le plus souvent dans un délai bref après l'intentement de l'action. Le choix de la procédure civile de saisie-description n'obère en rien la faculté de déposer une plainte pénale contre les auteurs des faits délictueux. Cette dernière voie est parfois choisie par ceux qui, confrontés à des récidivistes de la contrefaçon, estiment qu'une condamnation pénale et un casier judiciaire présentent à terme un caractère plus dissuasif qu'une procédure civile.

Les réticences vis-à-vis du dépôt d'une plainte pénale proviennent généralement de la crainte de la lenteur de ces procédures et de la perte de contrôle du dossier. Toutefois, dans un certain nombre de situations, la voie pénale pourra en pratique s'avérer nettement plus efficace que la procédure civile.

Un exemple typique concerne le cas d'une entreprise ou organisation suspectée d'utilisation de copies illicites d'un logiciel et qui possède un grand nombre de sites répartis en divers arrondissements judiciaires. Dans pareil cas, la procédure civile impose d'obtenir des jugements exécutoires en ces différents arrondissements, d'avoir autant de huissiers de justice à disposition qu'il n'y a de sites à investiguer et de coordonner parfaitement l'ensemble des opérations. Par contre, les forces de police disposent, de longue date, d'une expérience certaine en matière d'exécution de perquisitions simultanées. Les « Computer Crime Units », réparties sur l'ensemble du territoire, peuvent à cet égard apporter un concours efficace dans ce type d'opération.

Nous avons par exemple vécu une affaire dans le cadre de laquelle deux huissiers de justice devaient signifier simultanément une ordonnance à deux endroits distincts, à savoir le domicile privé d'un titulaire de profession libérale et le bureau où ses collaborateurs travaillaient. Un manque de coordination lors de la signification des ordonnances par les deux huissiers a eu pour effet que le responsable de l'affaire, dès qu'il eut connaissance de la signification, a prévenu ses collaborateurs par téléphone. Ceux-ci

ont immédiatement entrepris d'effacer les logiciels contrefaits, pendant que nous attendions avec l'autre huissier devant la porte du bureau. Cette erreur a entraîné un surcroît de travail considérable pour retrouver les traces partiellement effacées des contrefaçons.

Un autre cas concerne celui où, sur un seul site, un très grand nombre de stations de travail doivent être examinées. Une intervention de ce type requiert un personnel nombreux qu'il est plus facile de réunir dans le cadre d'une opération des forces de police que dans le cadre d'une saisie-description.

La suite de ce document se bornera à décrire le déroulement des seules procédures civiles de saisie-description.

3. De l'importance des requêtes et des dispositifs

La saisie-description est une procédure par laquelle le Juge des saisies désigne un expert judiciaire qu'il charge d'effectuer une mission, dont la portée est très précisément définie et limitée par le dispositif du jugement.

Le Juge des saisies est tenu de rédiger son dispositif sur base de la requête déposée parla partie requérante, le Juge ne pouvant, sous peine de statuer « *ultra petita* », accorder davantage que ce qui a été demandé par la partie requérante. Au contraire, il arrive souvent que le Juge des saisies ne fasse pas droit à l'intégralité des mesures demandées par la partie requérante.

Pour qu'une mission soit pleinement réussie, il est essentiel que le dispositif définisse de manière complète et précise la mission confiée à l'expert, ainsi que les autorisations qui seront conférées à celui-ci pour réaliser sa mission.

La qualité de la requête déposée par le conseil de la partie requérante conditionnera donc grandement la réussite de la saisie-description à exécuter. Il nous est arrivé dans un nombre de cas, heureusement restreints, d'être chargé d'une mission qui, telle que définie par le dispositif, était, presque à coup sûr, vouée à l'échec. Ceci conduit parfois la partie requérante à devoir introduire une requête complémentaire, soit en vue de mieux définir la mission dévolue à l'expert, soit pour lui donner les autorisations indispensables pour mener à bien la mission.

Quand bien même la requête est complète et bien formulée, les Juges des saisies peuvent réagir de façons très variables à l'égard de demandes a priori identiques ou à l'égard d'éléments importants, qui seront décrits ci-après, tels que : l'éventuelle caution à déposer par la partie requérante, l'autorisation de la présence de la requérante et/ou de ses conseils, la mise sous scellés des éléments de contrefaçon, etc.

Si l'indépendance des juges est un principe essentiel dans un régime démocratique, il n'en est pas moins souhaitable qu'il soit fait preuve d'une certaine cohérence au niveau du traitement des requêtes de saisie-description. À défaut, une société qui commercialise ses logiciels dans tout le Royaume risque de ne pas pouvoir imposer le respect de ses droits intellectuels avec la même efficacité dans tous les arrondissements.

Nous aborderons ci-après quelques-uns des points pratiques qu'il importe de préciser dans les requêtes et dispositifs, afin que l'expert puisse mener à bien la tâche qui lui est confiée.

4. Aspects pratiques de l'exécution des saisies-descriptions

4.1 Le ou les lieux d'exécution de la mission.

Le dispositif précise habituellement que l'expert doit exécuter sa mission à une adresse bien précise, qui est celle où le ou les objets prétendument contrefaits sont supposés pouvoir être trouvés.

Il nous est arrivé de nous présenter, en présence de l'Huissier de Justice, à l'adresse indiquée au dispositif pour apprendre que la société avait tout récemment déménagé de quelques centaines de mètres dans la rue. Toutefois, comme le dispositif ne prévoyait pas l'expression anodine « … *et en tous autres endroits et auprès de tout détenteur des objets prétendument contrefaits dans l'arrondissement judiciaire* », la partie requérante en fut quitte pour retourner auprès du Juge des saisies avec une requête amendée pour que la mission puisse être exécutée.

Nonobstant les investigations réalisées par la partie requérante et/ou par l'huissier de justice en préparation de la mission, il arrive bien souvent que l'on découvre, au moment même de la saisie-description, que d'autres lieux devraient recevoir la visite de l'expert en vue d'y rechercher les objets éventuellement contrefaits. Il faut dès lors que le dispositif permette de couvrir ces lieux.

Un exemple vécu concerne le cas où les copies pirates de logiciels standards ont, selon les dires de la partie saisie, été fournies et installées par son fournisseur. Il importe dans ce type de situation de pouvoir remonter la filière et de poursuivre sans délai les opérations de saisie-description auprès du fournisseur peu scrupuleux. On pourrait avancer que si le dispositif n'autorise pas cette visite, la partie requérante peut retourner auprès du Juge des saisies afin d'obtenir cette fois une ordonnance à l'encontre de ce fournisseur. La pratique apprenant toutefois que les informations circulent extrêmement vite, il y a fort à parier que toutes les preuves auront disparu dans l'intervalle.

La limitation aux lieux de l'arrondissement est une limitation inappropriée lorsque l'on est confronté à une société disposant de succursales ou sièges dans une multitude d'arrondissements judiciaires. Tel est typiquement le cas de grandes chaînes de distribution.

Par ailleurs, à une époque où l'informatique devient de plus en plus mobile, il importe quelquefois de pouvoir investiguer des ordinateurs portables qui se trouvent dans les véhicules des responsables de l'entreprise, parfois situés sur la voie publique, juste devant le siège de l'entreprise. Si l'ordonnance ne couvre pas ce cas précis, l'expert ne pourra faire porter ses investigations sur ces ordinateurs portables.

4.2 L'interdiction de communication à des tiers de l'action en cours

Il importe que la requête et le dispositif comportent une formule telle que: « *interdisons à la société XYZ d'avertir ses préposés et/ou mandataires de la saisie-description, de la présence de l'expert et de l'huissier et/ou de l'expert judiciaire afin d'éviter qu'en toute hâte des programmes et/ou fichiers, qui pourraient prouver la contrefaçon, ne soient effacés* ».

En effet, nous avons été confrontés à diverses reprises au fait que lorsqu'une société ou une organisation prend conscience de la portée de l'opération en cours et sait qu'elle dispose de copies illicites d'un programme ou de données, elle avertisse en panique une série de ses collaborateurs, qui s'évertueront à la hâte d'effacer ou de désinstaller les objets contrefaits.

Il est difficile de ne pas laisser diverses traces de ces opérations d'effacement réalisées à la hâte. Toutefois, la tâche de l'expert s'en trouve considérablement compliquée et accrue.

La nature des opérations à effectuer par l'expert pour recouvrer les éléments de preuve effacés est souvent lourde, de telle sorte que ce travail ne pourra s'effectuer sur place le jour même. Il importe dès lors que l'expert puisse soit emporter les équipements pour réaliser en son cabinet avec les outils appropriés les investigations requises, soit faire mettre les équipements sous scellés pour réaliser ces investigations par la suite.

Il peut donc être utile de prévoir dans la requête et le dispositif une clause telle que : *« Interdisons à la société XYZ elle-même, ses préposés et/ou mandataires de gêner de quelque manière le travail de l'expert en effaçant par exemple des programmes ou fichiers à partir du moment de la signification de la présente ordonnance, sous peine d'une astreinte de € … par ordinateur/station de travail pour lesquels l'expert serait gêné de la sorte dans ses travaux* ».

Dans cet ordre d'idée, on relèvera que l'huissier a, dans le cadre d'une saisie-description, essentiellement pour tâche de permettre à l'expert de réaliser sa mission et d'éventuellement acter dans son procès-verbal certains faits ou éléments importants. En dehors de cela, l'huissier de justice ne joue pas à proprement parler un rôle actif dans ce type de mission. Un stade crucial est toutefois celui de la signification.

Une saisie-description se doit, par essence, d'avoir un effet de surprise. Afin d'éviter que les membres du personnel de la société auprès de laquelle la saisie est effectuée n'aient des réactions de panique et ne commencent à tenter d'effacer les preuves, il importe que la signification s'opère en un laps de temps très court. Dès que la signification est faite, l'expert doit pouvoir entamer sa mission sans retard.

La communication du seul nom de la partie requérante suffit généralement à faire comprendre à la société saisie la nature de l'opération qui va se dérouler. Il faut dès lors éviter qu'avant de signifier l'ordonnance, l'huissier de justice ne se perde en inutiles explications ou encore n'entame une cascade de communications superflues avec un tas d'interlocuteurs. À défaut, au moment où il aura finalement signifié l'ordonnance, instant que l'expert doit attendre pour pouvoir commencer ses opérations, l'entièreté de la société sera au courant de ce qui va se dérouler.

4.3 La présence d'autres personnes que l'expert

L'huissier de justice est le plus souvent accompagné de son témoin, ce qui est par ailleurs requis dès lors que le dispositif prévoit la possibilité d'une mise sous scellés des objets prétendument contrefaits.

L'huissier peut d'office requérir la présence d'un ou plusieurs représentants des forces de l'ordre. Il est exceptionnel, mais cela s'est néanmoins malheureusement produit, que l'intégrité physique de l'expert soit menacée par un représentant de la partie saisie. La présence des forces de l'ordre permet d'éviter ces désagréments. La participation de policiers peut encore être utile à un double titre. En effet, en dehors de l'impact psychologique que leur présence confère, les représentants des forces de l'ordre peuvent veiller à ce que les membres du personnel de la société saisie cessent de travailler sur les ordinateurs à investiguer. Ceci permet de limiter le risque d'un effacement à la hâte, mentionné plus haut.

Lorsque la partie saisie dispose de nombreux ordinateurs, répartis en de multiples locaux, il est souhaitable que l'expert puisse se faire assister par une équipe de collaborateurs, qui opéreront sous ses ordres et sa direction. L'expert ne pouvant être présent dans tous les bureaux à la fois, ces collaborateurs permettront notamment de contrôler que les membres du personnel de la société visitée n'effectuent pas de manipulations indésirables sur les ordinateurs. Ils pourront par ailleurs aider l'expert dans la collecte des preuves requises pour l'accomplissement de sa mission.

Un thème particulièrement sensible est la présence éventuelle d'un ou plusieurs représentants de la partie requérante lors de la saisie-description. Cette présence n'est possible que si elle est explicitement autorisée par le Juge des saisies. Nous avons pu constater que dans certains arrondissements judiciaires, la présence de représentants de la partie requérante est presque systématiquement refusée. Or, cette présence peut s'avérer extrêmement utile, voire même indispensable, pour permettre à l'expert de mener à bien sa mission car dans certains domaines techniques très pointus, la présence de ces représentants permet de fournir immédiatement des renseignements techniques dont l'expert a besoin. Ces représentants peuvent aussi attirer l'attention de l'expert sur certains éléments qui sinon auraient pu échapper à sa vigilance, du fait de sa moins grande familiarisation avec le produit, dont une éventuelle contrefaçon est recherchée.

Il est dès lors regrettable que cette présence soit refusée dans les cas où elle apporte une réelle valeur ajoutée. Ceci justifie largement le besoin d'une certaine harmonisation et la nécessité pour certains juges de reconsidérer leur attitude à l'égard de ce type de demande.

Bien entendu, il faut que l'expert judiciaire veille scrupuleusement à ce que l'assistance d'un représentant de la requérante se borne au seul apport technique dont il peut avoir besoin sur le terrain. Lorsque les parties requérante et saisie sont des concurrents, le risque d'espionnage industriel par le biais d'une saisie-description est un danger non négligeable, qui justifiera dans le chef de l'expert une vigilance toute particulière. Il devra s'assurer de ce qu'à aucun moment, un éventuel transfert de secrets de l'entreprise saisie ne soit effectué vers la partie requérante, que ce soit lors des opérations sur place ou ultérieurement par les informations figurant dans le rapport d'expertise.

Dans certains cas, comme la recherche de copies pirates d'un logiciel standard, ce risque d'espionnage industriel est inexistant. Il n'est guère compréhensible que cette présence soit refusée. Afin d'éviter de prêter le flanc au reproche d'espionnage industriel ou de s'exposer à d'autres critiques, il importe que les représentants de la requérante, autorisés à être présents sur place, s'abstiennent de tout rôle actif. Ainsi, ils ne doivent en aucun cas manipuler les systèmes informatiques et doivent toujours rester aux côtés de l'expert et limiter leur rôle à répondre aux questions de celui-ci et éventuellement à formuler des suggestions.

Une autre personne qui peut être autorisée à être présente lors de la saisie-description est l'avocat de la partie requérante. Cette présence est un sujet pour le moins controversé.

Ne pouvant témoigner dans les causes qu'il instruit, un avocat ne pourra ni conclure ni plaider sur des évènements auxquels il a lui-même participé. Par conséquent, si un incident se produit ou si tout simplement la partie saisie reproche une exécution au-delà des limites de l'ordonnance, l'avocat de la partie requérante pourrait être mis directement en cause et ainsi être amené à éventuellement devoir défendre sa propre cause, ce qui est assurément ni souhaitable ni l'objectif poursuivi.

En outre, un des principes essentiels de l'expertise est le strict respect des droits de la défense, qui veut notamment que si une partie est assistée de son conseil, l'autre le soit également. Dès lors que seul le conseil de la partie requérante serait présent sur place, un déséquilibre potentiel peut se créer vis-à-vis de la partie visitée.

Bien souvent, dès la signification de l'ordonnance de saisie-description, la partie saisie prend contact avec son conseil, qui souhaitera soit parler à l'expert, soit se rendre sous le bénéfice de l'urgence sur les lieux de la saisie. Dans ce dernier cas, l'équilibre entre parties ne pourra s'opérer que si le conseil de la partie requérante est également présent sur les lieux. À diverses reprises, nous avons pu observer que le conseil de la requérante pouvait ainsi, de façon dépassionnée, expliquer le fondement juridique de l'action au conseil de la partie saisie et convaincre ce dernier, lorsqu'il n'est pas familiarisé avec la procédure de saisie-description, de la nécessité de laisser l'expert exécuter sa mission en toute quiétude.

Nous avons pu observer que lorsque le conseil de la partie requérante est autorisé à être présent sur les lieux, il se confine le plus souvent, comme il se doit, à un rôle totalement passif au niveau du déroulement de l'action elle-même. Il lui arrive toutefois de jouer un rôle dans la résolution de problèmes juridiques. En effet, les dispositifs laissent parfois des questions ouvertes, auxquelles il convient de répondre sur base des règles de droit, qui ne sont pas du ressort de l'expert. Par ailleurs, on ne perdra pas de vue que l'exécution de la saisie-description se fait aux risques et périls de la partie requérante et qu'en fonction des circonstances, celle-ci peut, avec l'aide de son conseil, décider d'aller plus ou moins loin dans l'exécution des mesures autorisées par le Juge des saisies.

On arguera, bien entendu, que la présence physique du conseil de la partie requérante sur les lieux de la saisie n'est pas indispensable pour jouer le rôle décrit ci-dessus. Il

peut veiller à se rendre disponible et/ou appelable pendant la durée d'exécution des opérations, à la planification desquelles il aura participé.

Au terme d'une saisie-description, où la partie requérante est représentée, il arrive qu'un dialogue s'établisse entre parties en vue de rechercher une solution amiable au litige. Dans ce cas, un contact devra s'établir entre les conseils des deux parties. Ceci se fera d'autant plus facilement que le conseil de la partie requérante est déjà présent sur place. Celui-ci attendra que le conseil de la partie saisie puisse également se rendre sur place pour entamer des négociations en vue d'un règlement amiable. Nous avons pu observer que plus de 90 % des saisie-descriptions concernant la possession de copies pirates de logiciels standards se clôturent par un accord amiable, conclu le plus souvent le jour même de l'action.

Toutefois, et même lorsque les négociations en vue d'un règlement amiable ont été menées avec le conseil de la partie visitée, il est, dans de très rares cas, arrivé que l'accord conclu le jour même soit contesté par la suite en justice par la partie visitée, sous le motif que cet accord a été obtenu sous l'effet du choc prétendument produit par la saisie-description, voire le risque que le système informatique soit mis sous scellés, ce dont question ci-après. Dans les cas dont nous avons connaissance, ces recours n'ont cependant pas abouti à remettre en cause ou à modifier les termes des transactions visées.

Lorsque la saisie-description concerne des logiciels non standard ou des bases de données, la situation est différente dans la mesure où il peut y avoir matière à discussion quant à la portée et la nature de l'éventuelle contrefaçon. En effet, si l'expert peut sur le terrain, au terme de ses constats, attester de la présence d'éventuelles copies pirates de logiciels standards, il n'en est pas de même pour des contrefaçons d'autres logiciels ou autres objets, qui ne sont pas toujours des copies serviles. Il n'incombe en effet pas à l'expert de déterminer s'il y a contrefaçon mais uniquement de décrire les objets prétendument contrefaits. Seul le Tribunal pourra statuer quant au fait qu'il y ait contrefaçon ou non.

4.4 La protection d'ordinateurs ou de fichiers par mots de passe

Il importe que la requête et le dispositif comportent, en matière d'examen de systèmes informatiques, une clause telle que : « *Interdisons à la société XYZ, ses préposés et/ou mandataires de rendre les ordinateurs, ordinateurs portables ou stations de travail, inaccessibles par l'usage de mots de passe et les obligeons, au cas où des mots de passe seraient utilisés, de les communiquer à l'expert, sous peine d'une astreinte de € … par ordinateur/station de travail pour lequel l'expert judiciaire serait gêné dans ses travaux par l'usage de ces mots de passe ».*

En effet, si moyennant l'utilisation des outils adéquats et parfois un temps important, il est possible de casser les systèmes de protection de nombre d'ordinateurs et de logiciels, le but d'une saisie-description n'est pas de transformer l'examen de l'expert en un exercice de contournement de systèmes de protection ou de perçage de mots de passe. Il importe dès lors que la partie saisie ait l'obligation de communiquer les dits mots de passe à l'expert, sous peine d'une astreinte.

4.5 Les astreintes

De manière assez surprenante, nombre de dispositifs définissent des interdictions qui s'appliquent à la partie saisie mais ne sanctionnent pas leur non-respect par une astreinte.

Dans pareil cas, l'expert ne dispose d'aucun moyen de pression pour forcer l'entreprise saisie à respecter ces points du dispositif. Il pourra tout au plus faire constater la chose par l'huissier, qui pourra l'acter dans son procès-verbal. Toutefois, l'expert sera, le cas échéant, considérablement gêné, voire empêché de réaliser sa mission.

4.6 Les visites répétées de l'expert

En cas de saisie-description concernant la contrefaçon de programmes ou de données, il importe que l'expert puisse « figer » la situation lors de sa première visite sur les lieux. À défaut, il y aura un risque considérable que les preuves recherchées à l'occasion d'une deuxième visite auront disparu dans l'intervalle.

Toutefois, la détermination de l'étendue de la contrefaçon ou la nécessité de procéder à des investigations techniques complémentaires peuvent avoir pour effet que l'expert doive se rendre à plusieurs reprises dans les locaux de l'entreprise saisie.

Il importe dès lors que le dispositif précise que l'expert *« puisse se rendre sur les lieux autant de fois que requis pour l'exécution de sa mission »*.

4.7 La communication de documents

Bien qu'il arrive dans de rares cas, résultant principalement d'une omission au stade de la requête, de devoir se limiter à la seule description d'objets contrefaits, dans la quasi-totalité des cas, l'expert est également amené à devoir déterminer l'étendue ou l'importance, ainsi que l'origine de la contrefaçon.

Ceci conduit l'expert à devoir accéder à des documents administratifs et comptables, comme des licences, des factures, etc.

Ces documents ne sont pas toujours disponibles sur place. Ils peuvent le cas échéant être conservés par une fiduciaire comptable ou au siège de la société-mère. D'où la nécessité susmentionnée pour l'expert de pouvoir se rendre sur place autant de fois que requis pour l'accomplissement de sa mission.

L'expert peut également demander à l'entreprise de mettre ces éléments à sa disposition. Dans ce cas, il importe que le dispositif précise le délai raisonnable dans lequel l'entreprise doit communiquer ces pièces à l'expert, de même qu'une astreinte définie par jour de non-respect du délai de communication.

Dans d'autres cas, l'expert peut être autorisé à emporter les pièces administratives et comptables pour en prendre une copie en ses bureaux. Il importe alors que l'expert puisse disposer d'un délai raisonnable en fonction du volume concerné pour réaliser cette tâche. Celui-ci peut être de 1 ou 2 jours ouvrables et non de 24 ou 48 heures,

comme précisé dans certains dispositifs car cela peut poser de sérieux problèmes lorsque la saisie-description s'effectue juste avant un week-end ou un congé. En dehors de ces prestations imposées hors jours normaux de travail, se pose, bien entendu, le problème de la preuve de la restitution des pièces par l'expert dans le délai imparti !

4.8 La mise sous scellés

La mise sous scellés des éléments de la contrefaçon est un des thèmes délicats de la saisie-description en matière informatique. Mises à part la très vaste majorité des saisie-descriptions en matière de piratage de logiciels standards qui se terminent par la conclusion d'une transaction le jour même de la saisie-description, le problème de la conservation des preuves des éventuelles contrefaçons se pose de manière aiguë.

Lorsqu'en l'absence de règlement amiable, l'expert est amené à devoir rédiger son rapport, ce dernier devra pouvoir faire l'objet d'une éventuelle contre-expertise. Il n'est pas rare que la partie saisie émette, avant ou même après le dépôt du rapport, diverses remarques qui demanderont d'éventuels examens complémentaires de la part de l'expert. La constatation de la présence d'une ou plusieurs copies pirates d'un logiciel standard requiert bien plus qu'une simple impression d'écran avec un numéro de licence attestant de la présence de tel ou tel logiciel. Il faut donc absolument que l'état des systèmes informatiques, au moment de la saisie-description, soit figé et préservé.

En effet, de nombreux éléments sont susceptibles de devoir être exploités par l'expert pour établir son rapport : des données figurant dans des fichiers du système d'exploitation (p.ex. dans le fichier « *Registry* » de Windows) ou dans des fichiers aux extensions de type « *.ini* », des dates de création de catalogues de fichiers parfois utiles pour déterminer les dates d'installation de logiciels, les références vers les fichiers récemment accédés pour démontrer une éventuelle utilisation récente du ou des logiciel(s), la présence de fichiers créés par le(s) logiciel(s) pour établir la date à laquelle remonte l'utilisation des copies pirates, etc. La situation est encore davantage compliquée lorsqu'on a tenté de désinstaller ou d'effacer des copies illicites d'un logiciel.

Afin de lui permettre de rédiger un rapport complet et exact et de répondre à toutes les questions que les parties requérante et saisie, ainsi que le Tribunal, pourraient lui poser, l'expert doit par conséquent avoir le souci de prendre une copie complète et conforme « bit par bit » du ou des disques durs du ou des système(s) investigué(s). Une telle opération est une opération extrêmement onéreuse en temps, qu'il est impossible de réaliser le jour de la saisie-description sur un nombre de machines dépassant quelques unités. Autrement dit, l'expert ne sera pas dans la possibilité matérielle de réaliser ces copies « images conformes » le jour même de la saisie-description.

Il importe de préciser qu'une copie conforme « bit par bit » se distingue d'une copie de sauvegarde logique, encore appelée « back up ». En effet, la copie conforme est une image complète du premier au dernier bit du disque. Une telle copie est essentielle car elle permettra de révéler des éléments qui n'apparaîtraient pas avec un back up ordinaire. Il en va ainsi des preuves que la partie saisie aurait tenté de faire disparaître par un effacement ou une désinstallation à la hâte. Une copie conforme prendra généralement beaucoup plus de temps qu'un simple back up.

Pour préserver les preuves sans risque d'altération, il s'impose donc de mettre les systèmes litigieux sous scellés. Cette opération a donc avant tout un but probatoire, c'est-à-dire de préserver l'intégrité des éléments de preuve. Elle se distingue en cela des saisies dites « réelles », dont le but premier est de faire cesser la commercialisation ou l'utilisation de contrefaçons.

Cette décision de mise sous scellés est, bien entendu, lourde de conséquences car elle risque d'entraîner des désagréments réels pour l'entreprise saisie. Elle ne peut être réalisée que si le dispositif l'autorise. Dans le cas contraire, si l'expert aura généralement la possibilité de collecter les preuves essentielles lui permettant de rédiger son rapport, ce dernier ne reposera pas sur les mêmes assises solides que si l'expert avait pu mettre les systèmes sous scellés et/ou prendre une copie complète des systèmes litigieux.

Il arrive régulièrement que le dispositif précise : « *ordonnons la mise sous scellés des logiciels et fichiers prétendument contrefaits et des supports d'information, sur lesquels ceux-ci se trouvent ».* Pareille formulation ne souffre pas d'interprétation. Toutefois, certains dispositifs contiennent la formulation suivante : « *autorisons l'expert à procéder à la mise sous scellés…*». Dans pareil cas, il n'est pas rare que la partie saisie considère que la mise sous scellés relève du libre-arbitre de l'expert. Rien n'est moins vrai, ce qui n'empêche que c'est l'expert qui subira, sur le terrain et de plein fouet, les pressions de l'entreprise saisie pour que cette mise sous scellés n'ait pas lieu. C'est, bien entendu, la partie requérante et non l'expert, qui a la seule responsabilité de l'exécution de l'ordonnance et donc de faire procéder ou non à la mise sous scellés. L'expert pourra éclairer la partie requérante sur la nécessité de poser des scellés tout en mettant celle-ci devant ses responsabilités face à la décision finale.

D'un point de vue pragmatique, il importe également que le dispositif prévoie que ce soit les ordinateurs contenant les éléments contrefaits qui soient mis sous scellés et non simplement les supports magnétiques. En effet, si l'on interprète cette dernière formulation de façon restrictive, cela pourrait impliquer que l'expert doive, lors de la saisie-description, se mettre à démonter physiquement des disques dans toute une série de PC's. Pareille opération comporte des risques, sans compter le temps considérable qu'elle peut prendre. Elle doit donc être évitée à tout prix.

Il est vraisemblable de considérer que le Juge des saisies ordonnant une mise sous scellés vise en principe uniquement les logiciels contrefaits. Toutefois, la difficulté pratique est que l'on ne peut mettre sous scellés une partie seulement d'un disque dur. Dès lors, si on met sous scellés un ordinateur ou un disque dur contenant des logiciels contrefaits, on mettra également sous scellés les autres logiciels, éventuellement licites, et les données qu'ils contiendraient. Contrairement à un entrepôt où se trouveraient des marchandises contrefaites et qu'il serait possible de mettre séparément sous scellés, dans le domaine informatique, on ne peut isoler une partie de l'entrepôt. En mettant un ordinateur sous scellés, c'est comme si on mettait l'entièreté d'un l'entrepôt sous scellés. Il importe donc de bien mesurer les conséquences et la portée de pareille mesure.

Dans certains cas, il arrive que le dispositif ordonne la mise sous scellés « *à condition que le fonctionnement de l'entreprise n'en soit pas rendu impossible* ». Une telle formulation est particulièrement ambiguë et problématique sur le terrain. En effet, chaque entreprise se devrait de disposer d'un plan de continuité lui permettant de faire face à des

incidents catastrophiques, comme le vol ou l'incendie de ses ordinateurs. Dans ces situations, l'entreprise est tout autant privée de ses systèmes informatiques. Même si l'entreprise aurait bien tort de ne pas se doter de pareils plans de continuité, il ne s'agit bien entendu pas d'une obligation légale et d'aucuns estiment que l'on ne peut sanctionner une entreprise de ne pas l'avoir fait.

Rien n'exclut qu'une entreprise, confrontée à ce genre de situation, ne procède à la location ou à l'acquisition de matériel de remplacement, pendant le temps où les ordinateurs sont mis sous scellés. Cela suppose bien sûr que l'entreprise dispose de copies de sécurité de ses données. Le contraire témoignerait d'une gestion particulièrement légère et irresponsable ! Le cas échéant, ces données pourront être transférées, sous le contrôle de l'expert, du système original mis sous scellés vers le système de remplacement. Bien entendu, ce type de travail, qui empêche la paralysie de l'entreprise, prend du temps et grève les frais d'expertise.

La mise sous scellés fait l'objet d'une vive opposition de la part de certains qui y voient principalement un moyen de pression utilisé par la partie requérante pour tenter de contraindre la partie saisie à conclure le plus rapidement possible un règlement transactionnel, dans des conditions qui lui seraient plus favorables que si les équipements n'étaient pas mis sous scellés.

Il s'agit d'une vision tronquée de la réalité. Ayant pratiqué un nombre élevé de saisie-descriptions, il nous est maintes fois arrivé de devoir répondre après la saisie-description à des questions, parfois très pointues, pour lesquelles seul un accès aux équipements litigieux permettait d'apporter la réponse. Au même titre que dans une procédure pénale, où les pièces à conviction sont conservées en l'état jusqu'au terme de la procédure, il importe que les preuves en matière de contrefaçons informatiques soient conservées sans possibilité de les altérer.

Une solution que nous préconisons, mais que nous n'avons pas encore rencontrée dans des dispositifs, consisterait donc à ordonner la mise sous scellés mais ensuite à permettre à l'expert de procéder à la prise des copies « images conformes » aussitôt après, afin qu'il puisse lever la saisie des matériels concernés dans les jours qui suivent la saisie-description. Ceci aurait pour effet de ne paralyser que temporairement l'entreprise en veillant à prendre d'abord les copies des systèmes prioritaires, sur base des indications fournies par la partie saisie. Toutefois, il faut se rendre compte que ce genre d'opération est chronophage. Cela augmentera inévitablement les frais d'expertise, mais ceux-ci seront en finale répercutés sur la partie qui serait reconnue coupable de contrefaçon.

Considérant parfois que la mise sous scellés devrait se borner à rendre inutilisables ou inaccessibles les seuls logiciels argués de contrefaçons, il n'est pas rare que la partie saisie invite l'expert à désinstaller ou effacer le ou les logiciels litigieux. Une telle option ne peut, bien entendu, être envisagée.

D'abord, de pareils agissements de l'expert auraient pour effet de modifier les systèmes qu'il est censé examiner, ce qui pourrait aboutir à la mise en cause de la responsabilité de l'expert et de la partie requérante. À juste titre, un des principes de base de

l'expertise est précisément que les opérations réalisées par l'expert ne devraient pas, dans toute la mesure du possible, apporter de modifications aux pièces à conviction.

Ensuite, cela reviendrait à demander à l'expert d'effacer les preuves que sa mission lui demande précisément de collecter. Une contre-expertise ne pourrait conclure qu'au fait que les logiciels contrefaits ne se trouvent pas sur le système en question, et pour cause, puisque l'expert lui-même les aurait effacés !

Tout cela concourt à démontrer la nécessité de pouvoir prendre des copies « conformes », bit par bit, des disques durs des systèmes litigieux, ce qui, hors cas triviaux, ne peut se faire le jour même de la saisie-description.

5. La preuve de l'utilisation licite de logiciels standards

Nous avons pu constater que nombre d'entreprises n'exercent pas de contrôle et de gestion de leur parc de logiciels installés. Elles ne possèdent pas d'inventaire détaillé des logiciels installés sur leurs divers ordinateurs. Par ailleurs, elles éprouvent souvent de grandes difficultés à rassembler les preuves susceptibles de montrer qu'elles possèdent les droits d'utilisation des dits logiciels. La licéité d'utilisation des logiciels devra être prouvée par un ensemble de moyens comme la production des licences, des factures d'acquisition, des preuves d'enregistrements des logiciels auprès des éditeurs, etc.

Nous ne pouvons que recommander aux entreprises de maintenir un inventaire permanent des logiciels installés. Il existe maints outils pour réaliser cet inventaire de manière permanente et automatisée.

6. La protection du logiciel par ses auteurs

Les auteurs de logiciels ne prennent pas toujours toutes les précautions voulues pour protéger ceux-ci. On relèvera un ensemble de mesures telles que :

- la preuve de la propriété : une saisie-description ordonnant la comparaison entre un logiciel donné et une éventuelle contrefaçon peut conduire à la conclusion que les deux produits sont quasiment identiques. La question peut toutefois se poser de savoir quel était le produit original. Il importe dès lors de pouvoir prouver que le produit a été soit obtenu par acquisition auprès d'un tiers, soit au terme d'un processus de développement interne dont il faudra prouver la matérialité ;

- le recours au dépôt auprès d'un séquestre des sources du logiciel et de sa documentation technique, à divers moments ;

- des protections contractuelles figurant dans les contrats avec les membres du personnel ou des tiers ayant participé au développement des logiciels ;

- des mesures de contrôles internes visant à limiter les risques d'accès non autorisés aux sources ;

- l'utilisation et le suivi rigoureux de numéros de série des copies de logiciels diffusés en clientèle ;
- le recours à des clefs « hardware », encore appelées « dongle » ;
- des procédures d'activation en ligne des produits ;
- des techniques de « marquage » (watermarking) permettant de faciliter la détection d'éventuelles copies illicites.

7. Les règlements amiables

Comme cela a déjà été indiqué, la très grande majorité des expertises constatant l'utilisation de copies pirates de logiciels débouchent sur des règlements amiables du litige. Ces règlements comportent généralement 3 volets :

- la régularisation des licences des copies utilisées ;
- le paiement d'une indemnité visant à dédommager le titulaire des droits d'auteur du produit pour l'utilisation illicite de ses logiciels par le passé. En cas de logiciels standards, ce poste de dommage s'élève en général à une fois et demi le prix de la licence de chaque produit utilisé illégalement ;
- le paiement par la partie défaillante des frais de procédure et d'expertise.

Lorsque au terme d'une saisie-description, il s'avère que la présence de contrefaçons n'a pu être établie, la partie requérante peut faire l'objet d'une demande, émanant de la partie saisie, d'obtenir réparation du préjudice subi suite à la saisie-description. En effet, l'exécution de la saisie-description causera inévitablement une perte de productivité, car tout ou partie du personnel de la partie saisie aura été empêché de travailler normalement pendant une partie du déroulement des opérations de saisie-description.

* *

*