Note d'observations[3]

Les fournisseurs d'accès à internet, nouveaux gendarmes de la toile ?

I. INTRODUCTION

C'est un lieu commun que d'affirmer que l'avènement des nouvelles technologies ne cesse, depuis deux décennies au moins, de bouleverser notre quotidien. La procédure pénale – qui est toujours régie par un code qui a vu le jour en 1867 – a du mal à s'adapter à ces changements. Le législateur tente, par à-coups, de rattraper le retard et d'anticiper les évolutions. L'arrêt publié nous donne l'occasion de démontrer comment une disposition qui avait été imaginée en 2000 pour combler une lacune du Code d'instruction criminelle (rendre possible la saisie d'éléments incorporels, soit des données informatiques) est devenue, en 2013, le fer de lance dans la lutte contre la criminalité liée au développement de sites permettant le partage illégal de fichiers de manière mutualisée. Le problème est que cette métamorphose se fait au détriment des fournisseurs d'accès à internet qui se retrouvent «propulsés» aux premières loges de la procédure pénale, se voyant imposer de jouer le rôle (ingrat) de sentinelle.

Sur la base de telles prémisses, le lecteur aurait pu s'attendre à ce que pareille situation soit sanctionnée par la Cour de cassation. Et pourtant, elle a trouvé grâce à ses yeux, ainsi que nous allons tenter de vous l'expliquer…

II. EXPOSÉ DES FAITS

La procédure à l'origine de l'arrêt rendu par la Cour de cassation le 22 octobre 2013 concerne une ordonnance prise par un juge d'instruction le 6 avril 2012 en application des articles 39*bis* et 89 du Code d'instruction criminelle. Par cette ordonnance, le juge d'instruction a requis tous les opérateurs et fournisseurs d'accès à Internet, de rendre inaccessible l'accès au contenu hébergé par le serveur associé aux noms de domaine principaux «thepiratebay.org».

Le juge d'instruction enjoint également les opérateurs et fournisseurs d'accès à Internet d'utiliser tous les moyens techniques possibles pour rendre ce contenu inaccessible, dont, à tout le moins, le blocage de tous les noms de domaine qui renvoient au serveur associé au nom de domaine «the piratebay.org».

Pour déterminer la liste des noms de domaine à rendre inaccessibles, le juge d'instruction suggère aux opérateurs et fournisseurs d'accès à Internet d'utiliser le procédé technique de «reverse IP domain check», qui consiste à rechercher tous les noms de domaine qui renvoient à une adresse IP déterminée par le juge, et de l'appliquer ensuite à chaque adresse IP dont il est constaté que l'utilisation par le serveur est associée au nom de domaine principal «thepiratebay.org», afin d'assurer l'accès internet au contenu hébergé par le serveur associé au nom de domaine principal «the piratebay.org». Selon l'ordonnance du juge d'instruction, cette liste de domaines à rendre inaccessibles pourra par ailleurs être déterminée par toute autre constatation technique matérielle, qui établirait qu'un nom de domaine déterminé renvoie au contenu hébergé par le serveur associé au nom de domaine principal «the piratebay.org».

[3] Pierre Monville (avocat, assistant à l'ULg) et Mona Giacometti (avocat, assistante à l'UCL (CRID&P).

Le juge d'instruction requiert finalement les enquêteurs de la *Regional Computer Crime Unit* (RCCU) de Malines et ceux de la *Federal Computer Crime Unit* (FCCU) de constater les noms des domaines à rendre inaccessibles et d'en informer les opérateurs, lesquels sont quant à eux chargés d'informer la RCCU et la FCCU de l'exécution de la mesure ordonnée.

Plusieurs opérateurs et fournisseurs d'accès à internet se sont opposés à l'ordonnance prise par le magistrat instructeur, en déposant, en application de l'article 61*quater* du Code d'instruction criminelle et à défaut d'autre fondement légal plus approprié, une requête visant à obtenir la levée de l'ordonnance du juge d'instruction. À titre subsidiaire, ces opérateurs sollicitaient que la mesure soit limitée dans le temps, qu'il soit précisé qu'ils ne consentiront pas à dresser eux-mêmes la liste des noms de domaine à rendre inaccessibles, et que la mesure technique spécifique à implémenter soit précisée, en plus de prévoir qu'ils seront censés avoir satisfait à la demande dès que la mesure aura été prise.

Le juge d'instruction a rejeté cette requête le 19 juillet 2012. Appel a été interjeté contre l'ordonnance rendue, lequel a été déclaré non fondé par la chambre des mises en accusation, dans un arrêt du 14 février 2013.

C'est à l'encontre de cet arrêt que les fournisseurs d'accès ont introduit un pourvoi en cassation.

III. L'ARTICLE 39*BIS* DU CODE D'INSTRUCTION CRIMINELLE ET LA SAISIE DE DONNÉES INFORMATIQUES

Pour bien comprendre la portée de l'arrêt rendu par la Cour de cassation, il est indispensable de revenir sur l'article 39*bis* du Code d'instruction criminelle qui organise la saisie de données informatiques[4].

Cette disposition, introduite par la loi du 28 novembre 2000 relative à la criminalité informatique[5], visait, avant tout, à permettre aux autorités de poursuites de procéder à la saisie d'éléments incorporels, ce que le libellé de l'article 35 du Code d'instruction criminelle (qui se réfère à la notion de choses) n'autorisait pas[6].

La finalité assignée à l'article 39*bis* du Code d'instruction criminelle était donc de rendre possible et de baliser la saisie de données numériques. La solution technique retenue par le législateur, et qui était fonction de l'environnement technologique du moment, était de décomposer la saisie informatique en deux séquences, soit une copie de données assortie de leur blocage[7].

Il est important de détailler les modalités concrètes de cette nouvelle forme de saisie.

- Quant à son objet tout d'abord : les données concernées par la saisie s'entendent des données stockées dans un système informatique, que ce soit celui qui fait l'objet de la recherche initiale ou le réseau vers lequel le juge d'instruction aurait ordonné une extension de la recherche en application de l'article 88*ter* du Code d'instruction criminelle[8].
- Quant à son déroulement : la saisie se décline, en principe, en deux temps, soit une copie de données assortie de leur blocage. En effet, la simple copie de données informatiques ne correspond pas à une saisie au sens classique du terme, dans la mesure où une telle saisie implique une dépossession du

[4] Cette disposition concerne les saisies opérées par le procureur du Roi, mais également en application de l'article 89 du Code d'instruction criminelle qui y renvoie, aux saisies opérées par le juge d'instruction.

[5] *M.B.*, 3 février 2001, p. 2909.

[6] C. Meunier, «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et de la procédure pénale à l'ère du numérique», *Rev. dr. pén. crim.*, 2001, pp. 611-690, spéc. p. 670.

[7] *Ibid.*

[8] *Ibid.*, pp. 671-672.

titulaire des biens saisis[9] ainsi que le transfert de cette possession aux autorités juridiques saisissantes[10].

Les paragraphes 2 et 3 de l'article 39*bis* imposent ainsi à l'autorité compétente de prendre copie des données informatiques utiles pour les mêmes finalités que celles prévues pour la saisie, avant d'en empêcher l'accès[11]. Copie d'abord, blocage ensuite des données préalablement copiées, telle semble être la logique à laquelle répond la saisie de données informatiques. Il n'entrait cependant pas dans l'esprit du législateur de permettre un blocage de données non préalablement copiées. Le blocage répond à la finalité propre de la saisie, à savoir rendre les données indisponibles après avoir été copiées[12].

- Il faut, à ce propos, distinguer l'empêchement d'accès aux données utiles à la manifestation de la vérité ainsi qu'à celles qui sont susceptibles de confiscation (article 39*bis*, § 3, alinéa 1er, du Code d'instruction criminelle) de l'interdiction d'accès visée à l'article 39*bis*, § 3, alinéa 2 du même article[13].

L'empêchement d'accès – c'est-à-dire le blocage des données – se justifie par la volonté de conserver intact l'original des données afin de permettre la vérification de la concordance de deux versions, si par exemple, le prévenu conteste, devant le juge du fond, la conformité des copies aux originaux[14].

L'interdiction d'accès – c'est-à-dire le retrait des données – a lui pour objet de prévenir autant que possible leur dissémination compte tenu de leur caractère préjudiciable à l'ordre public, ou aux bonnes mœurs, ou du danger qu'elles représentent pour les données ou les systèmes informatiques[15]. L'article 39*bis* admet que les données préalablement copiées soient ainsi retirées du système informatique[16].

- L'article 39*bis*, § 4 prévoit enfin la possibilité pour l'autorité compétente de rendre des données non préalablement copiées inaccessibles, c'est-à-dire de les bloquer dans l'attente du moment où elle sera en mesure d'en prendre copie. Dans une telle hypothèse, le blocage constitue une véritable mise sous scellés des données probantes[17].

L'on constate donc, à l'issue d'un examen sommaire de l'article 39*bis* du Code d'instruction criminelle que cette disposition n'avait aucune vocation à s'appliquer au cas d'espèce soumis à la Cour de cassation, à savoir une réquisition adressée par un juge d'instruction à tous fournisseurs d'accès à Internet de rendre inaccessible l'accès au contenu de domaines.

Non seulement, aucune mesure de copie préalable de données informatiques n'avait été ordonnée par le magistrat instructeur voire n'était à l'ordre du jour mais, en outre, il n'envisageait à aucun moment de procéder à une saisie « pénale » de données informatiques.

9 Sauf lorsque le saisi reçoit la possibilité de continuer à utiliser la chose saisie sans pouvoir s'en déposséder jusqu'à ce qu'il soit statué sur le fond de l'action publique par une décision définitive.

10 C. Meunier, *op. cit.*, p. 670.

11 D. Vandermeersch, O. Klees et F. Rousseau, « Les saisies en matières pénale et de référé pénal », in *Droit pénal et procédure pénale*, Malines, Kluwer, 2006, pp. 59-152, spéc. p. 68.

12 *Ibid.*, p. 69.

13 *Ibid.*

14 C. Meunier, *op. cit.*, p. 674.

15 *Ibid.*, p. 676.

16 *Ibid.*, p. 675.

17 D. Vandermeersch, O. Klees et F. Rousseau, *op. cit.*, p. 71.

IV. EXAMEN DE LA DÉCISION RENDUE PAR LA COUR DE CASSATION

Nous nous proposons d'examiner, par le détail, la décision rendue par la Cour de cassation, laquelle a conclu à un rejet des pourvois. Pour dire vrai, les moyens soulevés par les fournisseurs d'accès à Internet nous semblaient mériter un meilleur sort.

Le premier moyen critiquait le fondement légal de la « saisie » ordonnée par le juge d'instruction, aucune des finalités, telles qu'énoncées par l'article 35 du Code d'instruction criminelle, qu'une telle mesure est censée poursuivre n'étant en l'espèce présente (à savoir la manifestation de la vérité, le recueil des preuves ou une conservation en vue d'une confiscation ultérieure).

La Cour de cassation fait œuvre de législateur puisqu'elle complète le prescrit des articles 35 et 39*bis* du Code d'instruction criminelle, en assignant à la saisie pénale deux nouveaux objectifs, à savoir la cessation d'agissements qui semblent constituer une infraction ou la sauvegarde des intérêts civils.

Certains commentateurs de l'arrêt annoté ont estimé que la référence à la sauvegarde des intérêts civils bien qu'inexistante dans toutes les dispositions du Code d'instruction criminelle relatives à la saisie, n'était en fait pas une première dans le chef de la Cour de cassation qui avait déjà exprimé pareil point de vue dans un arrêt du 25 février 2003[18]. Nous ne sommes pas d'avis qu'un lien aussi étroit puisse être établi entre les deux décisions vu que la Cour suprême n'était saisie, en 2003, que d'un moyen tiré d'une violation de l'article 507 du Code pénal[19] et non d'une violation du prescrit des articles 35 à 39*bis* du Code d'instruction criminelle.

Le second moyen faisait grief à la décision attaquée d'avoir imposé à un fournisseur d'accès à Internet[20] l'obligation de bloquer l'accès au contenu de domaines internet, en application de l'article 39*bis* du Code d'instruction criminelle, alors qu'une telle obligation ne peut être imposée qu'à un fournisseur d'activités d'hébergement, en vertu de la loi du 11 mars 2003 sur certains aspects juridiques des services de l'information (qui à l'époque était d'application[21]).

L'article 20 de cette loi[22] prévoyait, en effet, pour les prestataires qui développent une activité d'hébergement, une obligation de communiquer sur le champ la connaissance qu'ils auraient d'une activité ou information illicite au procureur du Roi, ce dernier pouvant prendre les mesures utiles conformément à l'article 39*bis* du Code d'instruction criminelle. Une procédure similaire existe pour les prestataires d'une activité de stockage sous forme de copie temporaire de données (article 19 de la loi[23]). Par contre, pour l'activité de simple transport, soit celle des fournisseurs d'accès à Internet (article 18 de la loi[24]), rien de tel n'était prévu. Bien plus l'article 21 de la loi[25]

18 K. Schoefs, « Strijd tegen The Pirate Bay over ander boeg gegooid: databeslag toegestaan », note sous Cass., 22 octobre 2013, *T. Strafr.*, 2014, pp. 131-142, spéc. p. 138.

19 Cette disposition punit le saisi ou tous ceux qui auront frauduleusement détruit ou détourné, dans son intérêt, des objets saisis entre ses mains, ainsi que l'époux ou l'épouse qui détruirait, dégraderait, détournerait des biens frappés d'opposition, conformément à l'article 1253*septies* alinéa 2 ou 1280 du Code judiciaire.

20 Service de simple transport d'informations ou fournisseur d'accès à un réseau de communication.

21 Depuis lors, en effet, les dispositions de la loi du 11 mars 2003 ont été intégrées dans le Livre XII du Code de droit économique, voy. la loi du 15 décembre 2013, *M.B.*, 14 janvier 2014, p. 1524.

22 Actuellement article XII.19 du Code de droit économique.

23 Actuellement, article XII.18 du Code de droit économique.

24 Actuellement, article XII.17 du Code de droit économique.

25 Actuellement, article XII.20 du Code de droit économique.

précisait que les prestataires (des trois catégories confondues) n'avaient aucune obligation générale de surveillance des informations qu'ils transmettent ou stockent, ni de rechercher activement des faits ou circonstances révélant des activités illicites.

La Cour de cassation ignore tout simplement l'argument et se cantonne à une lecture autonome de l'article 39*bis* du Code d'instruction criminelle, indiquant au passage que c'est à tort que la violation des dispositions de la loi du 11 mars 2003 était invoquée comme soutènement juridique du moyen.

Dans l'examen des conditions permettant la saisie de données informatiques, la Cour de cassation est tout aussi sélective. Elle se précipite tout d'abord sur le § 4 de l'article 39*bis* du Code d'instruction criminelle qui prévoit la mise sous scellés provisoire des données alors que, il faut le rappeler, cette mesure est subsidiaire à l'impossibilité de procéder à la copie de ces données en application du § 2.

À bien comprendre le raisonnement suivi par la Cour, l'on devrait considérer que l'article 39*bis*, § 4, du Code d'instruction criminelle a toujours eu pour vocation de s'appliquer aux fournisseurs d'accès à Internet.

Et peu importe qu'un tel prestataire soit un tiers par rapport à l'exploitant du site web pirate (celui qui a lui-même stocké ou fait stocker les données), rien ne s'oppose à ce qu'un tel ordre lui soit adressé et ce nonobstant le fait que cette mise sous scellé provisoire aura pour conséquence d'atteindre non pas les gestionnaires des données litigieuses (qui pourrait encore les consulter, les modifier ou les effacer) mais les seuls utilisateurs d'Internet qui n'auront plus accès auxdites données; les moyens techniques appropriés au sens du même § 4 peuvent consister à ordonner à ces fournisseurs d'accès à Internet de rendre inaccessible le serveur hébergeant les données litigieuses.

Finalement, l'on en viendrait presqu'à se demander à quoi peut encore servir le régime de limitation de responsabilités des prestataires intermédiaires mis en place par le législateur de 2003 (chapitre VI de la loi du 11 mars 2003[26]). En effet, tous les prestataires, quelles que soient leurs activités (simple transport, stockage temporaire, hébergement), se retrouvent logés à la même enseigne: ils sont susceptibles de faire l'objet de mesures visées par l'article 39*bis* du Code d'instruction criminelle. Si l'on admet ce constat, il vide l'article 21 de la loi du 11 mars 2003 (devenu l'article XII.20 du Code de droit économique) de toute sa substance.

Les demandeurs en cassation estimaient encore, dans les troisième et quatrième branches de leur deuxième moyen, que les conditions d'application de l'article 39*bis*, § 3, alinéa 2, du Code d'instruction criminelle n'étaient en l'espèce pas réunies vu que:

(1)l'interdiction d'accès est accessoire à la copie des données, or aucune copie des données n'avait été ordonnée;

(2)une telle mesure ne peut être envisagée que dans les hypothèses énumérées limitativement par le Code d'instruction criminelle qui, en l'espèce, n'étaient pas réunies: en effet même si les données litigieuses forment l'objet d'une infraction ou proviennent d'une infraction à la loi sur les droits d'auteur, les autres conditions (contrariété à l'ordre public, aux bonnes mœurs, danger pour l'intégrité des systèmes informatiques ou des données stockées) n'étaient pas présentes.

La juridiction suprême a répondu de manière très laconique à ces moyens en précisant que l'article 39*bis*, § 4, du Code d'instruction criminelle constitue un fondement légal suffi-

[26] Actuellement, chapitre 6 du Livre XII du Code de droit économique.

sant (autonome) à la demande du magistrat instructeur.

Restait alors à la Cour de cassation à écarter le dernier moyen soulevé par les fournisseurs d'accès à Internet, qui s'articulait à nouveau sur la loi du 11 mars 2003 sur certains aspects juridiques des services de l'information dont l'article 21, § 1er[27] prévoit qu'aucune obligation générale de surveillance ne peut leur être imposée. Or, l'ordre adressé par le magistrat instructeur de bloquer par tous les moyens techniques l'accès au contenu hébergé par un serveur associé à un nom de domaine déterminé, sans durée de validité concrète, ni énumération des moyens techniques à mettre en œuvre pour observer l'obligation imposée, ni même les noms de domaine à bloquer, impliquerait une telle obligation de surveillance.

La Cour de cassation répond au moyen en affirmant que tel n'est pas le cas, et en reproduisant le prescrit de l'article 21 de la loi du 11 mars 2003. Difficile de trouver une justification plus tautologique!

V. OBSERVATIONS CRITIQUES

Après l'examen de l'arrêt rendu par la Cour de cassation le 22 octobre 2013, un sentiment mitigé se dégage: quel enseignement peut-on, *in fine*, retenir de la décision annotée?

L'arrêt rendu par la Cour de cassation nous semble, en définitive, ne comporter qu'un message très clair: les fournisseurs d'accès à Internet ont vocation à jouer un rôle de gendarmes de la toile. L'arrêt rendu par la chambre des mises en accusation d'Anvers annonçait la couleur. On peut y lire que «les [fournisseurs d'accès à Internet] sont requis, dans le cadre d'une instruction pénale de fournir leur concours technique afin de mettre un holà aux infractions en matière de droits d'auteurs qui pourraient être commises via Internet, même si l'ordre qui leur est adressé ne crée dans leur chef aucune responsabilité et même s'il n'est pas attendu de leur part qu'aucune infraction subséquente ne puisse être commise».

À l'instar de ce qui a été mis en place par le législateur vis-à-vis des prestataires de services de réseaux de télécommunication, le vrai enjeu est de savoir dans quelles conditions et surtout, dans quelles limites, les prestataires de services liés à l'économie électronique sont tenus de fournir leur concours à une enquête pénale. Pour rappel, en ce qui concerne les services de réseaux de télécommunication, les articles 46*bis* et 88*bis* permettent au procureur du Roi ou au juge d'instruction de requérir tout opérateur de fournir certaines données[28]. Cette obligation de collaboration est motivée par les problèmes qui se posent dans les formes modernes de télécommunication et dans les nouveaux médias comme Internet, où il est effectivement très facile d'utiliser les réseaux de manière anonyme, écrit I. Delbrouck[29]. Cette exigence de collaboration s'exprime encore dans l'obligation imposée aux fournisseurs de services de réseaux de télécommunication d'identifier les utilisateurs[30], la loi exigeant qu'ils prennent les mesures pour pouvoir retrouver les données d'appel de télécommunication (origine, destination, localisation, durée...) d'une part, identifier les utilisateurs qui fournissent ces informations au public d'autre part, et conserver ces renseignements[31].

Aucun cadre légal aussi précis et détaillé n'existe pour les activités des prestataires de

[27] Actuellement, article XII.20 du Code de droit économique.

[28] I. Delbrouck, «Criminalité informatique», *Postal Mémorialis*, septembre 2010, C 362/28.

[29] *Ibid.*, C 362/29.

[30] Voy. article 126 de la loi du 13 juin 2005 relative aux communications électroniques, qui a abrogé l'article 109*ter* E de la loi du 21 mars 1991 portant réforme des entreprises publiques économiques.

[31] I. Delbrouck, *op. cit.*, C 362/29.

services de l'économie électronique. L'arrêt annoté a tenté de remédier à cette lacune de la loi.

Nous nous permettrons de pointer les limites de cette approche et les risques qu'elle comporte en évoquant cinq questions.

1) Y a-t-il détournement de la *ratio legis* de l'article 39*bis* du Code d'instruction criminelle ?

Comme nous l'avons vu, la justification donnée par la Cour de cassation pour considérer que l'ordre émis par le juge d'instruction rentrait bien dans le champ d'application de l'article 39*bis* du Code d'instruction criminelle ne convainc pas. Il tombe sous le sens que le législateur du début des années 2000 n'avait d'autre préoccupation que de rendre possible la saisie de données informatiques. Comme le souligne R. Schoefs[32], il est particulièrement interpellant que la Cour estime qu'il n'est pas relevant que celui qui stocke ou laisse stocker ces données ne puisse plus les consulter, les modifier ni les effacer. Si cela est, en effet, sans importance, la *ratio legis* de l'article 39*bis* (§ 4) est méconnue, puisqu'il vise expressément à garantir l'intégrité des données rendues inaccessibles.

2) Le régime de responsabilité des prestataires liés à l'économie électronique est-il neutralisé ?

Que reste-t-il du régime de responsabilité des prestataires intermédiaires mis en place par le législateur en 2003 ? Certainement pas grand-chose. La protection que les articles 18 et 21 de la loi du 11 mars 2003[33] étaient censés offrir aux fournisseurs d'accès à Internet laisse place à une situation d'insécurité juridique.

La Cour de cassation a beau rappeler qu'aucune obligation de surveillance ne leur est imposée et qu'il n'est pas demandé aux fournisseurs d'accès à Internet de surveiller les informations qu'ils transmettent ou stockent, ni de rechercher activement les informations révélant des activités illicites, il n'en reste pas moins que ces prestataires peuvent désormais être confrontés à des demandes des autorités judiciaires leur ordonnant de rendre inaccessible l'accès au contenu de certains sites, sans limite dans le temps, sans description précise des moyens techniques pour y arriver.

Consciente de la problématique, la chambre des mises en accusation d'Anvers a tenu à préciser que l'obligation ainsi imposée n'est qu'une obligation de moyen et non de résultat, ajoutant que lorsqu'un magistrat instructeur lui demande de bloquer l'accès au contenu hébergé par un serveur associé à un nom de de domaine « par tous les moyens techniques possibles », il exclut que le fournisseur d'accès à Internet soit tenu à l'impossible... Il n'est pas sûr que ceci soit suffisant pour dissiper tout malentendu.

3) Y a-t-il un risque d'instrumentalisation de la procédure pénale ?

En énonçant qu'une saisie de données informatiques (par le biais d'une demande de blocage d'accès à des noms de domaine) peut être ordonnée, notamment, en vue de la cessation d'agissements qui semblent constituer une infraction ou de la sauvegarde des intérêts civils, la Cour de cassation nous semble ouvrir la boîte de Pandore.

Aux yeux de certains commentateurs[34], cette décision constituerait une avancée significative dans la lutte contre les sites pirates puisque les parties préjudiciées peuvent

32 R. Schoefs, *op. cit.*, p. 139.

33 Actuellement, articles XII.17 et XII.20 du Code de droit économique.

34 R. Schoefs, *op. cit.*, p. 137.

désormais envisager d'agir au pénal pour obtenir le blocage de l'accès aux clients de fournisseurs d'accès à Internet, en déposant une plainte avec constitution de partie civile en lieu et place de procédures civiles au résultat incertain contre les plateformes sur lesquelles des fichiers média sont partagés de manière illégale.

Qu'il nous soit permis de ne pas partager ce même élan en évoquant le risque d'une instrumentalisation de la procédure pénale. Pour rappel, l'action publique est définie comme l'action d'intérêt général, née d'un fait qualifié infraction, qui a pour objet la poursuite devant les autorités compétentes, spécialement les cours et tribunaux, dans les formes prescrites par la loi, de la personne prévenue ou accusée de ladite infraction, aux fins d'examiner sa culpabilité, et de lui appliquer, si elle est coupable, les sanctions ou mesures prévues par les lois pénales[35].

Déposer plainte, dans le chef de titulaires de droits de propriété intellectuelle, dans le but (principal) de rendre inaccessible un site internet via un fournisseur d'accès à Internet, ne nous semble pas correspondre à la finalité des poursuites.

Ne pourrait-on s'interroger sur la recevabilité même de la constitution de partie civile qui serait actée dans de telles circonstances ? Il est traditionnellement enseigné qu'à défaut d'intérêt, l'action de la partie préjudiciée est irrecevable, l'intérêt devant être direct, personnel, légitime, né, actuel et découlant d'une infraction[36]. Une constitution de partie civile qui viserait à obtenir du magistrat instructeur une mesure de blocage dirigée non pas contre l'auteur de l'infraction mais bien vis-à-vis du fournisseur d'accès à Internet poserait, dès lors, problème en terme de recevabilité.

4) Les conséquences sur la poursuite de la procédure pénale ont-elles été prises en compte ?

Outre les autres observations critiques émises, le raisonnement suivi par la Cour de cassation nous semble porter en soi les germes qui en sapent le fondement. Si l'on pousse plus loin l'enseignement que les titulaires de droits de propriété intellectuelle peuvent en tirer, à savoir privilégier le recours à la procédure pénale pour faire triompher leurs droits face à des sites permettant le partage illégal de fichiers de manière mutualisée, l'on aboutit irrémédiablement à une impasse, sur le plan procédural.

Il est par exemple malaisé de répondre à une question simple : à quel moment la « saisie » opérée prendra-t-elle fin ? Faut-il rappeler qu'une saisie revêt un caractère provisoire et que sa vocation est soit de se voir transformée en confiscation, soit de cesser ses effets par décision du juge du fond. Or, qu'adviendra-t-il des mesures prises par le magistrat instructeur lorsqu'il aura terminé son instruction ? Devra-t-on considérer que la « saisie » est maintenue dans tous ses effets et que, par exemple, si le site pirate dont l'accès est censé être bloqué par les fournisseurs d'accès à Internet utilise de nouveaux noms de domaine, les prestataires devront étendre le blocage et obtempérer, sur simple demande en ce sens du « *Computer Crime Unit* » ?

Si l'on peut encore admettre qu'il en soit ainsi, une fois l'instruction clôturée, puisque le ministère public en charge du dossier récupère son pouvoir général d'information et pourrait adresser une apostille en ce sens aux enquêteurs, la situation devient

35 M. Franchimont, A. Jacobs et A. Masset, *Manuel de procédure pénale*, Bruxelles, Larcier, 2012, p. 42.
A. Verhelpen, *La poursuite civile des procédures pénales*, Waterloo, Kluwer, 2012, pp. 20-22.

plus problématique une fois que l'on arrive devant la juridiction de fond.

Une évidence tout d'abord: quelle qu'en soit sa teneur, la décision (définitive) rendue par une juridiction répressive mettra un terme à la mesure de blocage. Si l'on doit se résoudre à l'idée qu'une saisie peut être opérée à charge d'un tiers (étranger) à la procédure pénale, il n'en sera pas de même avec la peine que le juge du fond serait amené à prononcer, qui devra rester propre au condamné et sera mise à exécution à son égard uniquement... Donc, au plus tard, même dans l'hypothèse où la plateforme permettant le piratage d'œuvres protégées par les droits d'auteur se verrait condamnée, le fournisseur d'accès à Internet se verra délié de toute obligation de poursuivre le blocage de l'accès aux domaines litigieux. La difficulté sera bien entendu de savoir comment il sera informé de cette décision, vu que la procédure pénale ne le concerne pas.

Une autre question doit être soulevée: quels sont les droits que les fournisseurs d'accès à Internet peuvent faire valoir en cours de procédure? Il ne fait aucun doute – la procédure suivie dans le cadre de l'arrêt annoté le confirme – que le référé pénal, tel qu'organisé par l'article 61*quater* du Code d'instruction criminelle, offre une possibilité de faire cesser la mesure et que l'écoulement du temps voire son caractère disproportionné pourraient justifier sa mainlevée. Mais il paraît exclu que les fournisseurs d'accès puissent intervenir tant devant les juridictions d'instruction statuant sur le règlement de procédure que devant le juge du fond, puisqu'ils ne sont pas partie à la procédure.

5) Va-t-on importer dans le procès pénal des débats techniques qui n'y ont pas leur place?

Un autre écueil pourrait contaminer les procédures à venir. Dans le dossier soumis à la Cour de cassation, l'atteinte aux droits des titulaires de la propriété intellectuelle semblait avérée, le site «Pirate Bay» ayant déjà fait l'objet tant en Belgique qu'à l'étranger de plusieurs procédures ayant objectivé le caractère illicite de ses activités.

Mais qu'en serait-il si d'autres plateformes pirates étaient visées et dont le contenu des activités serait sujet à discussion. Va-t-on imposer à un magistrat instructeur de se pencher sur le bien-fondé, *prima facie*, d'une atteinte aux droits des titulaires de droits intellectuels sans réelle possibilité de contradiction (la plateforme ciblée étant bien souvent établie à l'étranger)? Les juges d'instruction ne semblent pas outillés pour trancher ce genre de contestations, sur lesquelles des tribunaux civils ont parfois du mal à se prononcer en raison de leurs aspects techniques.

Pierre Monville et Mona Giacometti

Bruxelles (9e ch.), 9 mai 2012

Note d'observations de Jean-Marc Van Gyseghem[1]

EID – SÉCURITÉ – CONFIDENTIALITÉ – NUMÉRO DE REGISTRE NATIONAL – PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

EID – SECURITY – CONFIDENTIALITY – NATIONAL IDENTIFIER – DATA PROTECTION

La cour d'appel de Bruxelles a eu l'occasion de connaître un dossier dans lequel une société commerciale, Fidel ID, utilisait le numéro de registre national stocké sur la puce de la carte d'identité électronique (eID) pour identifier les clients inscrits dans leur service de carte de fidélité.

Elle a jugé qu'«à défaut d'autorisation du comité sectoriel du registre national, Fidel ID utilise [ledit] numéro (...) en violation de la loi (du 8 août 1983 organisant le registre national)» et se rend coupable d'un acte contraire aux usages honnêtes en matière commerciale au sens de la loi sur les pratiques du commerce.

* * *

The Court of Appeal of Brussels dealt with a company, Fidel ID, using the national identifier stored in the chip of the Belgian identity card (eID) to identify the client affiliated to its fidelity program.

The Court considered that Fidel ID violates the legislation on the "Registre national" by using the national identifier without any authorisation by the "Comité sectoriel du Registre national" and, by consequences, is guilty of violation of the legislation on the commercial practices.

Siège: M. Mackelbert (cons., prés. f.f. ch.), Mme Carlier (cons.), M. van der Haegen (cons. suppl.)

Plaid.: MMes Van Fraeyenhoven, Meire et Defauw, Brocorens

R.G. n° 2011/AR/1038

I. DÉCISION ENTREPRISE

L'appel est dirigé contre le jugement prononcé contradictoirement le 28 février 2011 par le président du tribunal de commerce de Bruxelles, siégeant comme en référé en matière de cessation.

Les parties ne produisent aucun acte de signification de cette décision.

II. PROCÉDURE DEVANT LA COUR

L'appel est formé par requête, déposée par Fidelsys au greffe de la cour, le 29 avril 2011.

La procédure est contradictoire, ayant été mise en état sur la base de l'article 747 du Code judiciaire.

Il est fait application de l'article 24 de la loi du 15 juin 1935 sur l'emploi des langues en matière judiciaire.

III. FAITS ET ANTÉCÉDENTS DE LA PROCÉDURE

1. Fidelsys est une société qui a élaboré un système de fidélisation de la clientèle par la création d'une carte de fidélité unique qui peut être lue par toutes sortes de magasins différents. Liée à un serveur informatique, elle a pour vocation de remplacer l'ensemble des cartes

[1] Jean-Marc Van Gyseghem est Directeur de l'Unité de recherche «Libertés et société de l'information» du Centre de Recherches Information, Droit et Société (www.crids.eu) et avocat au barreau de Bruxelles (www.rawlingsgiles.be).
Le présent article ne reflète que les opinions personnelles de l'auteur qui remercie cependant les chercheurs du Crids pour les discussions fructueuses en matière de protection des données à caractère personnel.