Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La responsabilité des acteurs de l'Internet

Lerouge, Jean-Francois; Poullet, Yves

Published in:
Rapports belges au Congrès de l¿Académie Internationale de Droit Comparé à Brisbane

Publication date:
2002

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Lerouge, J-F & Poullet, Y 2002, La responsabilité des acteurs de l'Internet. Dans *Rapports belges au Congrès de l¿Académie Internationale de Droit Comparé à Brisbane.* Académia Bruylant, Bruxelles, p. 1043-1103.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 27. Apr. 2024

La responsabilité des acteurs de l'Internet[1]

Yves Poullet
Doyen de la Faculté de droit, FUNDP, Namur
Professeur ordinaire aux FUNDP et à l'ULG
Directeur du CRID

Yves.poullet@fundp.ac.be

Et

Jean-François Lerouge
LL.M Georgetown University
Professeur invité, HEC, (Liège)
Assistant CRID – FUNDP (Namur)
Avocat BIRD & BIRD (Bruxelles)

jean-francois.lerouge@fundp.ac.be
jean-francois.lerouge@twobirds.com

[1] Le présent article est à jour au 31 octobre 2001.

© Yves Poullet & Jean-François Lerouge

INTRODUCTION GENERALE

Les caractéristiques et la multiplicité des acteurs sur les réseaux génèrent de nouveaux risques, lesquels engendrent des problèmes de responsabilité posés en des termes inédits.

Le législateur européen, et à sa suite les législateurs nationaux, ont parfois tenté de les appréhender en adoptant de manière spécifique une série de dispositions légales, sensées clarifier la situation. Dans d'autres cas, les législateurs sont restés trop frileux. Parfois, ils ne se sont tout simplement pas aperçus que les règles qu'ils adoptaient suscitaient des problèmes particuliers de responsabilité difficilement solubles au regard des seules règles de droit commun.

On est dès lors en droit de se demander si et dans quelle mesure le droit commun de la responsabilité s'en trouve *in fine* affecté.

L'objet de la présente étude est de livrer au lecteur, en droit européen et en droit belge, quelques modestes observations sur cette question au départ de deux acteurs de l'Internet (les prestataires intermédiaires et les autorités de certifications) et à la lumière de deux risques particuliers (les paiements électroniques et la protection des données).

© Yves Poullet & Jean-François Lerouge

Chap. 1 : La responsabilité des prestataires intermédiaires

La responsabilité des prestataires intermédiaires sur les réseaux a déjà fait couler beaucoup d'encre[2]. Il faut dire que la matière faisait l'objet d'incertitudes et de controverses juridiques jusqu'à l'adoption de la Directive du 8 juin 2000 relative à certains aspects juridiques de la société de l'information et notamment du commerce électronique (ci-après, «la directive»)[3]. Cette directive, de l'aveu même de ses auteurs, entend instaurer un équilibre entre les différents intérêts en

---

2 Voyez à titre d'exemples non-limitatifs, E. MONTERO, "La responsabilité des prestataires intermédiaires de l'Internet", *Revue Ubiquité,* n°5, juin 2000, pp. 99 à 117; A. LUCAS, "La responsabilité civile des acteurs de l'Internet, *A&M,* 2000/1, p. 42 à 52. A. STROWEL, "La responsabilité des fournisseurs de services en ligne: développements récents" in "La responsabilité liée à l'information et au conseil, questions d'actualité, sous la direction de B. DUBUISSON et P. JADOUL, Facultés Universitaires Saint-Louis, Bruxelles, 2000, pp. 215 à 267; K. BODARD, "Aansprakelijkheid van Internet Service Providers in Europees perspectief", in *Internet & Recht*, éds. K. Byttebier, R. Feltkamp & E. Janssens, Antwerpen, Maklu, 2001, p. 285 et s.; T. VERBIEST et E. WERY, "La responsabilité des fournisseurs de service Internet: derniers développements jurisprudentiels, *J.T.,* 2001, pp. 165 à 173.; R. JULIA-BARCELO, "On-Line intermediary liability issues: comparing E.U. and U.S. legal frameworks, *European intellectual Property review,* 2000, n°22/3, pp. 106-109; U. SIEBER, "Responsibility of Internet providers – a comparative legal study with recommendations for future legal policy", *Computer Law & Security Report,* Vol 15 n°15, n°5, 1999, pp. 292 à 308; Y. JOMOUTON, "Réseau Internet et responsabilité extra-contractuelle en droit belge", *R.E.D.C.,* 1999, 5-22; Pour un aperçu du droit italien, voy. M. DE ARCANGELIS, "La responsabilité des fournisseurs de services d'hébergement sur Internet en Italie", disponible sur http://www.juriscom.net, consulté pour la dernière fois le 5 août 2001.

3 Directive 2000/31/CE du parlement européen et du conseil du 8 juin 2000 relative à certains aspects juridiques de la société de l'information et notamment du commerce électronique, dans le marché intérieur, *J.O.,* 17/07/2000, L 178/1.

jeu et mettre fin «aux divergences existantes et émergentes entre les législations et les jurisprudences des Etats membres dans le domaine de la responsabilité des prestataires de services agissant en qualité d'intermédiaire ».[4]

La directive est en cours de transposition dans notre pays[5]. Le moment semble donc bien choisi pour reprendre la plume afin d'offrir au lecteur une vue d'ensemble, synthétique et, dans la mesure du possible, originale du sujet.

La nouvelle loi va-t-elle bouleverser notre droit de la responsabilité et instaurer un régime particulier pour certains acteurs du Net ? Dans quelle mesure convient-il d'adapter notre droit commun pour répondre aux vœux de la Directive ?

Il n'entre pas dans nos intentions de mener une étude détaillée du droit de la responsabilité civile[6]. Nous souhaiterions, après un bref aperçu de l'enjeu (I) circonscrire nos modestes observations à un rappel des principes directeurs de notre droit de la responsabilité extra-contractuelle (II), le confronter à notre problématique à la lumière de quelques décisions de jurisprudence belge et française (III), examiner rapidement le régime mis en place par la directive,

---

4 Considérants 40 et 41 de la directive.

5 Le premier avant projet de loi, proposé par le centre de recherches informatique et droit des facultés universitaires Notre-Dame de Namur, en charge d'une mission de consultance pour le Ministère des affaires économiques a été publié dans "Le commerce électronique européen sur les rails? Analyse et proposition de mise en oeuvre de la directive sur le commerce électronique", in *Cahiers du CRID,* n°19, spéc. les annexes. Ce projet de loi fait l'objet de commentaires détaillés dans la partie écrite par E. MONTERO "La responsabilité des prestataires intermédiaires sur les réseaux", in cahier du CRID n°19, chap. 6, spéc. pp. 274 – 295.

6 Nous souhaitons dans la présente analyse nous limiter à la responsabilité civile des prestataires intermédiaires d'Internet, même si la responsabilité pénale sera abordée de manière indirecte dans le cadre de l'analyse du régime mis en place par la directive "commerce électronique".

© Yves Poullet & Jean-François Lerouge

souligner ses faiblesses, notamment à la lumière de récentes décisions jurisprudentielles qui ont tenté de le mettre en œuvre et analyser la manière dont le législateur européen entend transposer ses dispositions(IV), pour enfin conclure par quelques réflexions.

© Yves Poullet & Jean-François Lerouge

I. L'enjeu de la problématique

Mais pourquoi donc les fournisseurs d'accès à Internet ont-ils défrayé le feu de la chronique ?

Une des grandes caractéristiques de l'Internet est sans aucun doute la possibilité offerte à chaque Internaute de diffuser largement leurs opinions, leurs produits ou services. Cette liberté n'est pas sans risque. Ainsi une information diffamatoire ou attentatoire à la vie privée, un acte déloyal ou une contrefaçon d'un droit intellectuel pourra, par le jeu d'un simple «clic », être diffusée à l'échelle planétaire et causer très rapidement, et sans que son auteur en soit toujours conscient, un préjudice important à la personne qui en est la victime.

Dans certains cas, l'auteur de l'acte préjudiciable pourra être identifié, poursuivi et condamné. Néanmoins, on ne peut exclure que dans une série d'hypothèses, les poursuites s'avèrent totalement illusoires ou inefficaces soit en raison des difficultés d'identification de l'auteur de l'acte répréhensible ou simplement en raison de son insolvabilité.

Il est dès lors tentant pour la victime de s'adresser à un tiers plus solvable et aisément identifiable. Les fournisseurs d'accès et de service Internet constituent les parfaites «victimes », pour dédommager les «préjudiciés d'Internet ».

C'est dans ce contexte que les actions en responsabilité contre ces acteurs de la vie économique se sont multipliées.

L'enjeu est alors pour le juge de trouver la solution la plus équitable possible dans le respect du droit et de la sécurité juridique.

II. Rappel des grands principes du droit de la responsabilité

La responsabilité civile des prestataires d'Internet est susceptible d'être engagée sur la base de plusieurs fondements. Tout d'abord, et même si cela ne constitue pas l'essentiel de notre propos, il ne peut être fait abstraction du contrat qui est conclu, même de manière fortuite, non seulement entre l'auteur du contenu préjudiciable ou illicite et le fournisseur d'accès, mais également entre un tiers et le fournisseur de contenu[7].

Ensuite, la responsabilité civile du prestataire peut être engagée sur le plan délictuel ou quasi-délictuel tant envers l'auteur du contenu préjudiciable qu'envers les tiers.

A. La responsabilité contractuelle

Le terrain de la responsabilité contractuelle ne suscite a priori pas de difficulté majeure. Bien souvent, le prestataire intermédiaire aura

[7] E. MONTERO rappelle à juste titre qu' « en cas de libre accès à des sites et données disponibles sur le réseau, l'existence d'un contrat n'est pas nécessairement exclue, même si l'usager n'a pas le sentiment d'être engagé dans des liens contractuels avec le producteur. En effet, les pages-écran qu'il visualise au cour de sa navigation peuvent contenir des mentions susceptibles d'être analysée comme une offre au sens juridique de la notion. Dès l'instant où il poursuit l'interrogation, on peut estimer qu'il manifeste son acceptation et qu'un contrat s'est ainsi formé.» ; voy. R. JULIA-BARCELO, E. MONTERO, A. SALAUN, « La responsabilité des prestataires intermédiaires », in *Commerce électronique, le temps des certitudes, Cahiers du CRID,* n° 17, p. 34.

pris soin d'exonérer sa responsabilité du chef de contenu illicite ou préjudiciable, dans les limites légales et notamment dans le respect des dispositions légales protectrices du consommateur. Il veillera par exemple à se ménager la possibilité de mettre fin au contrat d'hébergement en cas d'indice de contenu préjudiciable, voire même à obtenir des garanties.

Avec l'avènement du nouveau régime mis en place par la directive sur lequel nous reviendrons, il nous paraît particulièrement judicieux de lui recommander l'insertion de clauses l'exonérant de toute responsabilité du fait du retrait même temporaire de l'information stockée en cas d'indice, quel qu'il soit, d'illégalité. Certes, une telle clause ne supprime pas son obligation générale de se comporter de bonne foi. A ce titre, sa responsabilité pourrait toujours être engagée dans le cadre d'un retrait intempestif de l'information litigieuse. Néanmoins, il nous semble que sa responsabilité pourra être beaucoup plus difficilement engagée ; les raisons et les conditions d'intervention du fournisseur ayant été clairement explicitées.

B. Les fondements extra-contractuels

La responsabilité extra contractuelle du prestataire peut être engagée à la fois sur le plan de la formation du contrat mais également au niveau de son exécution vis-à-vis des tiers.

1. Au stade de la formation du contrat

L'auteur identifié d'un contenu préjudiciable, poursuivi par un tiers préjudicié et condamné, pourrait chercher, sans doute en faisant preuve d'un certain culot, à se retourner contre son prestataire de service.

Il ne peut par conséquent pas être exclu qu'il cherche à placer son action en responsabilité sur le terrain de la transgression de l'obligation d'information, de conseil et de collaboration qui pèse sur chacune des parties durant la période pré-contractuelle. Ces obligations repose sur le principe de bonne foi qui doit présider à la formation des conventions[8]. En matière informatique, ces obligations ont connu un développement considérable[9].

De manière générale et pour faire bref, l'obligation du fournisseur de services peut se décomposer de la manière suivante : informer ses clients de tous les renseignements qui pourraient lui être utiles (condition d'utilisation, risques encourus, …), le conseiller et le mettre en garde. Le degré d'implication du fournisseur dépend notamment de la qualité du client (professionnel ou profane, initié ou non). L'obligation de conseil nous semble en l'espèce être moins relevante. C'est surtout au niveau de la violation du devoir d'information que la responsabilité du fournisseur pourra être engagée. Les devoirs d'information du fournisseur ont toutefois pour limite les obligations corrélatives du client qui se doit lui-même de collaborer de bonne foi et donc de s'informer.

---

8 Voy notamment. *La bonne foi*, Travaux de l'association H. Capitant, Paris, Litec, 1994; W. DE BONDT, "Precontractuele aansprakelijkheid", *R.G.D.C.,* 1993/2, p.93, J.-F. ROMAIN, *Théorie critique du principe général de bonne foi en droit privé, des atteintes à la bonne foi en général, et de la fraude en particulier,* Thèse, Bruylant, Bruxelles, 2000, spéc. P.837 et s.

9 Voy not. J.-P. BUYLE, L. LANNOYE, Y. POULLET, V. WILLEMS "Chronique de jurisprudence, l'informatique (1987-1994)", *J.T.,* 1994, p.; E. DAVIO et E. MONTERO, "Aspects contractuels de l'informatisation de l'entreprise", *Guide Juridique de l'entreprise,* T.III, L.37, spéc p. 20 et s.; M. VIVANT, C. LE STANC et alii, *Lamy droit de l'informatique – Informatique, multimedia, réseaux,* éd. Lamy, 1997, pp. 640 et s.

A la lumière de la jurisprudence existante, il est permis d'affirmer que les fournisseurs ont l'obligation d'informer leurs abonnés sur les nécessaires respect des lois et des droits d'autrui[10].
Sans exagérer, il semble a priori justifié de mettre à leur charge une obligation d'identification (pour tenter d'enrayer l'anonymat, et ce, même s'ils conservent le droit de ne pas divulguer le nom de leur contractant), de recourir à tout procédé incitatif du respect du droit des personnes et d'encourager, sinon d'imposer, l'adhésion à une charte de bon comportement. Certains vont plus loin en allant jusqu'à recommander aux hébergeurs de site l'obligation de vérifier le titre et le thème des pages de leurs abonnés[11].

Il faut néanmoins, à notre sens, se garder d'une trop grande précision dans le respect de cette obligation d'information. Nous serions même tentés de recommander la plus grande prudence lors de l'élaboration, puis de l'incitation à l'adhésion, de la charte de bon comportement. Si ce procédé d'auto-réglementation par la voie contractuelle a certes beaucoup de vertus, il pourrait néanmoins, dans certains cas, se retourner contre son auteur. Si le code «d'adhésion» est trop précis quant aux obligations du bénéficiaire de services et aux moyens de contrôle éventuels dont dispose le fournisseur pour en assurer le respect, il pourrait, comme nous le verrons dans la section suivante, permettre à un tiers de s'en prévaloir pour engager la responsabilité du fournisseur.

2. Vis-à-vis des tiers

[10] En ce sens voy. not. L'affaire dite "Lynda Lacoste", Trib. Gde inst. Nanterre, 8 déc. 1999, *Gaz.Pal.*, 11-12 févr. 2000, p.2, note H. BITAN.

[11] A. GITTON, "Responsabilité des hébergeurs, coke en stock?", *Dossier a.s.b.l. droit nouvelles technologies,* 13 avril 2001, disponible à l'adresse suivante: http://www.droit-technologie.org, consulté pour la dernière fois le 16 juillet 2001.

La règle énoncée à l'article 1383 du Code civil est limpide : "*Chacun est responsable du dommage qu'il a causé non seulement par son propre fait mais encore par sa négligence ou par son imprudence"*.

A ce jour, les prestataires de service n'échappent pas à ce devoir général de diligence. Selon les circonstances de l'espèce, il est donc possible d'engager leur responsabilité dès lors qu'un manquement à ce devoir peut être prouvé.

Ainsi, il pourrait leur être reproché, par exemple, de ne pas avoir pris les mesures raisonnables qui s'imposaient afin de procéder au retrait immédiat d'un contenu apparent manifestement illicite. Certains vont plus loin en imposant un devoir minimum de contrôle de ce qui transite. Nous y reviendrons.

La question peut également se poser de savoir si et dans quelle mesure un tiers pourrait se plaindre de la mauvaise exécution d'un contrat d'hébergement et mettre en cause de ce fait la responsabilité civile du fournisseur en invoquant par exemple une disposition de la charte de bon comportement ou une stipulation contractuelle alors qu'il n'en est pas le destinataire ni le bénéficiaire.

Depuis un arrêt de la Cour de cassation de 1909[12], il est très clair, «à la différence de la jurisprudence française qui, en certaines occasions a admis que la faute contractuelle puisse être comme telle la source d'une responsabilité aquilienne envers le tiers auquel elle a causé un dommage »[13], que le tiers préjudicié peut se prévaloir du contrat et du manquement par une partie à ses obligations, comme de simples faits, pour en déduire une conséquence de droit. En d'autres termes, il est tout à fait possible de se prévaloir sur le plan délictuel d'un fait

12 Cass. 24 mai 1909, *Pas.,* I, 271.

13 X. DIEUX et D. WILLERMAIN, "La responsabilité civile du prestataire de services à l'égard des tiers", in *Les contrats de service,* éd. Jeune Barreau de Bruxelles, 1994, p. 219 et les références citées.

constitutif de l'inexécution ou de l'exécution défectueuse d'un contrat de service pour démontrer la faute aquilienne au sens des articles 1382 et 1383 du Code civil.

Dans notre cas, un tiers pourrait dès lors parfaitement se prévaloir de la charte de bons comportements[14], entrée dans le champ contractuel de la relation fournisseur-abonnés, afin de démontrer qu'un prestataire a été négligent car il n'a pas procédé au contrôle minimum qu'il s'était engagé à opérer au titre de la charte.

III. De quelques décisions jurisprudentielles

La jurisprudence belge et française[15] a été confrontée à plusieurs reprises à l'application des principes énoncés ci-dessus.

Nous nous proposons dans les quelques lignes qui suivent d'en présenter les grandes tendances.

A. En France

14 Par charte de bons comportements, on ne vise pas uniquement les codes de conduite pertinents visés à l'article 10 de la Directive, mais bien toute forme d'engagement que le fournisseur s'engage à prendre concomitamment à l'offre de ses services.

15 Nous éludons volontairement l'analyse des autres décisions européennes dans le but de nous concentrer sur l'application du Code civil belge et français. Pour un aperçu des décisions françaises liées au contenu illicite, Voy "Jurisprudence: France: résumés contenus illicites", disponible sur http://www.juriscom.net/txt/jurisfr/cti/resum.htm, consulté pour la dernière fois le 16 juillet 2001; pour un aperçu de la jurisprudence américaine et européenne, voy. A. STROWEL, *op.cit.,* p. 252 et s.

En France, plusieurs affaires ont amené les cours et les tribunaux à se prononcer sur l'étendue de la responsabilité des prestataires Internet.

La décision *Estelle L. c/ Lacambre* ne peut être passée sous silence. Elle a donné lieu à une décision en première instance qui a fait l'objet d'un appel[16]. Dans cette affaire, Estelle Hallyday, s'estimant victime d'une atteinte à son droit à l'image et à l'intimité de sa vie privée suite à la diffusion de photos la représentant dénudée, avait demandé en référé au Tribunal de grande instance de Paris, d'enjoindre Valentin Lacambre, gestionnaire du service d'hébergement de cesser la diffusion des photos litigieuses. Par ordonnance du 9 juin 1998, le Tribunal fit injonction à l'hébergeur sous astreinte de FR 100.000 par jour, de «mettre en œuvre les moyens de nature à rendre impossible toute diffusion des clichés photographiques en cause à partir de l'un des sites qu'il héberge ». Le tribunal motiva sa décision comme suit :

« (…) S'agissant de l'hébergement d'un service dont l'adresse est publique et qui est donc accessible à tous, le fournisseur d'hébergement a, comme tout utilisateur du réseau la possibilité d'aller vérifier le contenu du site qu'il héberge et en conséquence de prendre le cas échéant les mesures de nature à faire cesser le trouble qui aurait pu être causé à un tiers (…) Le fournisseur d'hébergement devra donc justifier du respect des obligations mises à sa charge, spécialement quant à l'information de l'hébergé sur l'obligation de respecter le droit de la personnalité, le droit des auteurs, le droit des propriétaires de marque ; de la réalité des vérifications qu'il aura opérées, au besoin par des sondages et diligences qu'il aura

[16] T.G.I. Paris (réf.), 9 juin 1998, *J.C.P.,* E, 1998, p. 953, n°21, obs. M. VIVANT et C. LE STANC; Paris (14e ch.), 10 février 1999, *D.,* 1999, p. 389, note N. MALLET-POUJOL; décision disponible sur http://www.juriscom.net, visité pour la dernière fois le 16 juillet 2001. Voy. également G. HAAS et O. de TISSOT, "La mise à disposition de pages web est-elle dangereuse?", chronique du 5 juin 1999, disponible sur http://www.juriscom.net, visité pour la dernière fois le 16 juillet 2001.

accomplies dès la révélation d'une atteinte aux droits des tiers pour faire cesser cette atteinte » (c'est nous qui soulignons). Sans entrer dans les détails de la décision de la cour d'appel du 10 février 1999, l'on relèvera que la Cour confirme la décision et justifie l'octroi d'une indemnité comme suit «en offrant, comme en l'espèce, d'héberger et en hébergeant de façon anonyme, sur le site altern.org qu'il a créé et qu'il gère, toute personne qui, sous quelque dénomination que ce soit, en fait la demande aux fins de la mise à disposition du public ou de catégories de public de signes ou de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère de correspondances privées, Valentin Lacambre excède manifestement le rôle technique d'un simple transmetteur d'informations ». En l'espèce, la Cour semble estimer que V. Lacambre ne peut être exonéré de toute responsabilité parce qu'il a accepté d'offrir un service d'hébergement anonyme.

La décision est intéressante à plus d'un titre. Comme le relève judicieusement Etienne Montero, elle fait peser sur le prestataire d'hébergement des obligations de trois ordres (i) le devoir de conseiller les clients sur leurs propres obligations, (ii) le devoir d'opérer des contrôles au besoin par des coups de sonde (iii) le devoir de faire diligence, dès la révélation d'une atteinte aux droits des tiers, pour faire cesser cette atteinte[17].

Le tribunal et la Cour, on le voit, donnent un contenu spécifique à l'article 1383 du Code civil. Par ailleurs, ils rappellent les devoirs élémentaires de conseil et d'information (en l'espèce sur le respect des droits et libertés des individus) dont tout prestataire est tenu tant durant la phase pré-contractuelle que durant l'exécution du contrat d'hébergement. Enfin, la Cour d'appel reproche de ne pas avoir livré l'identité de l'auteur du contenu. On peut se demander si elle irait jusqu'à condamner par principe toute possibilité laissée à l'anonymat sous le couvert duquel agis l'éditeur du site litigieux, contribuant

[17] E. MONTERO, *op.cit.,* p.113-114.

ainsi de manière passive aux activités illicites. Le 24 mai 2000, le tribunal de grande instance de Nanterre a toutefois estimé que l'hébergeur n'a pas l'obligation de s'assurer de l'identité de l'éditeur du site lors de l'ouverture du compte auprès de lui.[18] Cette analyse est néanmoins quelque peu contredite par la cour d'appel de Versailles qui estime que l'anonymat doit être prohibé. Selon la Cour, les obligations incombant à l'hébergeur doivent se traduire «au stade de la formation du contrat avec le client-créateur de site, par des mesures préventives telles la prohibition de l'anonymat ou de la non-identification, l'adhésion à une charte de comportement ou tout autre procédé incitatif au respect des textes et des droits des personnes, et au stade de l'exécution du contrat, par des diligences appropriées pour repérer tout site dont le contenu est illégal, illicite ou dommageable afin de provoquer une régularisation ou d'interrompre la prestation »[19] (c'est nous qui soulignons).

L'affaire dite « *Lacoste* » présente des faits similaires à l'affaire Estelle L. c/ Lacambre. Dans son jugement, le T.G.I. de Nanterre[20]est encore plus clair puisqu'il précise qu'en l'absence de disposition étatique[21] régissant la question, « (…) la responsabilité de

---

18 Trib. Gde. Inst. Nanterre, 1ere ch., 24 mai 2000, disponible sur http://www.juriscom.net, cité par T. VERBIEST et E. WERY, *op.cit.,* p.166.

19 Versailles, 8 juin 2000, disponible sur http://droit-technologie.org, cité par T. VERBIEST et E. WERY, *op.cit.,* p.167.

20 T.G.I. Nanterre, première chambre, section A, 8 décembre 1999. Pour un commentaire succinct de la décision, voy. M. PENDU, "L'étendue de la responsabilité du fournisseur d'hébergement sur Internet", *Expertise,* avril 2000, p. 109 et s. La jurisprudence du tribunal a été confirmée par une décision rendue en référé (Trib.gde.inst. Nanterre, juin 2000 disponible sur http://www.legalis.net/jnet/index.htm

21 Depuis la France s'est dotée d'une législation transposant les principes énoncés dans la directive commerce électronique, voy. Loi 2000-719 du 01 Août 2000 Loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, entrée en vigueur le 02 Août 2000, *JORF*, 2 août 2000.

l'hébergeur doit être recherchée par référence au droit commun défini par l'article 1383 du Code civil ». Le tribunal, pour retenir la responsabilité de l'hébergeur relève divers manquements à l'obligation générale de prudence et de diligence. A ce propos, le juge relève que s'il n'appartient pas au fournisseur d'hébergement d'exercer une surveillance minutieuse et approfondie du contenu des sites, ce dernier doit en revanche prendre les mesures raisonnables qu'un professionnel avisé mettrait en œuvre « pour évincer de son serveur les sites dont le caractère illicite est apparent, cette apparence devant s'apprécier au regard des compétences propres du fournisseur ». Le tribunal va même plus loin dans la détermination du contenu de l'obligation de diligence en reprochant au fournisseur de ne pas avoir mis en place un système de détection pour repérer les illégalités dans un domaine que « l'actualité signalait particulièrement à leur vigilance et qui appelait de leur part une réaction ». Le respect de cette obligation passe ici par le respect d'un devoir d'action.

Dans certains cas la jurisprudence va jusqu'à instituer une présomption de connaissance du contenu des sites. En l'espèce le tribunal de grande instance de Paris a estimé que la responsabilité d'un hébergeur devait être retenue pour le motif qu'il ne pouvait ignorer qu'un nom de domaine, exclusivement constitué de la reproduction servile d'une marque de renommée était contrefaisant.[22]

B. En Belgique

La jurisprudence belge est nettement moins prolixe sur la responsabilité des prestataires de l'Internet.

Plusieurs décisions, pour la plupart rendues en référé et motivées de manière sommaire, abondent dans le sens de la jurisprudence

[22] Voy. T. VERBIEST et E. WERY, *op.cit.,* p.167

française en reprochant aux prestataires des manquements aux devoirs de diligence et de prudence. Ces derniers devraient jouer un rôle actif dans la lutte contre les actes illicites commis sur Internet en mettant en place toutes les mesures nécessaires que l'on peut raisonnablement escompter de la part d'un professionnel ; particulièrement lorsqu'ils avaient ou devaient avoir connaissance de la présence d'un contenu illicite ou préjudiciable sur le net[23].

Dans l'affaire *Easy Computing c. Ad Valvas*[24], le juge a reconnu le rôle actif du fournisseur d'accès dans la lutte contre les actes illicites commis sur Internet. En l'espèce toutefois, qui concernait une annonce publicitaire de vente de logiciels piratés, l'hébergeur avait été mis en demeure de cesser l'atteinte aux droits litigieux de la société Easy Computing. La société Ad Valvas, qui avait donc connaissance des actes litigieux, n'avait pas prétendu y mettre fin spontanément.

Le 2 novembre 1999, le tribunal de commerce de Bruxelles a rendu un jugement dans le cadre d'un litige qui opposait l'ASBL IFPI et la SA Polygram contre la SA Belgacom Skynet[25]. La société Skynet hébergeait des sites qui offraient des hyperliens[26] vers des sites permettant des enregistrements musicaux « pirates » en format

---

23 Voy. par exemple, Trib. 1ère instance de Bruxelles (réf.), 2 mars 2000 (propos racistes et xénophobes), disponible sur http://www.droit-technologie.org (consulté pour la dernière fois le 9 avril 2001). Pour un aperçu d'autres décisions rendues en référé, voy. A. STROWEL, *op.cit.*, p. 265.

24 Civ. Courtrai (réf.), 10 septembre 1998, RG 98/275/C, citée par R. JULIA-BARCELO, E. MONTERO, A. SALAÜN, *op.cit.,* p. 50.

25 Le texte de la décision et sa traduction libre en français peut être lu sur le site http://www.droit-technologie.org, consulté pour la dernière fois le 16 juillet 2001. La décision est commentée par S. MALENGREAU, "Responsabilité des hébergeurs: un fournisseur condamné en Belgique", 6 février 2000.

26 Sur cette notion voy.infra.

MP3[27]. A deux reprises, celle-ci fut mise en demeure de supprimer ces liens. En l'absence de réaction de Skynet, les sociétés IFPI et Polygram introduisirent une action en cessation sur la base de l'article 93 de la loi sur les pratiques du commerce et de la protection et l'information du consommateur[28]. Le tribunal fait droit à leur demande estimant que la défense est responsable de ne pas avoir supprimé les liens litigieux alors qu'elle avait été mise au courant que ces liens encourageaient la visite de site web pirates notoirement connus. Il condamne par conséquent Skynet, sous peine d'astreinte à cesser ces pratiques.

La décision a fait l'objet de vives critiques. On reproche au juge d'avoir opéré un renversement de la charge de la preuve « en obligeant le fournisseur d'hébergement à juger lui-même si oui ou non le contenu du site hébergé ou lié est illicite. Dans une matière quasi-délictuelle comme celle-ci, n'appartient-il pas au demandeur de prouver ce qu'il prétend ? Le fournisseur d'hébergement ne doit-il pas intervenir que quand il est suffisamment assuré par le demandeur que le site qu'il héberge ou que le site vers lequel le site hébergé établit un lien a un contenu illicite ? Le fournisseur d'hébergement est ainsi placé dans une situation particulièrement délicate. S'il s'abstient de réagir lorsqu'il a connaissance d'une activité illicite ou préjudiciable, sa responsabilité pourra être engagée. S'il réagit de manière erronée, l'abonné pourra mettre en cause sa responsabilité du chef d'interruption injustifiée des services. Serait-il dès lors contraint de s'entourer de consultants pour procéder lui-même à des examens de licéité de sites web qu'il héberge ? »[29].

---

27 MP3 est un format de compression des fichiers sonores qui réduit leur taille et permet leur transmission sur des réseaux informatiques.

28 En vertu de cet article, "Est interdit tout acte contraire aux usages honnêtes en matière commerciale par lequel un vendeur porte atteinte ou peut porter atteinte aux intérêts professionnels d'un ou de plusieurs autres vendeurs".

29 S. MALENGREAU, *op.cit.,* p. 3. Dans le même sens voy. E. MONTERO qui s'interroge sur le bien-fondé de cette décision dans la mesure où le

En appel[30], la cour a infirmé le jugement en estimant que l'hébergeur n'avait commis aucune faute. Néanmoins, pour arriver à une telle conclusion, la cour rappelle le principe de base selon lequel l'hébergeur ne peut rester inactif lorsque la présence d'un contenu illicite sur ses serveurs lui est notifiée.
Selon la cour d'appel de Bruxelles[31], en présence d'un contenu illicite, le plaignant a l'obligation de notifier la présence du contenu illégal en exposant les arguments qui démontrent l'illégalité du contenu en question. L'hébergeur aurait alors trois jours ouvrables pour réagir et apporter la preuve de la légalité. S'il ne parvient pas à démontrer une telle légalité, il doit alors suspendre l'accès au site. Le plaignant quant à lui devra assumer la responsabilité d'une suspension injustifiée et le cas échéant indemniser l'hébergeur qui serait poursuivi par son abonné. En l'espèce, comme on le montrera dans la section qui suit, la cour fais échos aux dispositions européennes et entend donner un contenu plus précis aux dispositions normatives sujettes à critique et énoncées dans la directive commerce électronique.

Le raisonnement suivi par la cour n'en est pas moins surprenant dans la mesure où, en l'absence de toute disposition légale, la cour semble imposer la mise sur pied d'une procédure de vérification pour le moins précise.

---

défendeur ne pouvait pas être certain que le contenu du site était illicite. E. MONTERO, "La responsabilité des prestataires intermédiaires sur les réseaux", in *Cahiers du CRID,* n° 19, p.290, note 639.

30 Cour d'Appel de Bruxelles, 13 février 2001, jugement disponible et commenté sur http://www.droit-technologie.org.

31 "BELGACOM SKYNET dient binnen de drie werkdagen na de ontvangst van de kennisgeving die aan bovenvermelde voorwaarden beantwoordt, deze links te verwijderen of de toegand ertoe onmogelijk maken, tenzij zij binnen diezelfde termijn het bewijs kan voorbrengen dat de muziekopnames, waarnaar de gewraakte links verwijzen legaal zijn".

© Yves Poullet & Jean-François Lerouge

IV. La transposition en droit belge du régime juridique mis en place par la directive « commerce électronique »

La directive commerce électronique a notamment, nous l'avons dit, pour objectif d'uniformiser les règles relatives à la responsabilité des prestataires de services Internet agissant en qualité d'intermédiaire. La directive lui consacre une section 4,et 4 articles (articles 12 à 15).

Dans cette section, nous souhaiterions succinctement présenter le régime juridique mis en place par la Directive : Quel est ce nouveau régime (A) ? Quelle en est la nature, l'étendue et dans quelle(s) mesure(s) entend-t-il déroger au droit commun de la responsabilité (B)? Et enfin, quel jugement peut-on en faire (C)? Nous tenterons dans cette dernière section de mettre en évidence la manière dont le droit belge entend répondre aux faiblesses ou insuffisances de la directive.

A. Vue d'ensemble du régime mis en place par la directive

1. Champ d'application et réflexions liminaires

La directive commerce électronique instaure un régime d'exonération de la responsabilité civile et pénale qui diffère selon le type d'activité exercée par le prestataire intermédiaire. La directive opère en effet une distinction très nette selon que le prestataire se contente de transmettre de l'information (activité de « simple transport »), la stocke (activité de stockage, dite « catching ») ou au contraire l'héberge. La directive n'entend pas réglementer d'autres types d'activités comme la production ou l'édition de contenu, les

activités relatives aux hyperliens ou aux moteurs de recherche[32], lesquelles restent donc soumis au droit commun.

Le régime mis en place couvre tout type de contenu illicite[33]. D'une manière générale, il convient de souligner, et sous réserve de ce qui sera dit plus loin[34], que la directive prévoit, pour les activités concernées, une absence d'obligation générale de surveillance des informations transmises ou stockées. Les états membres ne peuvent donc pas imposer aux prestataires de rechercher activement des faits ou des circonstances révélant des activités illicites[35]. Cet article met dès lors clairement fin aux obligations de « monitoring » imposée par une certaine jurisprudence au titre de l'article 1383 du Code civil[36]. La directive réserve toutefois aux Etats membres la possibilité d'imposer aux prestataires des obligations de collaboration actives

---

32 Pour ces deux derniers services, la Directive se contente de proposer un réexamen de la situation avant le 17 juillet 2003 (voy. l'article 21.1 de la Directive). Voy. nos commentaires et références citées infra.

33 Il se différéncie dès lors du régime de responsabilité mis en place par le *"Digital Millenium Copyright Act",* législation américaine adoptée pour les problèmes liés au droit d'auteur sur le Net, dont le législateur européen s'inspire visiblement. Pour une analyse comparative des deux textes, voy. R. JULIA-BARCELO, *op.cit.,* supra, note 1; V. SEDAILLAN, "La responsabilité des prestataires techniques sur Internet dans le digital Millenium Copyright Act américain et le projet de directive européen sur le commerce électronique", *Cahiers Lamy droit de l'informatique et des réseaux,* n°110, 1999, pp. 1-4; également disponible sur http://www.juriscom.net (consulté pour la dernière fois le 16 juillet 2001); U. SIEBER, *op.cit.,* spéc. p. 297 et s.

34 Voir nos commentaires développés infra et liés aux considérants 47 et 48 de la directive.

35 Article 15.1 de la directive.

36 Voy. notamment en France les décisions étudiées *Estelle L. c/ Lacambre*, cour d'appel de Versailles et dans une moindre mesure l'affaire *Lacoste*. En Belgique, la jurisprudence analysée a essentiellement trait à l'activité liée aux hyperliens. La directive n'a donc théoriquement aucun impact sur cette jurisprudence belge en raison de son champ d'application limité. Nous y reviendrons.

(informer promptement les autorités publiques compétentes d'activités ou d'informations illicites alléguées) et passives (conserver les informations permettant l'identification des destinataires des services d'hébergement)[37].

2. Les activités exonérées par la Directive

2.1. L'activité de simple transport (article 12 de la Directive)

a) Notion

25. L'activité de simple transport regroupe, au sens de la Directive, le fait

- de transmettre sur un réseau de communication des informations fournies par le destinataire de services[38] ou ;
- de fournir un accès au réseau de communication.

Ces activités englobent « le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission ».

b) Régime juridique

26. Pour ces activités, la Directive prévoit un régime d'exonération de la responsabilité civile et pénale pour toutes les

[37] Article 15.2 de la directive.

[38] Par "destinataire de services", la directive vise "toute personne physique ou morale qui, à des fins professionnelles ou non, utilise un service de la société de l'information, notamment pour rechercher une information ou la rendre accessible" (article 2 d. de la Directive)

informations transmises sur le réseau à la triple condition que le prestataire de services :

- ne soit pas à l'origine de la transmission ;
- ne sélectionne pas le destinataire de la transmission et
- ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission.

On le voit, les conditions posées visent à s'assurer que le prestataire n'est impliqué en aucune manière dans la sélection ou le traitement de l'information transmise, sauf à des fins de pure transmission.

Dans la mesure où ces conditions sont rencontrées et sans préjudice des actions en justice au provisoire (actions en cessation)[39] ou au fond[40], les opérateurs de réseaux et fournisseurs d'accès agissant en cette qualité ne pourront voir leur responsabilité engagée, *alors même par exemple, qu'ayant connaissance de la présence d'informations sur le réseau et ayant prise sur ces dernières, ils s'abstiennent d'intervenir*[41]. Pour être précis, il faut néanmoins lire l'article 12 à la lumière du considérant 44 de la Directive qui rappelle fort judicieusement à l'attention des libertaires qu' «un prestataire de services qui collabore délibérément avec l'un des destinataires de son service afin de se livrer à des activités illégales va au-delà des activités de « simple transport » ou de « catching » et, dès lors, il ne peut pas bénéficier des dérogations en matière de responsabilité prévues pour ce type d'activités ».

---

39 Voy. le considérant 45 de la Directive.

40 Article 12.3 de la Directive (possibilité pour une juridiction ou une autorité administratived'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation).

41 R. JULIA-BARCELO, E. MONTERO et A. SALAUN, "La proposition de directive européenne sur le commerce électronique: questions choisies", in *Cahiers du CRID n°17,* p. 39.

27. L'affaire dite « Front 14 », jugée en référé par le Tribunal de grande instance de Paris en juin dernier constitue une première illustration d'application du régime mis en place par cet article (et singulièrement du pouvoir d'injonction de l'autorité judiciaire)[42].

28. D'aucuns estiment qu'il n'est pas exagéré de considérer, à la lecture de l'article 12 de la Directive que « l'on a affaire, en pratique, à une véritable immunité pour l'activité de « simple transport », …et à une impunité sur le plan pénal »[43].

Sur un plan purement contractuel, l'affirmation ne nous paraît pas dénuée de fondement, sauf à considérer que la responsabilité puisse être engagée pour une autre raison que le simple transport d'information illicite, comme en raison d'un dysfonctionnement des serveurs.

Sur le plan extra-contractuel, nous sommes un peu plus réservés. Théoriquement, concédons-le, sa responsabilité pré-contractuelle du chef, par exemple, de l'absence d'information sur le nécessaire respect des lois et des droits d'autrui, de l'absence de charte de bons comportements, pourrait toujours être engagée, spécialement dans l'hypothèse où un texte imposerait le recours à cette forme

---

42 "Racisme sur l'Internet: 16 fournisseurs d'accès assignés à Paris", *Dossier asbl droit et nouvelles technologies,* 27 juin 2001, disponible à l'adresse suivante: http://www.droit-technologie.org, consulté pour la dernière fois le 16 juillet 2001. Les dommages et intérêts octroyés symboliquement ont toutefois une justification périlleuse en l'absence de faute du prestataire.

43 R. JULIA-BARCELO, E. MONTERO et A. SALAUN, *op.cit.,* p. 41. Les auteurs, envisageant le maintien d'une responsabilité extra-contractuelle uniquement en cas de non respect des conditions visées à l'article 12. "Celles-ci sont si strictes qu'on peut tenir que la voie contractuelle est elle aussi pratiquement vérouillée. Ils estiment par conséquent qu'une action sur cette base est toute théorique . Par ailleurs, pour eux, la responsabilité contractuelle ne peut être engagée car le contrat conclu avec les abonnés vise seulement à régler les modalités d'accès au réseau; son objet est étranger au bon fonctionnement et au contenu des services.

d'autorégulation. Il faudrait toutefois être en présence d'un réel profane.

Par ailleurs, et cette hypothèse nous paraît plus réaliste, un tiers pourrait toujours se prévaloir du contrat d'hébergement ou d'une charte de bons comportements, comme de simples faits pour en déduire que le prestataire s'engageait à contrôler, par coup de sonde, le contenu et qu'il se réservait le droit de mettre fin à l'accès en cas d'activité illicite et dès lors qu'il était bien impliqué dans la transmission de l'information. Les conditions d'exonération prévue par la Directive ne seraient alors plus rencontrées.

2.2. L'activité de stockage (article 13 de la Directive)

a) Notion

Par activité de stockage, la directive entend le stockage automatique, intermédiaire et temporaire d'une information opérée dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service[44].

b) Régime juridique

L'exonération de la responsabilité se fait moyennant la réunion d'une série de conditions. Il faut nécessairement que:

a) le prestataire ne modifie pas l'information;
b) le prestataire se conforme aux conditions d'accès à l'information[45];
c) le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisée par les entreprises;

---

44 Article 13 de la directive.

45 Cette condition, reprise par l'avant-projet de loi belge nous semble très obscure. Que veut dire exactement dire le législateur européen?

d) le prestataire n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information
et
e) le prestataire agisse promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible

A nouveau, les conditions posées visent à s'assurer que le prestataire s'en tienne strictement à son rôle. L'exonération n'est ici cependant plus automatique. Elle suppose que le prestataire ait agi lorsqu'il a eu connaissance d'une information illicite. Par ailleurs, une juridiction ou une autorité administrative peut toujours exiger du prestataire qu'il mette fin à un acte illicite ou qu'il prévienne un tel acte et les réserves énoncées dans le considérant 44 décrit dans la section précédente sont également valables ici.

2.3. L'activité d'hébergement (article 14 de la Directive)

a) Notion

L'activité d'hébergement consiste à stocker des informations fournies par un destinataire de services.

b) Régime juridique

Pour autant qu'il ne contrôle pas les agissements du destinataire de services, le prestataire ne sera pas responsable des informations

stockées à la demande d'un destinataire lorsque les conditions suivantes sont réunies:

a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicite et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente
ou

b) le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

Le régime mis en place pour les activités d'hébergement ne diffère pas de celui mis en place pour l'activité de stockage. Le prestataire se verra exonéré de toute responsabilité vis-à-vis des tiers si, une fois informé de la présence d'information illicite sur l'un de ses serveurs, il a agi promptement pour retirer les informations illicites ou pour bloquer l'accès à celles-ci.

B. Un régime dérogatoire au droit commun de la responsabilité ?

Les grandes lignes du régime de responsabilité mis en place par la Directive ayant été présentées à la suite de la jurisprudence actuelle, il nous semble opportun de nous interroger sur l'impact de la Directive sur le droit commun de la responsabilité. En d'autres termes, la Directive bouleverse-t-elle notre droit commun de la responsabilité et dans l'affirmative quelle est l'étendue de ce bouleversement ?

Nous sommes d'avis que le législateur européen n'innove pas[46]. Au contraire, il nous semble qu'il s'évertue à tenter d'unifier la jurisprudence européenne en prescrivant des lignes directrices et des critères d'appréciation communs concernant le contenu et l'étendue du devoir général de prudence et de diligence du fournisseur de services sur Internet[47]. Se faisant, il essaie de limiter les hypothèses où la responsabilité du prestataire peut être mise en cause en «hiérarchisant » les obligations que les utilisateurs du Net sont en droit d'attendre de lui en fonction du type d'activité exercée. Il instaure par ailleurs un devoir de collaboration avec les autorités judiciaires et administratives qui n'a rien d'innovant ou de choquant[48].

Le droit belge et français de la responsabilité, essentiellement basé sur les articles 1382 et 1383 du Code civil ne s'en trouvent pas affectés. Tout au plus, il nous faudra désormais prendre en considération l'existence d'une série de comportements non susceptibles d'engager la responsabilité de leur auteur et la mise sur pied de présomptions réfragables[49] et conditionnées de non-responsabilité. Fondamentalement, nous restons toutefois dans l'orbite de notre droit commun et un novice ne sera pas perdu.

---

46 En ce sens lire E. CRABIT, "La directive sur le commerce électronique. Le projet Méditérranée", *Revue du Droit de l'Union Européenne,* 4/2000, p. 811. L'auteur confirme que "la directive ne cherche pas à élaborer un régime de responsabilité des prestataires de services intermédiaires, mais uniquement à clarifier la question de la non responsabilité des intermédiaires se livrant à trois types d'activités spécifiques".

47 Dans le même sens, E. MONTERO, *op.cit.,* Cahier du CRID n° 19, p. 278.

48 Ces devoirs existent déjà dans le droit belge et notamment dans la loi du 28 novembre 2000 relative à la criminalité informatique (*M.B.*, 3 février 2001, p. 2909), article 14 complétant l'article 109 ter, E, de la loi du 21 mars, dite loi Belgacom.

49 Nous prenons ici position sur l'incertitude relative à la charge de la preuve dénoncée infra.

Cela étant, le régime n'en est pas pour autant exempt de critiques en ce qu'il ne présente pas toujours la clarté voulue et l'unification prétendue.

B. Appréciation critique

La volonté de mettre fin aux divergences existantes entre les Etats membres et aux distorsions de concurrence est élogieuse. Néanmoins, le régime mis en place peut être critiqué au moins sur cinq points.

1. Le caractère non-contraignant de la disposition relative à l'identification des auteurs d'un acte illicite

L'article 15.2 de la directive dispose que les Etats membres ont la *faculté* d'instaurer l'obligation pour les prestataires de la société de l'information de communiquer aux autorités compétentes, à leur demande, «les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement ».
La directive laisse donc largement le choix aux Etats membres. Ces derniers restent libres de n'imposer aucune procédure, fût-ce-t-elle indirecte pour lutter contre l'anonymat sur Internet ou à tout le moins pour faciliter l'identification de ses acteurs.

Il est vrai que la question du droit au respect de l'anonymat apparaît sur Internet comme particulièrement controversée. « Les uns voient dans l'anonymat l'ultime rempart de la liberté et de la vie privée ; (…). Les autres redoutent l'anarchie et l'incivisme. (…) Toute la

difficulté consiste à trouver un équilibre entre la préservation, dans le cadre de la liberté d'expression, de l'*obligation de rendre compte*, appuyée par le principe d'identifiabilité, et ce droit à l'expression anonyme»[50].

Cela étant, l'analyse des décisions a révélé que l'anonymat a été, dans certains cas l'un des facteurs déclenchant la responsabilité des prestataires d'hébergement[51]. La directive met-elle fin à cette jurisprudence ?
Pour certains auteurs, il semble clair que l'exonération de responsabilité instaurée par la directive pour l'activité d'hébergement vaut seulement si le prestataire s'en tient à ce rôle. « En choisissant d'abriter des sites anonymes, on peut penser qu'il excède le rôle technique de fourniture d'un service de stockage d'informations. Le prestataire entre dans une logique de production ou d'édition de contenu. Dès lors, sur le plan de sa responsabilité, on change aussi de logique juridique : il ne peut bénéficier de l'exonération prévue à l'article 14 et se trouve ainsi soumis au droit commun »[52].

L'affirmation a été critiquée, faute de voir en quoi l'éventuel anonymat des hébergés affecterait la définition de la fonction d'hébergement visée à l'article 14-1 de la directive. Par ailleurs, la possibilité laissée aux Etats membres d'instaurer ou non une

---

50 E. DAVIO, "Anonymat et autonomie identitaire sur Internet", in *Cahiers du CRID,* n°16, p. 303 et p. 319 et les références citées.

51 On rappelera à cet égard que la Cour d'appel de Versailles a estimé que les obligations incombant à l'hébergeur doivent se traduire au stade de la formation du contrat par des mesures préventives telles que la prohibition de l'anonymat ou de la non-identification. Par ailleurs, dans l'affaire *Lacambre,*la Cour d'appel a condamné très nettement la possibilité laissée à l'anonymat sous le couvert duquel agissait l'éditeur du site litigieux. Ceci fait l'objet d'un rappel judicieux de C. ROJINSKY, "L'approche communautaire de la responsabilité des acteurs de l'Internet", disponible à l'adresse suivante: http://www.juriscom.net (consulté pour la dernière fois le 16 juillet 2001).

52 R. JULIA-BARCELO, E. MONTERO et A. SALAUN, *op.cit.,* p. 44.

obligation d'identification démontrerait que «le législateur européen n'a pas entendu réserver le bénéfice de l'exonération de responsabilité aux seuls hébergeurs assurant l'identification de leurs clients »[53].

La première affirmation nous semble maladroite à défaut d'éléments concrets qui en précise la portée. Sans doute les auteurs, qui s'inspire visiblement d'une décision de la cour d'appel de Paris[54], estiment-ils qu'à défaut de s'assurer de l'identité de la personne qui est l'auteur du message litigieux, le prestataire se substitue à lui.

La seconde vision nous paraît extrêmement dangereuse. Le maintien d'une obligation d'identification est une manière de mettre l'auteur d'un contenu litigieux face à ses responsabilités en l'incitant au respect des lois et des droits d'autrui. Ce dernier informé, au titre de l'obligation pré-contractuelle d'information et de conseil, du devoir du prestataire de communiquer l'identité de tout contractant dans certaines circonstances et moyennant le respect des dispositions légales relatives à la vie privée, saurait à quoi s'en tenir. Il craindrait la menace du couperet que serait une décision judiciaire le condamnant à indemniser toute victime d'un contenu illicite. En décider autrement serait encourager l'instauration d'un régime, qui non seulement immunise les prestataires de services mais également et, c'est plus grave, immunise les auteurs de contenu illicite, faute de pouvoir les identifier. Or, il nous semble que la philosophie générale de la directive procède d'une volonté d'éviter que la responsabilité des prestataires soit mise en cause alors même qu'ils n'ont pas la faculté de contrôler le contenu de ce qui est mis en ligne. Le législateur européen n'entend pas instaurer une immunité totale des acteurs de l'Internet, aussi respectueux qu'il soit du droit à la liberté d'expression. Le régime juridique mis en place ne doit donc pas

---

53 T. VERBIEST et E. WERY, *op.cit.,* p. 169.

54 Aff. *Estelle L. c/ Lacambre,* Cour d'appel de Paris, 10 février 1999, étudiée supra.

avoir l'effet pervers d'encourager l'immunité du véritable coupable, l'auteur de l'acte illicite.
En faisant preuve d'une certaine souplesse le législateur européen risque en outre de mettre à mal le processus d'unification des législations et des jurisprudences des Etats membres qu'il souhaite instaurer. Pourquoi pourrions-nous dans certains pays émettre ou éditer en toute impunité, faute de pouvoir être identifié, des sites attentatoires aux droits et libertés des individus alors que dans d'autres pays nous serions susceptibles d'être identifiés et condamnés ?

Nous plaidons dès lors pour le maintien d'une obligation de moyen[55] d'identification, légale ou jurisprudentielle, avec pour corollaire l'obligation d'en informer clairement les utilisateurs au stade pre-contractuel.
En Belgique, la loi du 28 novembre 2000[56] relative à la criminalité informatique impose déjà aux opérateurs de réseaux de communications et aux fournisseurs de service de communications, sous peine de sanctions pénales, "d'enregistrer et de conserver, pendant un certain délai en vue de l'investigation et de la poursuite d'infractions pénales, (…) les données d'appel de moyens de télécommunications et les données d'identification d'utilisateurs de services de télécommunications". Le champ d'application de la loi est théoriquement large, sous réserve de l'adoption d'un Arrêté Royal pris après avis de la Commission de la protection de la vie privée. Il couvre notamment, outre les opérateurs de réseaux de téléphone ou d'Internet, les fournisseurs d'accès Internet, de courriers électroniques, de forums de discussion, de *chat*, de services

55 Instaurer une obligation de résultat serait démesuré. En effet, les prestataires n'ont ni le droit (il s'agit d'un droit réservé à certaines entités publiques) ni les moyens de vérifier l'identité de chacun de leur abonné.

56 Loi du 28 novembre 2000 relative à la criminalité informatique (*M.B.*, 3 février 2001, p. 2909), article 14 complétant l'article 109 ter, E, de la loi du 21 mars, dite loi Belgacom.

de cryptographie ou de conservation de clés. Les données d'appel et d'identification comprennent également les adresses IP des ordinateurs émetteurs et récepteurs de la communication, le début et la fin de la connexion afin de pouvoir relier cette adresse IP à un utilisateur précis, le *log book* des prestataires de services, les adresses de site visité, voire la durée de ces visites, les adresses e-mails des messages échangés, tant de l'émissaire que du destinataire, l'identité réelle de la personne se cachant derrière un email ou une connexion anonyme etc.[57].

L'avant-projet de loi belge transposant la directive rappelle en son article 22§2 alinéa 2 que les prestataires sont tenus de communiquer aux autorités judiciaires ou administratives compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un contrat d'hébergement[58].

2. L'insécurité juridique générée par certains considérants

[57] Ces exemples nous sont livrés par F. de VILLENFAGNE et S. DUSSOLIER, "La Belgique sort enfin des armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique", *A&M,* 2000/1, p. 60 à 81 et spéc. p. 78 et s; sur ce sujet, voy. également les articles de C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique", *Formation CUP,* Liège, 2001, pp. 135-160; Y. POULLET, "A propos du projet de loi dit n°214. La lutte de la criminalité dans le Cyberspace à l'épreuve du principe de la régularité des preuves", in *Liber amicorum Jean du Jardin,* Bruxelles, Kluwer, 2001, p. 3 à 31. Ces auteurs se livrent à un excellent commentaire analytique et critique de la loi.

[58] Avant-projet de loi sur certains aspects juridiques des services de la société de l'information, *op.cit.,* supra, note 4.

Deux considérants de la directive sèment le trouble : Le considérant 44, succinctement présenté plus haut[59] et le considérant 48.

2.1. Le considérant 44

Pour rappel, ce considérant stipule qu' «un prestataire de services qui collabore délibérément avec l'un des destinataires de son service afin de se livrer à des activités illégales va au-delà des activités de « simple transport » ou de « catching » et, dès lors, il ne peut pas bénéficier des dérogations en matière de responsabilité prévues pour ce type d'activités ».

Mais quelle est donc la portée exacte de ce critère de responsabilité (« collaboration délibérée ») dérogatoire aux dispositions de la directive ? Le fait d'héberger anonymement un site suffit-il pour satisfaire à ce critère ? Une collaboration délibérée peut-elle se déduire d'une violation manifeste de droits notifiée au prestataire et laissée sans suite par ce dernier[60] ? Dans cette hypothèse quel serait alors la différence avec le régime juridique mis en place pour l'activité d'hébergement ?
Faut-il au contraire une action davantage positive impliquant une collaboration active dans la transmission ? Dans cette dernière hypothèse, pourquoi ne pas simplement avoir eu confiance aux conditions mentionnées aux articles 12 et 13 (notamment le fait de ne pas modifier ou sélectionner les informations faisant l'objet du transport ou du stockage).

2.2 Le considérant 48

Le considérant 48 précise que l'interdiction énoncée à l'article 15 en vertu de laquelle les Etats membres ne peuvent imposer aux

---

59 Voy. l'analyse de la directive consacrée à l'activité de simple transport et de stockage.

60 Voy. l'affaire Front 14 décrite plus haut.

prestataires de services une obligation générale de surveillance n'affecte en rien la possibilité qu'ont les Etats membres "d'exiger des prestataires de services qui stockent des informations fournies par les destinataires de leurs services qu'ils agissent avec les précautions que l'on peut raisonnablement attendre d'eux et qui sont définies par la législation nationale et ce, afin de détecter et d'empêcher certains types d'activités illicites" (c'est nous qui soulignons).

Selon nous, ce considérant est malheureux. Par sa rédaction imprécise, il ouvre à nouveau la porte à l'exigence d'un devoir de diligence dans le chef des prestataires et est par conséquent, même circonscrit, susceptible de mettre à mal l'ensemble du régime de la directive[61].

Par ailleurs, il pourrait conduire à l'instauration de mécanismes automatiques de censures[62], tels celui étonnamment préconisé par la décision du Conseil du 29 juin 2000 pour combattre la pornographie enfantine sur Internet[63]. En effet, quel choix serait laissé aux

---

61 Nous ne sommes pas convaincus que les Etats Membres et à leur suite les cours et tribunaux se rallieront aux propose de E. Crabit, selon lequel la volonté de l'union européenne consistait à ne porter en aucun cas atteinte à l'effet utile de la section 4 et pour qui "le fait qu'un l'opérateur ait manqué à une obligation visée dans ce considérant pourrait entraîner une sanction mais en aucun cas sa responsabilité dès lors qu'il peut se prévaloir de la disposition de l'article 14". Lire E. Crabit, *op.cit.*,p. 815.

62 Dans le même sens, E. MONTERO, in *Cahiers du CRID,* n°19, p. 289, pour qui " (…) ce considérant sème une certaine confusion. En paraissant ouvrir la voie à l'instauration légale de contrôles *a priori*, nous pensons qu'il met à mal l'économie générale du régime institué par les articles 14 et 15. A défaut de précisions supplémentaires, cette dernière éventualité porte en germe un risque de glissement vers la généralisation d'un contrôle *a priori*, d'une censure élargie, d'une part, et vers une objectivation de la responsabilité des hébergeurs d'autre part".

63 Council Decision of 29 May 2000 to combat Child pornography on the Internet, *J.O.,* 9 juin 2000. Cette décision impose aux Etats membres

prestataires confrontés à une législation qui leur prescrirait de prendre toutes les mesures utiles afin d'empêcher le développement de sites révisionnistes, terroristes et consacrés au plus vieux métier du monde. Devraient-ils supprimer tous les sites contenant le mot sexe, terrorisme et révisionnisme afin d'éviter toute responsabilité ?

3. Le manque de clarté sur l'étendue de la différence entre l'immunité pénale et civile des prestataires

Nous l'avons souligné au début de notre propos, le législateur européen a entendu régir à la fois les hypothèses de responsabilité pénale et civile des prestataires.

Néanmoins, le critère de différenciation entre ces deux types de responsabilité n'est pas toujours clair dans la directive. Ainsi, l'article 14 dispose, pour la fonction d'hébergement, qu'aucune responsabilité ne peut être engagée à condition que « le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicite et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance des faits ou des circonstances selon lesquels l'activité ou l'information illicite est apparente ».

Si nous comprenons à la lecture de la disposition que la responsabilité civile pourra être plus facilement engagée, nous restons néanmoins bien en mal de saisir la portée exacte du terme « connaissance effective ». Le droit pénal ne doit-il pas reposer sur une définition claire des infractions ?

---

d'examiner avec l'industrie, les possibilités d'établir leurs propres mécanismes de contrôle pour lutter contre les contenus de pornographie infantile.

4. La charge de la preuve

On a également reproché à la directive son imprécision concernant la charge de la preuve. En d'autres termes, sur qui repose la charge de prouver que les conditions d'exonération des prestataires sont réunies?[64] L'exonération est-elle de principe? Ou au contraire le prestataire doit-il démontrer qu'il a satisfait aux conditions lui permettant de bénéficier d'un régime de faveur ? Le législateur européen ne s'est pas prononcé sur cette importante question[65].

5. La mise sur pied d'une "justice privée"

La critique est notoire[66]. La directive souffre d'une carence et d'un manque de précision au niveau du critère de responsabilité mis en place à l'article 14.

En vertu de l'article 14, le prestataire n'encourt pas de responsabilité tant qu'il n'a pas connaissance du caractère illicite de l'activité ou de l'information auquel cas il doit agir pour retirer promptement les informations ou rendre l'accès à celles-ci impossible.

Il est assez surprenant que le législateur n'ait pas indiqué quand l'hébergeur est sensé avoir connaissance de l'élément litigieux. Faut-il une réclamation formelle ou une simple information à caractère public suffit-elle. Quid en cas de dénonciation anonyme ? Nous ne sommes pas convaincus par l'explication livrée par E. Crabit pour qui « les mécanismes de notification à l'intermédiaire par

---

64 *Ibid*. p. 285.

65 Avec E. MONTERO, nous penchons pour la première hypothèse. *Ibid.,* p. 286.

66 La plupart des commentateurs cités dans la note 1 critique cet aspect de la directive.

un tiers demandant le retrait de l'information illicite, les procédures de « notice and take down », doivent être particulièrement évolutifs et s'adapter en permanence à l'évolution du marché et des techniques. Pour répondre à ces contraintes, les codes de conduite paraissent plus adaptés que la méthode législative. (…) »[67].

En outre, en l'état, la directive confère au prestataire une compétence qu'il ne peut avoir et qu'il n'est pas en mesure d'exercer. Elle instaure une sorte de justice privée puisqu'elle octroie au prestataire, dans un domaine aussi délicat que celui lié à la liberté d'expression, le soin d'apprécier les contenus prétendument illicites. Il est légitime de se demander comment le prestataire pourra apprécier si tel ou tel contenu viole des droits intellectuels ou illicites au regard de telle ou telle loi[68]. Ce dernier se retrouve, comme nous l'avons vu, entre le marteau et l'enclume. S'il n'obtempère pas à la notification le priant de rendre impossible l'accès à une information illicite, sa responsabilité pourra être engagée. S'il obtempère mais que la notification s'avère par la suite téméraire et vexatoire, sa responsabilité pourra également être engagée à moins qu'il n'ait pris soin de bien s'exonérer de toute responsabilité dans le contrat le liant avec son client[69]. La directive – qui ne prévoit aucun régime de sanction pour les notifications abusives - aboutit ici au résultat opposé à celui qu'elle voulait atteindre en renforçant la précarité de la situation du prestataire. Il aurait été souhaitable d'instaurer un mécanisme clair avec des conditions objectives et précises de non-responsabilité.

---

67 E. CRABIT, *op.cit.,* p. 814.

68 Voy. l'exemple cité par E. MONTERO, *op.cit.,* p. 291, note 640. L'exemple d'une décision rendue en référé où le juge est confronté à des difficultés d'appréciations, illustre à suffisance l'embarras d'un prestataire d'hébergement qui n'a pas formation pour apprécier le bien-fondé des plaintes qui lui sont notifiées.

69 Même dans les Etats Membres qui instaureraient une procédure précise de notification et de retrait, il reste prudent de recommander aux prestataires d'en informer contractuellement les utilisateurs.

En Belgique, l'affaire Skynet[70] analysée plus haut illustre bien l'embarras du juge qui entend appliquer la directive tout en offrant une solution praticable. Le résultat offert par la décision est assez maladroit puisque le juge crée de toute pièce une procédure de notification en prévoyant un délai de réaction de trois jours.

L'avant-projet de loi belge actuellement en discussion, fort heureusement, prévoit la possibilité pour le Roi d'arrêter des procédures précises régissant la notification et le retrait des informations ou activités illicites[71].

6. Le champ d'application limité de la directive et l'instauration (même temporaire) d'un régime de responsabilité "à capacité duale"

Enfin, le champ d'application limité de la directive en terme d'activités visées est également critiquable. Le législateur européen ne souffle mot (à l'exception d'une mention à l'article 21 en envisageant un réexamen des dispositions) de la responsabilité des fournisseurs de liens hypertextes et de services de moteur de recherches et d'annuaire. Selon E. Crabit, ce silence s'expliquerait par le fait qu'au moment où la directive a été conçue, l'insécurité juridique qui découlait des jurisprudences nationales se trouvait essentiellement dans les activités de simple transport de catching et d'hébergement[72]. L'indexation automatique de sites illicites est-elle susceptible d'engager la responsabilité de la société qui met à disposition des utilisateurs le moteur ? L'hébergeur d'un site qui

---

70 Cour d'Appel de Bruxelles, 13 février 2001, jugement disponible et commenté sur http://www.droit-technologie.org. (consulté pour la dernière fois le 16 juillet 2001.

71 Article 21 §2 de l'avant-projet de loi sur certains aspects juridiques des services de la société de l'information, *op.cit.,* supra, note 4.

72 E. CRABIT, *op.cit.,* p. 813.

établit un lien vers un autre site à contenu préjudiciable engage-t-il sa responsabilité juridique ? Ces questions demeurent entières.

On peut s'en étonner tant les problèmes de responsabilité semblent se poser en des termes similaires (sous réserve de la responsabilité des services liés à la mise à disposition de moteurs de recherche où le rôle du prestataire dans la sélection de l'information semble plus important), outre les problèmes spécifiques relatifs à la liberté d'expression. En Belgique la majorité des décisions ont d'ailleurs trait à ce problème. Les auteurs sont nombreux à s'être penchés sur le problème[73] et tous semblent recommander une application par analogie des dispositions de la directive.

Le juge confronté à ces activités devra-t-il ou non raisonner par analogie en comblant le vide législatif ou au contraire appliquer sans restrictions les articles 1382 et 1383 du code civil en instaurant un régime de responsabilité à deux vitesses.

---

[73] Parmi une bibliographie abondante, voy. A. STROWEL, "Liaisons dangereuses et bonnes relations sur Internet. A propos des hyperliens", *A&M,* 1998/4, p. 296 à 308. A. STROWEL et N. IDE, "La responsabilité des intermédiaires sur Internet: actualités et question des hyperliens, deuxième partie, la responsabilité en matière des hyperliens", dossier asbl droit des nouvelles technologies, 2 février 2001, disponible à l'adresse suivante: http://droit-technologie.org (consulté pour la dernière fois le 25 août 2001); T. VERBIEST, "La responsabilité des outils de recherche sur Internet en droit français et en droit belge, dossier Juriscom, 30 avril 1999, disponible sur http://www.juriscom.net, (consulté pour la dernière fois le 16 juillet 2001), V. SEDALLIAN, "A propos de la responsabilité des outils de recherche", dossier Juriscom, 19 février 2000, disponible sur http://www.juriscom.net, G. DESGENS-PASANAU et J. GIUSTI, "La guerre contre les moteurs de recherche aura-t-elle lieu ?, dossier asbl droit des nouvelles technologies, 12 février 2001, disponible à l'adresse suivante: http://droit-technologie.org (consulté pour la dernière fois le 25 août 2001); Voy également A. LUCAS, *op.cit.,* spéc. p. 46 et s.

© Yves Poullet & Jean-François Lerouge

Les auteurs de l'avant-projet de loi belge ont quant à eux estimé qu'il était plus prudent de ne pas régler ces questions dans la loi de transposition pour éviter de se mettre en porte-à-faux par rapport à une intervention ultérieure du législateur européen.

© Yves Poullet & Jean-François Lerouge

V. CONCLUSION

Au terme de l'étude de la responsabilité des prestataires intermédiaires sur le Net, le bilan est assez contrasté. La directive ne déroge pas au droit commun de la responsabilité. Il faut s'en réjouir. Elle s'évertue à éviter que les fournisseurs de services ne constituent la parfaite victime face aux préjudiciés de l'Internet en raison de leur solvabilité et de leur identification aisée. Néanmoins, le législateur européen se montre trop frileux dans sa volonté d'uniformisation des règles juridiques régissant la responsabilité des prestataires intermédiaires de l'Internet. Se faisant, il est à l'origine de brèches ou d'incertitudes, sources d'insécurité juridique. Mal transposée, la directive pourrait créer plus de litiges qu'elle n'en évite. Il y a alors fort à parier que le bon sens des cours et tribunaux dans l'application des articles 1382 et 1383 sera encore fort sollicité.

A cet égard, on relèvera que le législateur belge semble partir dans la bonne direction en invitant le Roi à adopter progressivement des règles claires et objectives de partage de responsabilité en caractérisant de manière plus précise les obligations essentielles des prestataires (notamment en arrêtant des procédures précises régissant la notification et le retrait des informations ou activités illicites).

© Yves Poullet & Jean-François Lerouge

Chap. 2 : La responsabilité des autorités de certifications

Les communications et le commerce électronique exigent, à des fins de sécurité des transactions qui s'y concluent, des « signatures électroniques ». Le développement de la pratique de la « signature électronique » entraîne l'apparition de toute une série de services nouveaux. Ces services ne se limitent pas à la délivrance et à la gestion des certificats qui aident à leur authentification[74] mais à bien d'autres services, tel en amont les services d'enregistrement qui assurent la vérification de l'identité ou d'un attribut[75] de la personne qui se prévaut d'une signature électronique, tels en aval, les services d'annuaire ou de consultation qui permettent aux tiers l'accès au certificat.

Il est remarquable de constater que la directive européenne du 13 décembre 1998[76]- que la loi belge du 9 juillet 2001[77] a sur ce point copié servilement- ne traite premièrement que de la responsabilité des prestataires de service de certification et non des autres intervenants et, secondement, n'envisage que les seuls prestataires

74 Selon l'article 2 de la loi belge du 9 juillet 2001, *M.B.*, 29 sept. 2001, pp. 33070 et s. le certificat est : "une attestation électronique qui lie les données afférentes à la vérification de signature à une personne physique morale et confirme l'identité de cette personne ».

75 Ainsi, le fait que la personne est bien notaire, avocate, fonctionnaire ou qu'à l'intérieur de l'entreprise, elle occupe tel poste ou dispose de telle compétence.

76 Directive 1999/93/Ce du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques*, J.O.C.E.*, L.13, 19 janvier 2000, pp. 12 à 20.

77 Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *M.B.*, 29 sept. 2001, *op. cit.*, supra note 74.

délivrant des certificats dit qualifiés selon la terminologie européenne, c'est-à-dire des « attestations » satisfaisant à un certain nombre d'exigences[78]. Ces prestataires doivent par ailleurs répondre à un certain nombre de conditions[79]. La conjonction de ces différents types de conditions donne à la signature électronique avancée réalisée sur la base d'un certificat qualifié et conçu au moyen d'un dispositif sécurisé de création de signature électronique, une valeur équivalente à une signature manuscrite selon l'article 4 § 4 de la loi. L'absence de ces conditions ne prive pas la signature électronique de toute valeur dans la mesure où l'article 4 § 5 de la loi interdit au juge le rejet a priori d'une signature électronique pour ce seul motif[80].

Notre propos sera donc double. Il convient d'abord de s'interroger sur les dispositions légales. Les articles 14 et suivants de la loi à propos de la responsabilité des prestataires de service de certification délivrant des certificats qualifiés dérogent-ils aux règles classiques de la responsabilité ? Ensuite, dans la mesure où la loi n'évoque pas la question de leur responsabilité, que peut-on dire – en droit belge – de la responsabilité des autres intervenants, ainsi les autorités dites d'enregistrement qui, en amont des prestataires délivrant des certificats, vérifient l'identité ou les qualités des futurs titulaires de certificats ? Que peut-on dire de la responsabilité des prestataires délivrant des certificats non qualifiés ? **A propos de ces autres prestataires, la question de leur responsabilité mérite d'être posée : les exigences fixées aux annexes 1 et 2 de la loi, dont l'accomplissement est nécessaire pour prétendre à la qualité être**

78 … fixées par l'annexe 1 de la loi.

79 … fixées par l'annexe 2 de la loi.

80 Sur les principes d'équivalence et de non discrimination édictées en matière de signatures électroniques, le lecteur se réfèrera à une doctrine abondante. Parmi les auteurs, citons P. LECOCQ-B. VANBRABANT, « La preuve du contrat conclu par voie électronique », in *Le Commerce électronique : un nouveau mode de contracter ? Actes du colloque de Liège, 19 avril 2001*, Ed. Jeune Barreau de Liège, 2001, p. 105 et s.

© Yves Poullet & Jean-François Lerouge

« prestataire délivrant des certificats qualifiés, le respect de telles exigences[81]

I. Responsabilité et prestataires de services de certification délivrant des certificats qualifiés

Le régime minimal[82] de responsabilité prévu par la directive est devenu le régime légal belge. L'article 14 de la loi énonce les divers contenus des obligations de prestataire[83]. Il prévoit une obligation d'exactitude des informations contenues dans le certificat au moment non de sa consultation mais de son émission[84].

---

81 Ainsi l'annexe 2 : "Exigences concernant les prestataires de services de certification délivrant des certificats qualifiés" prévoit notamment que le prestataire doit enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai de 30 ans, utiliser des systèmes et des produits fiables, employer du personnel spécialisé, vérifier l'identité et les qualités spécifiques de la personne, etc.

82 Article 6 de la directive : « Les Etats membres veillent au moins … »

83 Sur ces obligations, lire M. ANTOINE, D. GOBERT, « La directive européenne sur la signature électronique », *J.T.D.E.*, 2000, p. 76 ; M.E. STORME, « De invoering van de elektronische handtekening in ons bewijsrecht », R.W., 2001, kol. 1518 et s. ; J. DUMORTIER, S. VAN DEN EYNDE, « De juridische erkenning van de elektronische handtekening in Belgie », *Computerrecht*, 2001, p. 193.

84 La date d'émission figure obligatoirement sur le certificat. Pour être complet, on ajoutera que le prestataire révoque un certificat lorsqu'il existe des raisons sérieuses pour admettre que le certificat a été délivré sur base d'informations erronnées ou falsifiées, que les informations contenues dans le certificat ne sont plus conformes à la réalité ou que la confidentialité des données afférentes à la création de signatures a été violée » (art. 12§ 2, 1°). L'article 12 voit dans cette possibilité de révocation du certificat plus un droit du prestataire qu'une obligation de ce dernier. Se pose dès lors la question : si le prestataire ne révoque point alors que des raisons sérieuses pouvaient et devaient lui être connues, est-il responsable ? L'article 14 ne prévoit pas ce cas. Il est difficile de tirer de cette absence de disposition expresse, une exonération de

Cette restriction s'explique tant par le rejet d'une obligation de contrôle permanent à charge du prestataire que par la volonté de mettre à charge du titulaire du certificat une obligation de mise à jour des données le concernant[85]. On notera au passage que l'obligation d'exactitude porte sur l'ensemble des informations contenues dans le certificat et vise donc des informations dont la présence n'est pas exigée par l'Annexe 1 pour que le certificat puisse être dit « qualifié ». Ainsi, si le certificat mentionne certains attributs, ces mentions doivent être exactes. Le fait que les informations mentionnées sur le certificat soient bien souvent vérifiées non par le prestataire mais par un tiers, l'autorité d'enregistrement, ne modifie rien à cette responsabilité du prestataire.

Certes, dira-t-on, c'est bien souvent le prestataire qui choisit l'autorité d'enregistrement et dès lors porte la responsabilité de cette dernière mais il se peut qu'exceptionnellement, tel ne soit point le cas, parce que l'autorité d'enregistrement dispose d'un monopole en la matière.
Ainsi, le prestataire de certificats mentionnant la qualité d'avocat doit entièrement se fier à l'Ordre qui lui a transmis une telle information. Ne peut-on considérer que dans ce cas, il serait injuste, nonobstant le prescrit légal, de lui faire porter la responsabilité pour l'erreur ou la faute d'un tiers qu'il n'a point choisi ?

La deuxième obligation porte sur l'obligation de vérifier la détention mais surtout la complémentarité des clés publique et privée, délivrées au titulaire lorsqu'elles sont générées par le prestataire lui-même. A

---

responsabilité du prestataire et les règles classiques de la responsabilité devraient à notre avis s'appliquer.

85 La loi prévoit d'ailleurs la possibilité pour le titulaire de certificat de le révoquer. Une question non réglée par la loi est celle où l'attribut dépend non d'une décision du titulaire mais de la reconnaissance d'un tiers comme un ordre professionnel pour la qualité de médecin.

contrario, cette obligation ne semble donc point viser les prestataires qui, ne générant pas eux-mêmes les clés, se contentent d'enregistrer la déclaration du titulaire. Cette réserve implicite a été à juste titre sévèrement critiquée par M. Antoine et D. Gobert[86]. Selon ces auteurs, l'obligation de vérification devrait peser sur tout prestataire de service de certification, qu'il soit ou non chargé de générer les clés privées et publiques. L'obligation de vérification est « fondamentale » dans la mesure où la certification, c'est-à-dire la confirmation du lien entre une personne et une clé publique, serait « vide de sens » si le prestataire ne vérifiait pas la complémentarité des clés.

La non-exactitude des mentions, la non-détention ou la non-complémentarité des clés entraînent-elles automatiquement la responsabilité du prestataire ? Deux réserves explicitement mentionnées conduisent à ne voir dans le texte qu'une simple présomption de responsabilité dans de tels cas. Ainsi, le prestataire est responsable à moins qu'il prouve n'avoir commis aucune négligence[87]. Il s'agit donc d'un simple renversement de la charge de la preuve. Mieux, sa responsabilité ne peut être engagée que vis-à-vis des personnes qui se sont fiées au certificat raisonnablement et en bon père de famille[88]. Ainsi, il ne peut être question pour le destinataire d'un message « apparemment signé par un émetteur dont le destinataire savait ou pouvait connaître la non-compétence du signataire ou son décès, de se prévaloir de la signature[89].

---

86 M. ANTOINE, D. GOBERT, *op.cit*., p. 77.

87 … ce qui implicitement revient à sanctionner toute faute même la plus légère du prestataire.

88 L'article 14bis de la loi stipule: "Un prestataire de service de certification… est responsable du préjudice causé à tout organisme ou personne physique ou morale qui, en bon père de famille, se fie raisonnablement à ce certificat …"

89 La loi type de la CNUDCI sur les signatures électroniques de la CNUDCI qui s'est tenue du 25 juin au 13 juillet 2001 (A/CN.9/WG.IV/W.P. 88. Les textes de la CNUDCI sont disponibles sur le site de la

Le non-enregistrement par le prestataire de la révocation opérée par le titulaire du certificat[90] entraîne selon l'article 14 § 2 la responsabilité du premier, sauf à prouver qu'il n'a commis aucune négligence ou que la personne qui se prévaut du certificat ne pouvait raisonnablement pas s'y fier.

Enfin, on notera à la suite de l'article 14 § 3 que la faute du destinataire d'un message qui se prévaut d'un certificat est présumée et exonère le prestataire de toute responsabilité lorsque ce destinataire a accepté un engagement signé alors que des limites d'utilisation du certificat à l'appui de cette signature avaient été exprimées par le prestataire, étaient « discernables » par les tiers et n'ont pas été respectées[91].

La lecture attentive des dispositions relatives à la responsabilité des prestataires de services de certification délivrant des certificats qualifiés conduit à affirmer que le régime mise en place par la

---

CNUDCI/UNCITRAL à l'adresse http://www.uncitral.org/english/texts/). La loi décrit longuement les "normes de conduite de la partie se fiant à la signature ou au certificat" (art. 11 de la loi-type) et réserve la protection de cette partie à celle qui a pu raisonnablement se fier à la signature électronique qui lui est présentée. "Une partie se fiant à une signature ou à un certificat assume les conséquences juridiques découlant du fait qu'elle s'est abstenue de :

a) prendre des mesures raisonnables pouré vérifier la fiabilité d'une signature électronique; ou,
b) si une signature électronique est étayée par un certificat, de prendre des mesures raisonnables pour :
   i) vérifier que le certificat est valide ou qu'il n' a pas été suspendu ou révoqué; et
   ii) tenir compte de toute restriction dont le certificat ferait l'objet".

90 Rien n'est dit à propos de la révocation de certificats ou de mentions de ces certificats opérée par des tiers (ainsi, la révocation par l'Ordre des avocats du certificat professionnel de ce dernier).

91 Même raisonnement à propos du dépassement de la valeur maximale des transactions (cf. §4 de l'article 14).

directive et à la suite par la loi belge, loin de déroger aux règles classiques de la responsabilité civile, cherche simplement à caractériser les obligations essentielles des trois principaux acteurs : celles du prestataire, de vérifier l'exactitude des données et la complémentarité des clés liées au certificat ; celles du titulaire de veiller à la confidentialité de ses clés, de mettre à jour les données contenues dans le certificat et, le cas échéant, de le révoquer[92]; celles du destinataire de prendre connaissance du contenu du certificat et d'en tirer les conséquences en cas de limitation d'utilisation y inscrites[93].

Ces obligations précises, qui incombent à chacune des parties, permettent de dessiner des lignes de partage de responsabilité que traduit l'article 14. Il n'y a là rien de dérogatoire au droit commun;

---

92 L'article 8 de la loi type de la CNUDCI résume comme suit les "normes de conduite du signataire": "

1. Lorsque des données afférentes à la création de signature peuvent être utilisées pour créer une signature ayant des effets juridiques, chaque signataire:
   a) prend des dispositions raisonnables pour éviter toute utilisation non autorisée de ses données afférentes à la création de signature;
   b) avise, sans retard injustifié; toute personne dont il peut raisonnablement penser qu'elle se fie à la signature électronique ou qu'elle fournit des services à étayer la signature électronique si:
      i) il sait que les données afférentes à la création de signature ont été compromises; ou
      ii) il estime, au regard de circonstances connues de lui, qu'il y a un risque important que les données afférentes à la création de signature aient été compromises;
   c) prend, lorsqu'un certificat est utilisé pour étayer la signature électronique, des dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat durant tout son cycle de vie ou devant figurer dans le certificat sont exactes et complètes.
2. Un signataire est responsable de tout manquement aux exigences visées au paragraphe 1."

93 Le projet de loi initialement discuté prévoyait expressément une obligation de vérification à charge de celui qui se fie à la signature ou au certificat. Comparer avec l'article 11 de la loi type de la CNUDCI sur la signature électronique cité supra note 21.

les standards de comportement de chaque acteur se voient simplement précisés.

On ajoutera que les dispositions de l'article 14 ne constituent pas le seul fondement de la responsabilité des prestataires. Bien d'autres obligations peuvent être déduites de l'annexe 2 qui fixe les exigences concernant les prestataires de service de certification délivrant des certificats qualifiés. Ainsi, le prestataire se doit-il, entre autres, « d'assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat », « de prendre des mesures contre la contrefaçon des certificats », « d'utiliser des systèmes et produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument ».

Il s'agit d'autant d'éléments qui relèvent de l'essence même du service de certification. On note que ces divers contenus d'obligation ne sont pas mentionnés à l'article 14 et que le contenu des standards de comportement qui sont induits par de telles exigences sera souvent fixé par des normes techniques ou organisationnelles dont on ne peut que réclamer l'adoption[94].

Le caractère incomplet de l'article 14 se constate aussi par le fait qu'aucune règle relative à l'étendue du dommage susceptible d'être réparé n'y est reprise. On appliquera sur ce point les règles du droit commun. Vis-à-vis du titulaire de certificat, rien n'interdit les clauses limitatives de responsabilité sous réserve bien évidemment

[94] A noter à ce propos, la reference explicite à de telles normes au point (e) de l'annexe 2 : "…, ils doivent également appliquer des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues ». Même remarque à propos du devoir d'utiliser des systèmes et produits fiables assurant la sécurité technique et cryptographique des fonctions qu'ils assument.

des règles de protection des consommateurs et des limites jurisprudentielles classiques.

En particulier, toute clause de limitation de responsabilité qui viderait le contrat de sa substance sera considérée comme nulle. Dans la mesure où la loi belge et ses annexes décrivent la substance des prestations du service délivrant un certificat agréé, on peut en déduire que toute clause contractuelle par laquelle directement ou indirectement le prestataire s'exonérerait substantiellement des prestations y prévues serait nulle.

Ainsi, l'annexe 2 insiste sur l'obligation d'offrir un annuaire des certificats à accès rapide et sûr. Il est évident que des clauses prévoyant une irresponsabilité totale ou partielle du prestataire pour toute panne du serveur, rendant l'annuaire inaccessible sont contraires à l'essence même du service et seront considérés comme nulles. Même remarque à propos d'autres obligations induites par l'annexe 2, comme celle d'offrir un service de révocation sur et immédiat, d'employer des procédures et méthodes administratives ou de gestion appropriées.

Vis-à-vis des tiers qui, en bon père de famille, se sont fiés raisonnablement aux données du certificat et aux limites y reprises explicitement, le prestataire sera tenu des seuls dommages dont l'existence est une conséquence directe de la violation des standards de comportement fixés par l'article 14 et l'annexe 2. Ceci exclut – des dommages pour manque à gagner, économies réalisées ou occasions perdues[95]. Ainsi, le tiers qui s'est fié à un certificat faux,

[95] La loi du Missouri (Signature Act, 1998 (1998, S.B. 680)) le prévoit expressément : "Est tenu, uniquement, en cas d'action en dommages-intérêts pour préjudice imputable à la confiance accordée au certificat, de verser des dommages-intérêts compensatoires directs ne comprenant pas :

a) des dommages-intérêts à titre de sanctions en des dommages-intérêts exemplaires ;

ayant fait l'objet d'une révocation et a conclu un contrat, ne pourra pas obtenir réparation pour le fait que la conclusion du contrat sur base de ce certificat faux lui a fait perdre l'occasion de contracter ailleurs sauf à démontrer par exemple en cas d'enchères, le lien direct et immédiat entre l'attribution du contrat au moins disant sur base d'un faux certificat et la perte d'autres opportunités de contracter.

II. Responsabilité et prestataires de services de certification délivrant des certificats non qualifiés

L'introduction mettait en évidence le caractère limité des dispositions de la loi belge sur la responsabilité. Que faut-il en déduire en ce qui concerne la responsabilité des prestataires de services de certification délivrant des certificats non qualifiés ?

Sans doute, faut-il sur ce point renvoyer au droit commun de la responsabilité ! A cet égard, quelques considérations pourraient guider la réflexion en la matière.

La première est offerte par la considération déjà énoncée suivant laquelle la responsabilité du prestataire doit se mesurer au degré de confiance susceptible d'être attendu par celui qui se prévaut du certificat. En d'autres termes, si un certificat ne présente pas les qualités requises pour être qualifié, il est normal que la partie destinataire d'un message ne puisse s'attendre à la même fiabilité du certificat. Ainsi, la partie qui entend se fier à une signature électronique doit s'interroger sur le caractère raisonnable de la

b) des dommages pour manque à gagner, économies non réalisées ou occasions perdues, ou
c) un pretium doloris

confiance à accorder au certificat émis. C'est à lui que revient ce devoir d'évaluation et de vérification[96].

Sans doute, appartient-il, au prestataire de service de certification de l'informer à cet égard et d'énoncer clairement sa politique[97] : ainsi décrira-t-il les procédures utilisées quant à la vérification de l'identité et des qualités de celui qui est certifié, les garanties de sécurité des procédures de génération de clés, utilisées la qualité du service de mise à jour et de révocation, enfin, les systèmes, les procédures et ressources humaines utilisées pour la prestation de ses services[98] C'est en effet sur base de cette information, que celui qui se prévaut d'une signature peut juger de la fiabilité de celle-ci. Toute information fausse ou erronée de la part du prestataire se retournera donc contre lui[99].

---

96 " En outre, l'établissement d'une norme de conduite en vertu de laquelle la partie qui se fie à la signature devrait vérifier la fiabilité de cette dernière par des moyens facilement accessibles peut être considéré comme essentiel au développement de tout système d'infrastructure publique » (Projet de guide pour l'incorporation dans le droit interne de la loi type de la CNUDCI sur les signatures électroniques, A/CN.9/493).

97 L'article 9 de la loi type de la CNUDCI sur les signatures électroniques (A/CN.9/493) énonce : que le prestataire

a) « agit en conformité avec les déclarations qu'il fait concernant ses politiques et pratiques »

b) prend des dispositions raisonnables pour assurer que toutes les déclarations qu'il fait concernant le certificat durant tout son cycle de vie ou figurant dans le certificat sont exactes et complètes ».

98 L'article 10 de la loi type CNUDCI énonce: "… pour determiner si, ou dans quelle mesure, tous systèmes, procedures et resources humaines utilisées par ….

99 Ainsi, le prestataire qui prétend satisfaire aux conditions des annexes 1 et 2, et donc être un prestataire de services de certification délivrant des certificats qualifiés, supportera la responsabilité plus lourde prévue à l'article 14 alors même qu'il s'avèrerait lors du contrôle de ces prestataires prévus par l'article 20, que le service offert ou la qualité des certificats émis ne correspondent pas aux exigences légales.

La seconde réflexion s'interroge sur les prestations essentielles d'un prestataire de service de certification, c'est-à-dire sur les prestations qui forment l'objet même du service de certification et auxquelles ce service ne pourra se soustraire même si le prestataire de ce service, comme nous l'avons indiqué plus haut, peut les moduler et dès lors accroître ou à l'inverse diminuer la fiabilité de l'information fournie par le certificat. Ces prestations peuvent s'énoncer comme suit :

- l'identification du signataire : s'agit-il d'une identification sur simple déclaration de celui-ci, d'une vérification par un tiers et par quel tiers, etc. ?
- la publication de données relatives au signataire : s'agit-il de reproduire des données fournies par le titulaire du certificat ou les données attestées par des tiers ? Par quel tiers ? etc.
- la conservation et la mise à jour de ces données : quelles mesures de sécurité organisationnelles et techniques sont utilisées ? Quelle est la fréquence de la mise à jour ? Comment s'opère cette mise à jour ?
- la mise sur pied d'un service de révocation : les questions de l'accessibilité de ce service et de la rapidité du traitement des demandes sont cruciales à cet égard.
- La mise à disposition d'un service d'annuaire : à nouveau, l'accessibilité à ce service, la rapidité de sa mise à jour sont déterminantes.
- La vérification de la concordance des clés publiques et privées : est-elle opérée par le prestataire ou se contente-t-on à cet égard de simple déclaration du titulaire ? Vérifie-t-on si les données afférentes à la création de signature sont toujours valides et n'ont point été compromises ?

La troisième réflexion met en jeu le troisième acteur, à savoir le titulaire du certificat. Moins le service de certification auquel il recourt est fiable, plus ses obligations et ses devoirs de vigilance seront importants et toute violation de celles-ci ou de ceux-ci

permettront aisément au prestataire de se dégager de sa responsabilité vis-à-vis du tiers qui se prévaut du certificat. Illustrons le propos : Alors que dans le service de délivrance de certificats qualifiés, la vérification des données inscrites sur le certificat incombe au prestataire, il peut ne pas en être de même pour des certificats de moindre qualité. C'est au demandeur d'un certificat qu'incombe l'obligation de veiller à ce que les informations qui seront publiées soient « exactes, complètes et faites de bonne foi »[100]. **Autre exemple, le fait que le service de révocation offert par le prestataire ne permette pas une mise à jour rapide, oblige le titulaire du certificat à prévenir des possibilités d'utilisation non autorisée de sa signature, certains tiers auprès desquels des messages seront selon toute probabilité envoyés.**

Conclusions

La création de signatures électroniques et leur utilisation, d'une part, la création, la tenue et la vie des certificats qui y sont liés et permettent leur utilisation, d'autre part, soulèvent nombre de questions de responsabilité dont bien peu sont évoquées par la loi belge du 9 juillet 2001.

Il est regrettable que celle-ci - mais la directive elle-même n'en souffle mot – n'ait pas mieux mis en évidence les « devoirs »de chaque acteur. Sans doute, comme nous l'avons montré, ces devoirs varient. Plus le service offert par le prestataire est de qualité, moins

[100] « Toutes les déclarations faites par le titulaire à une autorité de certification dans le but d'obtenir un certificat, y compris toutes les informations connues du titulaire et figurant dans le certificat, sont exactes, complètes et faites de bonne foi, qu'elles soient confirmées ou non par l'autorité de certification ». Nous reprenons ici l'article 37 de la loi de Singapour (Electronic Transactions Act 1998). La directive européenne ne souffle mot de ce devoir essentiel du titulaire.

le détenteur de certificat sera obligé et plus le destinataire du message, ainsi certifié pourra se fier raisonnablement au certificat émis.

L'article 14 de la loi belge traduit donc de manière bien incomplète ces principes. En outre, faute d'avoir mis en évidence préalablement les obligations de chaque acteur, le législateur ne permet pas d'appréhender facilement certains termes que pourtant il utilise, ainsi, que signifie concrètement la notion de destinataire qui se fie raisonnablement et de bonne foi à un certificat ou à ses mentions. Plus grave, il n'indique pas au juge la façon dont celui-ci devra trancher lorsque la situation concrète ne permettra pas – et ce sera fréquemment le cas – l'application de l'article 14.

Notre propos était modestement de tenter de lui servir de guide. Au terme de la réflexion, il apparaît en tout cas qu'en matière de signatures électroniques, le juge ne doive pas s'écarter des règles traditionnelles de responsabilité.

Simplement, ayant précisé les obligations de chaque acteur, il déterminera la mesure dans laquelle chaque acteur s'est comporté fautivement ou non, avant de répartir ou non les responsabilités.

© Yves Poullet & Jean-François Lerouge

Chap. 3 : LES PROBLEMES DE RESPONSABILITE LIES A L'UTILISATION DE MOYENS DE PAIEMENTS ELECTRONIQUES SUR LE NET

L'essor du commerce en ligne dépend pour partie du développement de moyens de paiements sûrs et efficaces. Les acteurs de l'Internet l'ont bien compris et on assiste actuellement avec plus ou moins de succès à l'émergence d'une pléthore de nouveaux moyens de paiement[101].

[101] Pour une étude détaillée sur les différents modes de paiement électronique et sur leur implication juridique, voy. par exemple J.-F. LEROUGE, "Le paiement sur Internet et le respect de la vie privée", *DAOR*, n°58, p. 88 à 102*;* L. EDGAR, *Electronic Commerce Legal Issues Platform, Electronic Payment Systems, Delverable 2.1.6,* Projet Esprit 27028, disponible à l'adresse suivante: <http://www.jura.uni-muenster.de/eclip/>, (dernière consultation, 19 octobre 2000). Voy. également M. H. BOULANGER, *Internet et les moyens de paiement,* mémoire présenté en vue de l'obtention du grade de licencié en Sciences Economiques, FUNDP, 1998, 115 pages. Voyez également comme exemples non exhaustifs les sites offrants ces nouveaux moyens de paiement tels que <http://www.emoneymail.com>, <http://www.amazonpayments.com>, <http://www.cybergold.com>, <http://www.cybercash.com>, <http://www.mondex.com>, http://www.proton.be etc. Pour un aperçu des problèmes de responsabilité générés pour les paiements par wap, lire E. MONTERO, "Transferts électroniques de fonds, le paiement par Wap, *Cahier AEDBF*, n°13, 2001, p. 165-186.

Les risques de fraude ne sont toutefois pas absents. Bien souvent, ils sont à l'origine de réticences de la part des consommateurs. Sont-elles justifiées ?

En droit européen, au minimum trois textes juridiques abordent cette question: (i) la recommandation de la Commission européenne du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation émetteur et titulaire[102] (ci-après la recommandation), (ii) et (iii) les deux directives européennes relatives aux conditions d'émission de la monnaie électronique[103].

Le but avoué de la recommandation est d'offrir un régime juridique clair afin d'assurer un degré élevé de protection des consommateurs dans l'utilisation des instruments de paiement électronique[104].

La Commission a délibérément choisi d'adopter un texte juridiquement non contraignant mais a indiqué son souhait de contrôler son implémentation et, si nécessaire d'adopter une directive. La recommandation a récemment fait l'objet d'un appel d'offres ayant pour but de procéder à l'évaluation de la mise en œuvre effective de la Recommandation au sein de l'Union.

---

102 Commission Recommendation concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, *O.J.,* L.208, 02.08.1997, p.52.

103 La directive 2000/28/CE du Parlement européen et du Conseil du 18 septembre 2000 modifiant la directive 2000/12/CE concernant l'accès à l'activité des établissements de crédit et son exercice et la directive 2000/46/CE du Parlement européen et du Conseil du 18 septembre 2000 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements*, J.O.,* 27/10/2000, L 275/39.

104 Considérant 8 de la Recommendation.

Les conclusions de cette étude sont publiées sur le site de la Commission et sont révélatrices[105]. A l'heure actuelle, seul le Danemark aurait correctement implémenté la Recommandation[106]. Le Luxembourg a récemment adopté un texte reprenant la plupart des dispositions de la Recommandation[107]. La Belgique entend faire figure de bon élève et a témoigné son intention de mettre en œuvre l'ensemble des dispositions de la recommandation en adoptant un avant-projet de loi[108]. Pour l'heure, ce dernier semble toutefois sommeiller.

En l'état, seules certaines dispositions légales visées par la recommandation protègent actuellement le titulaire belge d'un moyen de paiement électronique. Nous nous attarderons donc principalement sur ces dispositions, amenées à être complétées par un nouvel arsenal juridique. Nous négligeons à dessein l'analyse des directives sur la monnaie électronique; le droit de la responsabilité n'y étant abordé que de manière indirecte et leur implémentation n'étant actuellement pas à l'ordre du jour.

---

105 Call of Tender n°XV/99/0141/C*, O.J.*, January 16, 1999, S. 11/29. Pour les conclusions de l'étude, voy. http://europa.eu.int/comm/internal_market/en/finances/payment/instrument/parta.pdf

106 The Electronic Payment Instrument Act, adopté le 26 mai 2000 et entré en vigueur depuis le 1er juillet 2000.

107 Loi du 14 août 2000 relative au commerce électronique modifiant le Code civil, le Nouveau Code de procédure civile, le Code de commerce, le Code pénal, et transposant la directive 1999/93 relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance de biens et services autres que les services financiers, publiée au Mémorial A n°96 du 8 septembre 2000, p.2176 (doc.parlementaires n°4641).

108 Projet de loi relatif aux opérations effectuées au moyen d'instruments électroniques de transfert de fonds approuvé par le conseil des Ministres le 23.06.2000.

© Yves Poullet & Jean-François Lerouge

L'objet de ce chapitre vise essentiellement à démontrer succinctement qu'en droit belge les consommateurs ne doivent pas craindre d'avoir à supporter les pertes financières consécutives à une utilisation frauduleuse de leur instrument électronique de paiement sur le Net. Nous insisterons particulièrement sur les responsabilités particulières mises à charge d'un acteur important du développement du commerce en ligne : l'émetteur d'un moyen de paiement électronique.

Analyse des dispositions légales

La matière est principalement régie à l'article 81§5 de la loi du 14 juillet 1991[109] sur les pratiques du commerce et sur l'information et la protection du consommateur[110]. Cette loi a un champ d'application assez limité puisqu'elle ne concerne que les relations entre vendeurs[111] et consommateurs[112].

---

109 Pour un commentaire général de cet article, lire A. SALAÜN, Transposition de la directive contrats à distance en droit belge : commentaire de l'article 20 de la loi du 25 mai 1999, *J.T.,* 8 janvier 2000, p. 43 et s.

110 Pour être complet, il convient de mentionner également l'article 61 de la loi du 12 juin 1991 relative au crédit à la consommation qui contient des dispositions fort similaires, quoique moins formelles, à la loi du 14 juillet 1991 pour les instruments de paiement conféranr une ouverture de crédit.

111 Au sens de l'article 1 de la même loi, un vendeur est "tout commerçant ou artisan ainsi que toute personne physique ou moralequi offrent en vente ou vendent des produits ou des services, dans le cadre d'une activité professionnelle ou en vue de la réalisation de leur objectif statutaire; des organismes publics ou les personnes morales dans lesquelles les pouvoirs publics détiennent un intérêt prépondérant qui exercent une activité à caractère commercial, financier ou industriel et qui offrent en vente ou vendent des produits ou des services; les personnes qui exercent avec ou sans but de lucre une activité à caractère commercial, financier ou industriel, soit en leur nom propre, soit au nom ou pour le compte d'un

L'article 81§5 dispose que "(…) L'émetteur d'un instrument électronique de fonds doit mettre à la disposition du consommateur les moyens appropriés pour que celui-ci puisse adresser une notification, en cas de perte, de vol, ou d'utilisation frauduleuse dudit instrument. Le consommateur doit notifier à l'émetteur ou à l'entité désignée par celui-ci, dès qu'il en a connaissance :

la perte ou le vol de l'instrument de transfert électronique de fonds ou des moyens qui en permettent l'utilisation;
toute utilisation frauduleuse de l'instrument. (…)"

Nous nous proposons d'en un premier temps de nous attarder sur la définition des notions d'émetteur et d'instrument de transfert électronique de fonds. Nous étudierons ensuite le régime mis en place par la loi belge à la suite de la Recommandation.

La notion d'instrument de transfert électronique de fonds

La loi belge ne définit pas la notion de "transfert électronique de fonds".

L'exposé des motifs de la loi s'appuie toutefois sur la définition donnée par la recommandation à la notion d'"instrument de paiement électronique"[113].
La notion d'instrument de paiement électronique est définie par la recommandation comme étant un instrument permettant à son titulaire d'effectuer le type d'opération décrit à l'article 1er

---

tiers doté ou nom de la personnalité juridique, et qui offrent en vente ou vendent des produits ou des services".

112 Par consommateur, la loi entend toute personne physique ou morale qui acquiert ou utilise à des fins excluant tout caractère professionnel des produits ou des services mis sur le marché.

113 Exposé des motifs, documents de la chambre des représentants, sess.ord., 10 mars 1999, projets n°2050/1 et 2051/1-98/99, p. 33.

paragraphe 1 *(c'est-à-dire le transfert de fonds et le retrait d'argent liquide)*[114]. Ceci couvre à la fois les instruments de paiement d'accès à distance et les instruments de monnaie électronique[115]. Les paiements par intermédiaire n'entrent cependant pas dans le champ d'application de la recommandation. On peut s'interroger sur la notion d' « instrument ». Ce terme n'est pas défini par la recommandation et la question de savoir s'il concerne uniquement les éléments tangibles n'est pas claire[116]. Dans l'affirmative, cela signifierait que les porte-monnaie virtuels n'entrerait ni dans le champ d'application de la recommandation, ni par conséquent dans celui de la loi belge.

2. La notion d' "émetteur"

La loi belge reste également silencieuse sur la notion d'"émetteur". On peut s'en étonner étant donné l'importance de la notion.

La recommandation définit l'émetteur d'un instrument de paiement comme étant une personne qui, dans le cadre de son activité commerciale, met un instrument de paiement à la disposition d'une autre personne, conformément à un contrat conclu avec celle-ci[117].

La pertinence de cette définition prête à discussion. En effet, un site web de services peut très bien avoir reçu une licence de commercialisation d'un système de paiement et s'être vu octroyer le droit de proposer cette méthode de paiement à un visiteur, sans toutefois en assurer la gestion, tant au niveau de la sécurité qu'au niveau de la réalisation de la transaction. Suivant la définition, ce

114 Le terme paiement n'est toutefois pas défini par la recommandation. Il peut être compris comme étant l'exécution d'une obligation qui a pour objet une dette d'argent.

115 Article 2 de la recommandation.

116 L'on relèvera que l'article 39/2 évite soigneusement l'utilisation du terme "instrument", optant pour l'appellation générique de "tout moyen".

117 Article 2 (e) de la Recommandation.

sont toutefois les administrateurs de ce site qui mettent à la disposition du public l'instrument de paiement, suivant leurs conditions générales. Ils seront dès lors considérés comme émetteurs au sens de la recommandation, ce qui incontestablement pose problème au niveau de la possibilité effective de respecter les obligations mises à leur charge que nous identifierons ci-après.

Une définition calquée sur l'approche suivie par la Directive 2000/46/CE du Parlement européen et du Conseil du 18 septembre 2000 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements[118] nous paraîtrait plus heureuse. La Directive se réfère aux institutions de monnaie électronique, en les définissant comme des entreprises qui émettent des moyens de paiement sous la forme de monnaie électronique[119].

3. Analyse des dispositions relatives à la responsabilité

3.1 Régime général

La loi reprend partiellement le régime juridique proposé par la recommandation. Elle instaure un système de responsabilité autour du principe de notification à l'émetteur de toute perte, vol ou utilisation frauduleuse de l'instrument de paiement encourue par le titulaire.

---

118 Article 1 de la directive, JO 27/10/2000, L 275/39, disponible à l'adresse suivante <http://europa.eu.int/eur-lex/fr/oj/2000/l_27520001027fr.html>.

119 L'article 1er §3 (b) définit la monnaie électronique comme étant une valeur monétaire représentant une créance sur l'émetteur qui est:

(i) stockée sur un support électronique;

(ii) émise contre la remise de fonds d'un montant dont la valeur n'est pas inférieure à la valeur monétaire émise;

(iii) acceptée comme moyen de paiement par des entreprises autres que l'émetteur.

La responsabilité est placée dans le chef de l'émetteur avant la notification pour toutes les pertes financières consécutives à une perte, au vol, ou à l'utilisation frauduleuse de l'instrument par un tiers au-delà d'un montant de EUR 150.

Si l'émetteur parvient à prouver que le consommateur a agi avec une négligence grave ou frauduleusement, la responsabilité de principe de l'émetteur pourra être atténuée ou remise en cause. Dans le premier cas, le plafond limite de responsabilité du consommateur peut être porté à un montant fixé par Arrêté Royal. A notre connaissance, cet Arrêté Royal n'a toutefois pas encore été adopté. Il faut donc s'en tenir pour l'heure au montant minimal de EUR 150. Dans le second cas, l'émetteur ne sera pas responsable. Le titulaire de l'instrument de paiement électronique est par conséquent totalement exonéré de toute responsabilité au-delà de la somme de EUR 150. Après la notification, l'émetteur devra supporter seul toutes les pertes.

L'émetteur se voit donc actuellement dans l'obligation d'assumer les pertes financières supérieures à EUR 150 même si une négligence grave peut être reprochée au consommateur. Le système mis en place par la loi a certes pour mérite d'éviter toutes les controverses relatives à la notion de négligence grave trop souvent invoquée par les émetteurs. Néanmoins, il instaure une responsabilité de principe dans le chef de l'émetteur qui, sauf fraude avérée de la part du consommateur, devra pratiquement toujours assumer les pertes financières liées à l'utilisation du moyen de paiement électronique.

3.2. Le cas des instruments de paiement utilisés sans moyen d'identification

Lorsque l'instrument de transfert électronique de fonds est utilisé sans présentation physique ou identification électronique, la responsabilité du consommateur ne pourra, sauf fraude avérée,

jamais être engagée, même dans l'éventualité où aucune notification n'aurait eu lieu.

La loi, reprenant la disposition de la recommandation précise que "la seule utilisation d'un code confidentiel ou de tout élément d'identification similaire n'est pas suffisante pour engager la responsabilité du titulaire".

La volonté du législateur consiste à décourager l'utilisation sans présence physique ou sans identification électronique de l'instrument de paiement en raison du manque de sécurité.

La loi pêche toutefois par un défaut de clarté puisqu'on est bien en mal de déterminer avec précision ce qu'un émetteur doit faire pour éviter de tomber dans le champ d'application de cette dérogation.

De ces considérations, il ressort que les émetteurs ont l'intérêt, puisque les risques sont à leur charge, de mettre en place des systèmes ne permettant plus une utilisation aussi facile de l'instrument de transfert de fonds sur le Net. S'ils veulent avoir une chance d'échapper au prescrit légal dérogatoire et retomber dans le régime de notification étudié plus haut, ils doivent veiller à instaurer des systèmes techniques assurant de manière certaine l'identification du titulaire de l'instrument de transfert de fonds. Le problème d'identification certaine des acteurs de l'Internet trouve également ici un écho particulièrement important.

4. Une dérogation au droit commun de la responsabilité?

Le système mis en place par la loi déroge au droit commun de la responsabilité en instaurant, moyennant certaines conditions, une responsabilité objective dans le chef de l'émetteur. Ce dernier ne peut s'exonérer de cette responsabilité que s'il apporte la preuve de

la fraude du titulaire du moyen de paiement ou, dans une moindre mesure, sa négligence.

Pour bénéficier de la protection instaurée par la loi, le législateur impose au consommateur le respect d'une formalité (la notification) dans l'exercice de son devoir de diligence. Le respect de cette formalité peut être analysé comme étant une manière particulière d'exercer son devoir de diligence au titre de l'article 1383 du Code civil.

La preuve du respect de l'obligation de diligence, objectivée par le système de la notification semble donc conditionner le déclenchement corollaire du système de responsabilité objective.

CONCLUSION

La loi belge transpose de manière servile certaines des dispositions essentielles de la recommandation. Elle a toutefois un champ d'application assez limité comparé à la recommandation qui ne se contente pas de viser que les consommateurs. Elle fait l'impasse sur une série importante de dispositions dont les règles relatives à l'exécution incorrecte de l'ordre de paiement ou aux informations minimales à fournir relativement aux conditions d'émission et d'utilisation d'un instrument de paiement électronique. Rien d'étonnant dès lors que les consommateurs ne se sentent toujours pas en confiance au moment de régler leur transaction en ligne.

© Yves Poullet & Jean-François Lerouge

Chap. 4 : Responsabilité et données nominatives

L'article 23 de la directive 95/46[120] relative à la protection dite des données personnelles reconnaît le droit de la personne concernée d'obtenir du responsable la réparation des dommages subis « du fait » d'un traitement illicite ou de toute action incompatible avec les dispositions prises en exécution de la directive[121]. La possibilité d'une exonération totale ou partielle du responsable au cas où il démontre la non imputabilité du fait qui a provoqué le dommage est affirmée par l'alinéa 2 du même article. L'article 15bis de la nouvelle loi du 11 décembre 1998[122] transposant la directive reprend le principe de la directive mais l'exprime en des termes différents : « le responsable du traitement est responsable du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi. Il est exonéré de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable ».

---

120 Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, 281/31, 23 novembre 1995.

121 A noter que l'article 23 ne couvre pas la responsabilité pénale mais bien à la fois la responsabilité contractuelle et aquilienne. Il nous paraît que les dispositions de l'article 23 sont impératives et que des clauses contractuelles ne pourraient y déroger.

122 Loi du 11 décembre transposant la directive 95/46/CE du 24 octobre du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *M.B.*, 3 février 1999, p. 3049 et s. Cette nouvelle loi intervient par la voie de modification de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Dans le présent article, toute référence à un article de la "nouvelle loi" vise l'article de la loi de 1992 telle que modifiée par la loi du 11 décembre 1998.

On notera que ce qui était une simple possibilité de cause d'exonération laissée à la discrétion des législateurs nationaux est, par la volonté du législateur belge, cause automatique d'exonération.

L'interprétation du texte européen n'est point aisée. Faut-il considérer que l'article 23 ne modifie rien au régime classique de la responsabilité ou faut-il au contraire y voir une forme de responsabilité objective ? L'article 23 est en effet susceptible d'une double interprétation.

L'illicéité du traitement peut se référer à la conduite concrète du responsable du traitement : Chaque Etat membre appréhendera celle-ci selon son système de responsabilité, la portée du texte se limitant à l'affirmation du droit à réparation dans le chef de la personne concernée. Cette dernière devra donc rapporter la preuve de la responsabilité du responsable du traitement selon le droit commun applicable. « L'illicéité du traitement pourrait aussi se référer au fait même qui génère le dommage. Dès que ce fait est contraire à une disposition de la directive, il serait illicite. L'illicéité n'est alors plus liée au dommage (…). Si un fait peut être considéré comme illicite, le responsable du traitement en sera présumé responsable même si a priori aucune faute ne peut lui être imputée. Le texte ne parle pas de faute mais seulement du fait d'un traitement illicite. Le responsable du traitement ne pourra alors s'exonérer qu'en apportant la preuve que le fait ne lui est pas imputable »[123].

---

[123] CEDIB (Université des Baléares), CRID (FUNDP), *Intégration des réglementations de protection des données au sein des réseaux EDI*, étude PROTEDI, 1996, 163-167, publiée par la Commission européenne. Sur cette question, on renverra le lecteur à la thèse de P. GRIMALT, La responsabilitad civil del responsable del fichero en la Ley organica de regulacion del tratamiento de la datos de caractere personal, Thèse, 1998, Palma de Mallorca. Un bon résumé des discussions menées par l'auteur peut être trouvé dans son article; "La responsabilité civile résultant d'un traitement de données à caractère personnel selon la directive n° 95/46/CE

Le texte belge[124] ne lève pas ces difficultés d'interprétation.

Le Conseil d'Etat voit dans le système de la directive transposée par le droit belge un système analogue à celui retenu par le droit français en cas de violation d'une obligation contractuelle de résultat[125]. L'exposé des motifs parle quant à lui « d'une forme légère de responsabilité objective »[126]. En effet, la personne concernée qui se prétend victime d'un dommage doit seulement démontrer, outre la réalité de son dommage, l'acte contraire à la loi ou à ses arrêtés d'application. Elle ne doit par contre pas démontrer la faute du responsable du traitement. Le responsable ne pourra s'exonérer que s'il prouve dans un premier temps la réalité du fait qui a provoqué le dommage et dans un second temps que ce fait ne lui est pas imputable.

Notre propos est, sur base de la jurisprudence belge développée sous l'empire de l'ancienne loi, de démontrer que le texte nouveau modifiera peu les raisonnements jusqu'à présent tenus. Même si le souci de faciliter le recours de la personne concernée est indiscutable à la lecture des textes européen et belge, il incombe à celle-ci de démontrer « l'acte contraire aux dispositions de la loi », la réalité du dommage et *in fine*, le lien de causalité entre l'acte et le dommage. A sa démonstration, le responsable pourra lui opposer soit que l'acte à la base du dommage n'est pas contraire aux dispositions de la loi, soit que cet acte ne lui est pas imputable, soit que la réalité du

---

du Parlement et du Conseil du 24 octobre 1995 *», Lamy droit de l'informatique, Cahier n° 118*, Octobre 1999, p. 12-19.

124 On notera que depuis le 1er septembre la loi belge est entrée en vigueur 6 mois après son adoption et la publication de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 (*M.B.*, 13 mars 1992).

125 Avis du Conseil d'Etat 2 février 1998, *Doc. Parl., Ch. Repres.*, sess.ord. 1997-1998, n° 1566/1.

126 Exposé des motifs, *Doc. Parl., Ch. Repres.*, sess. Ord., 1997-1998, n°1566/1.

dommage n'est point prouvée, soit enfin que le lien de causalité n'est point évident.

Chacun de ces devoirs de preuve à charge tantôt du responsable du traitement, tantôt de la personne concernée fait l'objet des développements suivants.

I. La démonstration par la personne concernée de l'acte contraire à la loi

La personne concernée doit en effet démontrer « l'acte contraire aux dispositions déterminées par ou en vertu d'une loi ». Sans doute, la démonstration de l'acte contraire est facile lorsque la disposition légale ou réglementaire prescrit un comportement précis déterminé sans possibilité in casu d'interprétation possible mais de telles dispositions sont rares. Ainsi, l'article 17 prescrit une obligation de déclaration des traitements des données nominatives. L'absence de toute déclaration de la part d'un responsable est un acte contraire à la loi sauf, ajoutera-t-on, si le responsable peut démontrer qu'il tombe dans une des multiples exceptions prévues par l'arrêté royal du 13 février 2001[127].

Indubitablement, le recours de la personne concernée est facilité. Le juge, pour déclarer responsable le maître du fichier, n'a pas à analyser si l'absence de déclaration constituerait une faute de ce dernier. Ainsi, ne doit-il pas s'interroger sur le point de savoir si un responsable de traitement diligent aurait interprété les exceptions prévues à loi comme l'a fait in concreto le maître du fichier poursuivi ! Il lui suffit, ayant interprété lui-même la portée des

[127] A titre d'exemple, sur ces exceptions, lire C. de TERWANGNE, S. LOUVEAUX, « La protection de la vie privée face au traitement de données à caractère personnel: le nouvel arrêté royal », *J.T.*, 2001, p. 463.

exceptions, de condamner ou non le responsable au plan civil du moins et ce dernier ne pourra arguer contre cette condamnation du fait qu'il avait de bonne foi en responsable diligent jugé qu'il n'était pas tenu de cette déclaration.

Le même raisonnement pourra être tenu à propos d'autres obligations apparemment précises prévues par la loi, ainsi l'obligation d'informer la personne concernée de l'existence d'un traitement lorsqu'on collecte des données auprès d'elle. L'article 9 de la loi, qui prescrit cette obligation d'information, ne définit pas les modalités de cette information, Par exemple, peut-on reprocher au responsable d'un site web d'avoir informé l'internaute auprès duquel une collecte des données est opérée, par une page web appelable via un hyperlien auquel invitait un sigle Privacy placé sur la page d'accueil ? Ici aussi, ce sera au juge d'interpréter les devoirs du responsable sans que celui ne puisse protester d'avoir agi en bon père de famille, en informant l'internaute de cette manière.

La démonstration de « l'acte contraire » devient plus délicate lorsque la disposition légale est floue et requiert nécessairement l'interprétation du juge. Or telles sont les dispositions majeures de la loi, et dont les applications sont les plus susceptibles d'être invoquées en cas de dommages subis. L'article 16 prescrit l'obligation du responsable de prendre des mesures de sécurité appropriées compte tenu de l'état de l'art, de la nature des données à protéger et des risques de dommage en cas de non-confidentialité des données. Prenons un exemple : l'accès par un journaliste indélicat aux données bancaires d'un personnage politique permet certainement de mettre en cause la responsabilité du banquier pour violation de cette obligation de sécurité mais ce sera au juge – et son raisonnement n'aurait pas été différent en appliquant l'article 1382 - d'analyser en quoi le banquier ne s'est pas comporté comme un responsable diligent soucieux de la sécurité des données nominatives,

qu'il traite, obligation dont le législateur lui-même rappelle qu'il s'agit d'un obligation de moyens[128].

Certes, mais n'y-a-t-il pas malgré tout renversement de la charge de la preuve grâce au libellé de l'article 15bis : ce serait au banquier de prouver qu'il s'est comporté comme responsable diligent et non à la personne concernée de démontrer un quelconque écart de conduite !

L'assertion est plus que discutable : l'article 15bis ne met-il pas à charge de la personne concernée la démonstration de l'acte contraire à la loi ?

Le même raisonnement prévaut lorsque le responsable utilise des données que la personne concernée estime non « pertinentes » ou opère un traitement dont la personne concernée conteste la légitimité. Ainsi, dans quelle mesure, un employeur peut-il accéder au logbook de son entreprise pour vérifier les destinataires des e-mail de ses employés[129]? La démonstration de « l'acte contraire » à la loi

---

128 L'article 16 § 4 de la loi énonce en effet: " Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement est tenu… de prendre les mesures techniques et organisationnelles requises pour protéger les fichiers contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification , l'accès et tout autre traitement non autorisé de données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels". Un arrêt de la Cour d'arbitrage (arrêt n° 14/93, 18 février 1993, Arrêt C.A., 1993, p. 153) rappelle en effet que l'obligation de sécurité exige la prise de mesures de sécurité "dont l'effet de protection est dans un rapport adéquat avec les efforts qu'elles occasionnent".

129 Une proposition de loi a été déposée le 28 août 2001 devant le Sénat pour réglementer l'usage de l'Internet et de l'e-mail sur le lieu du travail. Le texte clarifie l'étendue des compétences de l'employeur en ce qui concerne à la fois la détermination de l'utilisation par les employés des outils de communication mis à leur disposition et le contrôle du respect

suppose que la personne concernée établisse qu'une telle surveillance excède les prérogatives de contrôle de l'employeur déduites du contrat de travail[130].

Bref, l'application de l'article 15bis conduit bien souvent à une appréciation par le juge de ce que devait être in concreto le comportement d'un « bon responsable de traitement ». Le juge compare le comportement ainsi décrit à celui suivi en réalité par le responsable.

L'interprétation de la loi modifiée en ce qui concerne cette obligation d'exactitude n'est pas aisée. L'obligation d'exactitude était, sous l'empire de l'ancienne loi, une simple obligation de moyens, elle constituait une simple application de l'obligation de sécurité de l'article 16 de la loi[131]. La loi du 11 décembre 1998 envisage pour elle-même la question de l'exactitude des données. Les données, dit l'article 4 § 1 4° de la loi du 8 décembre 1992 modifiée, « doivent être exactes » mais la loi ajoute immédiatement « toutes les mesures raisonnables doivent être prises pour que les données inexactes ou

---

par les employés de ces règles d'utilisation (cf. sur ce thème, également l'avis n° 10/2000 du 3 avril 2000 de la Commission de protection de la vie privée, publié sur le site de http://www.privacy.fgov.be)

130 Cf. à cet égard, l'arrêt du 27 février 2001 de la Cour de cassation (disponible au site JURIS de la cour de cassation: http://www.cass.be/cgi_juris/juris_cass_al.pl) où un travailleur se plaignait que l'installation de systèmes de vidéosurveillance par som employeur contrevenait au principe de proportionnalité prévue par l'article 5 ancien de la loi du 8 décembre 1992 et à l'obligation légale d'information à charge du maître du fichier. La Cour rejette la demande de la personne concernée à défaut pour elle de démontrer à suffisance la contravention à la loi.

131 Sur l'obligation d'exactitude comme simple obligation dans le cadre de l'ancien texte, lire Th. LEONARD, note sous Civ. Brux (prés.) 22 mars 1994, *J.T.*, 1994, n° 34, p. 82. L'auteur tire argument en particulier du fait des travaux parlementaires de la loi de 1992, qui atteste que l'absence de disposition expresse sur l'obligation d'exactitude était non un oubli mais un refus de principe.

incomplètes, … soient effacées ou rectifiées ». Bref, faut-il interpréter chaque phrase séparément ou au contraire, l'une par l'autre. Dans le premier cas, le devoir d'exactitude constituerait une sorte d'obligation de résultat et conduirait à la responsabilité du maître du fichier, sauf à ce dernier à démontrer la faute d'un tiers ou de la victime. La seconde phrase viserait le devoir du maître du fichier soit de réagir suite à la constatation d'une inexactitude, soit de veiller préventivement à la détection d'erreurs. La jurisprudence belge a fréquemment été confrontée au problème des conséquences de l'inexactitude des données traitées par un responsable de traitement, et ce en particulier dans le secteur bancaire.

A l'inverse, on peut considérer que les deux phrases doivent être combinées et que la seconde atténue la portée de la première. L'obligation d'exactitude ne conduit à la responsabilité du maître du fichier que si celui-ci est incapable de montrer qu'il a pris les mesures raisonnables et appropriées pour les éviter et, le cas échéant, les rectifier.

Cette seconde interprétation renvoie le juge à l'examen in concreto du respect ou non par le responsable du traitement de son devoir de diligence quant à la vérification de l'exactitude des données qu'il traite. Sans doute, l'inexactitude de la donnée présume-t-elle que le comportement du responsable était un acte contraire à la loi mais rien n'empêche que le responsable renverse la présomption.

La jurisprudence prise dans le cadre de l'ancien texte de la loi du 8 décembre 1992 s'en trouve-t-elle confirmée ?

Plusieurs décisions[132] concernent en particulier la responsabilité des centrales de crédit ayant enregistré à la demande d'un organisme de

[132] Civ. Brux (prés.), 22 mars 1994, *J.T.*, 1994, p. 82 et s. ; Liège 5 juin 1991, *DIT*, 1994/1, p. 37 et s. ; Trib. Civ. Liège, 11 mars 1987, *JLMB*, 1987, 549. Sur cette jurisprudence, lire J.P. BUYLE, L. LANNOYE, Y.

© Yves Poullet & Jean-François Lerouge

crédit une donnée s'avérant par la suite inexacte. Peut-on déduire du simple constat d'inexactitude de la donnée, une responsabilité du « maître du fichier », en l'occurrence la centrale de crédit. La jurisprudence a toujours estimé que la violation de la loi supposait la preuve d'un manquement à un devoir de vigilance et de prudence[133].

Un arrêt inédit tout récent de la Cour d'Appel de Bruxelles[134] s'interrogeait sur la responsabilité de l'organisme de crédit, ayant dénoncé un défaut de paiement à une centrale de renseignements, alors même que les défauts de paiement étaient dus, selon la personne en défaut, à une erreur postale qui l'avait privé de toute information sur les réclamations opérées par l'organisme de crédit. La Cour, dans cette affaire, s'interroge longuement sur les devoirs d'un créditeur prudent et soucieux de vérification des données qu'il détient pour conclure que la personne concernée n'établit pas à suffisance la faute de l'organisme créditeur.

Sans doute, les textes nouveaux, celui de l'article 4 § 1 4° relatif à l'obligation d'exactitude et celui de l'article 15 bis relatif à la responsabilité mettront dorénavant à la charge du « responsable du traitement », la preuve de l'inexistence de sa faute et faciliteront dès lors la démarche des personnes concernées.

POULLET et V. WILLEMS, L'informatique, *Chron. de Jurispr*., 1996, p. 234, n° 64 et s.

133 Cf. cet attendu du président du tribunal civil de Bruxelles (22 mars 1994, *J.T*., 1994, p. 82) : « Le maître du fichier doit procéder avec prudence au traitement de données qu'il reçoit, en étant constamment attentif à la finalité du traitement. Il ne peut donc reprendre servilement les données fournies par un tiers, mais doit vérifier s'il n'est pas prématuré de les traiter ».

134 Bruxelles (4è ch.) 11 juin 2001, en cause L.c. SCRL record, inédit, R.G. 1998/AR/2002.

© Yves Poullet & Jean-François Lerouge

II. La démonstration par le responsable du traitement de la non-imputabilité

La non-imputabilité du fait résultera tantôt la faute de la victime tantôt de la faute d'un tiers.

Quant à la faute de la victime, l'arrêt de la Cour d'appel de Liège, reproche à la personne concernée d'avoir transmis une adresse illisible et de ne s'être point inquiété du silence prolongé du créditeur[135]. De la même façon, la Cour d'appel du travail de Gand, le 16 septembre 1998[136] devait exonérer un organisme de paiement de toute responsabilité pour traitement de données inexactes quant au degré d'inaptitude d'un handicapé, alors que ce dernier n'avait pas pris les mesures nécessaires à la contestation de telles données inexactes.

L'invocation de la faute d'un tiers est également possible. On rappellera à ce propos l'affaire déjà évoquée[137] où une centrale de crédit s'était contentée de reproduire une information inexacte transmise par un organisme de crédit. En l'espèce, le président du tribunal civil de Bruxelles[138] estime que la faute de l'organisme de

135 "Que dans ces conditions, l'absence de réaction dans un premier temps (du responsable) à ce qui pouvait lui apparaître, dans l'état des informations qui lui étaient fournies à ce moment, comme la conséquence d'une négligence originairement commise par la personne concernée, ne présente pas en elle-même, un caractère fautif ».

136 Arbeidshof Gent (7e ch.), 16 sept. 1998, *Chr. D. Social*, 1999, p. 277.

137 P. GRIMALT (*op. cit.*, p. 15) cite divers cas d'exonération pour faute de la victime. Ainsi, le cas d'une transmission fautive par un responsable (un assureur) à un tiers (un banquier). Cette transmission porte sur une donnée erronée par suite d'une faute de la personne concernée qui souhaitait cacher la vérité à son assureur et entraîne un refus de crédit de la banque. La contravention par l'assureur à la loi est-elle cause du dommage ou l'assureur peut-il se prévaloir de la faute de la victime ?

138 Civ. Bruxelles (prés.) 22 mars 1994, *J.T.*, 1994, p. 82 et s.

© Yves Poullet & Jean-François Lerouge

crédit ne supprime pas celle de la mutuelle de crédit : « Le maître du fichier (la mutuelle de crédit) doit procéder avec prudence au traitement des données qu'il reçoit, en étant constamment attentif à la finalité du traitement. Il ne peut donc reprendre servilement les données fournies par un tiers, mais doit vérifier s'il n'est pas prématuré de les traiter »[139].

III. La démonstration du dommage et du tiers de causalité

La question du dédommagement de la victime à la suite de l'utilisation ou de la communication d'une donnée inexacte, incomplète ou obsolète la concernant donne lieu à des solutions diverses. Si certains jugements se bornent à noter que le dommage n'est pas prouvé par la victime[140] ou le lien de causalité douteux[141], d'autres évaluent ex æquo et bono le dommage moral subi[142].

---

139 Sur l'étendue de ce devoir de vérification cf. la note très fouillée de Th. LEONARD (en particulier, n° 35 et s.) déjà citée. Cf. également, Th. LEONARD et E. MONTERO, « La responsabilité civile du fait de données inexactes diffusées par une mutuelle d'informations », note sous Liège, 5 juin 1991, *DIT*, 1994, 1, p. 41 et s.

140 Ainsi, la decision inédite d'Anvers du 26 octobre 1992, en cause Van Riel D. c. de Beropsvereniging van het krediet, R.G. 55.219.

141 Ainsi, le seul fait qu'une centrale d'informations sur les mauvais risques dans les secteurs bancaires ou d'assurance renseigne à tort une personne comme fichée, peut-il être considéré comme la cause "évidente et nécessaire" du dommage que constitue le refus de crédit ou de police d'assurance.
La centrale aura tôt fait d'invoquer que l'insuffisance des garanties présentées par le demandeur de crédit ou le candidat souscripteur a pesé plus lourd dans la décision négative que le renseignement inexact transmis par elle.

142 Ainsi, le tribunal civil de Liège, le 11 mars 1987 (*J.T.* 1987, P. 426) et le président du tribunal civil de Bruxelles, le 22 mars 1994 (*J.T.* 1994, p.

© Yves Poullet & Jean-François Lerouge

Certains jugements ajoutent que la publication dans un quotidien, outre le franc symbolique constitue le mode adéquat de réparation[143]. D'autres préfèrent à une condamnation pécunaire, une réparation en nature[144].

On rappellera que les tribunaux déclarent comme irrecevables les actions intentées par les associations au motif que celles-ci peuvent difficilement se prévaloir d'un préjudice direct suite à la violation subie par un membre de leur association[145]. Sans doute, eût-il été bon de permettre les actions collectives, là où souvent les personnes concernées ont quelques hésitations à agir vis-à-vis d'un responsable du traitement vis-à-vis duquel ils sont en position de débiteurs voire de faiblesse[146].

---

843) évaluent à 50.000 BEF le préjudice : le juge de paix de Namur du 13 janv. 1987 (*R.R.D.*, 1987, p. 209) accorde le franc symbolique réclamé.

143 Civ. Namur (1ère ch.) 17 nov. 1997, *J.T.*, 1998, p. 187. A l'inverse, la décision de la Cour européenne des droits de l'Homme qui estime à propos de la publication par la justice suédoise du nom d'une partie dont l'arrêt révélait qu'elle était atteinte du sida : « Attendu qu'un constat de violation ne saurait constituer une satisfaction équitable et qu'il convient donc de lui accorder une indemnité (CEDH 25 fév. 1997, *Rev. de santé*, 1997-1998, p. 322).

144 A cet égard, Prés. Liège 6 juin 1995, *DIT*, 1996, p. 47, note P. Wéry. En l'occurrence, un éditeur d'annuaires avait omis de mentionner les coordonnées d'un médecin. Le juge a considéré que la mesure la plus adéquate consistait à joindre à chaque facture adressée aux abonnés de la zone concernée, un avis reprenant les coordonnées du médecin.

145 Cf. de manière ferme, la décision de la Cour européenne de Strasbourg dans une affaire contre l'Etat belge (C.E.D.H., 19 janv., *A.J.T.*, 1997-98, p. 501). En l'occurrence, il s'agissait d 'une requête de la L.D.H. contre des mesures de vidéosurveillance jugée contraire à la loi du 8 décembre 1992.

146 Sur cette question controversée, lire la note très critique de MM. de HERT et de SCHUTTER, Straatsburg, Videosurveillance en het vorderingsrecht van vereningen, observ. C.E.D.H., 14 janv. 1998*, A.J.T.,* 1997-98, p. 502 et s.

© Yves Poullet & Jean-François Lerouge

Conclusion

L'article 15bis de la loi belge du 8 décembre 1992 introduit, à la faveur de la transposition de la directive européenne 95/46, dans notre système juridique belge de la responsabilité, quelques confusions. La disposition est en effet ambiguë dans la mesure où elle renvoie à la démonstration qu'un comportement du responsable constitue un acte contraire à la loi[147]. Or cette démonstration, nous l'avons montré, n'est point aisée et suppose parfois que le juge soit amené à examiner si le comportement du responsable est celui d'un bon responsable.

Peut-être, l'article 15bis établit-il à cet égard un renversement de la charge de la preuve mais il apparaît douteux que les juges aillent au-delà et n'imputent aux responsables de traitement une responsabilité objective.

147 On rapprochera la formulation de l'article 15bis de celle utilisée par les présidents des tribunaux de commerce, lorsqu'ils ont à statuer dans le cadre d'actions en cessation pour pratiques contraire aux usages honnêtes suivant l'article 93 de la loi du 14 juillet 1991 sur les pratiques du commerce : "La violation de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et de l'obligation générale de prudence est une pratique contraire aux usages honnêtes en matière commerciale susceptible de porter atteinte aux intérêts d'un vendeur" (Trib. Comm. Antwerpen (Prés.), 7 juillet 1994, *DCCR*, 1994, 77 et s. décision confirmée en appel Anvers " mai 1999, *A.J.T.*, 1999-2000, p. 437).
Ainsi, la condamnation pour "pratique contraire aux usages honnêtes en matière commerciale" comme celle en responsabilité de l'article 15bis requiert la simple démonstration dans les faits de l'acte contraire à la loi (sur cette jurisprudence des présidents des tribunaux de commerce, lire J.P. BUYLE, L. LANNOYE, Y. POULLET et V. WILLEMS, L'informatique, *Chron. de jurisprudence*, *J.T.,* 1996, p. 237, n° 78 et s.

On ajoute que le responsable en toute hypothèse pourra, suivant l'article 15bis, s'exonérer en démontrant que nonobstant son non-respect de la loi, le fait ayant causé le préjudice peut être attribué à un événement extérieur à l'activité du responsable, y compris à la faute de la victime.

Enfin, les preuves du dommage, d'une part, et du lien de causalité entre le non-respect de la loi et le dommage, d'autre part, restent, la jurisprudence le démontre, difficiles à apporter.

CONCLUSION GENERALE

Au terme de ce rapide tour d'horizon une conclusion s'impose.

Notre bon vieux droit commun de la responsabilité a plus que jamais sa raison d'être. Internet ne contribue pas à l'enterrer sous prétexte de vétusté. Plus que jamais, sa souplesse sera recherchée et les plaideurs continueront à solliciter le bon sens de nos juges.

Néanmoins l'étude révèle la nécessité de déterminer avec davantage de précision et de cohérence les obligations des acteurs de l'Internet. Se faisant, les règles de comportement s'en trouveront immanquablement « objectivées ».

Objectiver et préciser les règles de comportement, pour renforcer la clarté et se faisant la sécurité juridique, ne signifie toutefois pas que nous plaidons pour l'instauration de régimes de responsabilité objective qui, à nos yeux, doivent rester l'exception.

*

* *

© Yves Poullet & Jean-François Lerouge