

Texte pseudonymisé

Avertissement: Ce document pseudonymisé a une valeur purement informative. Le document original seul fait foi.

Arrêt N° 77/25 - II - CIV

Audience publique du sept mai deux mille vingt-cinq

Numéro CAL-2023-00808 du rôle

Composition:

Danielle SCHWEITZER, président de chambre,
Béatrice KIEFFER, premier conseiller,
Martine WILMES, premier conseiller,
Alexandra NICOLAS, greffier.

E n t r e :

la société de droit hongrois **SOCIETE1.) Kft.**, établie et ayant son siège social à ADRESSE1.), inscrite sous le numéro d'entreprise NUMERO1.), représentée par son conseil d'administration actuellement en fonctions, sinon par son organe de gestion ou tout autre organe autorisé actuellement à la représenter,

appelante aux termes d'un exploit de l'huissier de justice Geoffrey GALLE de Luxembourg du 4 août 2023,

comparant par la société à responsabilité limitée M&S LAW, inscrite à la liste V du Tableau de l'Ordre des Avocats du Barreau de Luxembourg, représentée aux fins des présentes par Maître Joram MOYAL, avocat à la Cour, demeurant à Luxembourg,

e t :

la société à responsabilité limitée de droit luxembourgeois **SOCIETE2.)**, établie et ayant son siège social à ADRESSE2.), inscrite au registre de commerce et

des sociétés de Luxembourg sous le numéro NUMERO2.), représentée par son gérant actuellement en fonctions,

intimée aux fins du prêt exploit Geoffrey GALLE du 4 août 2023,

comparant par Maître Jean MINDEN, avocat à la Cour, demeurant à Luxembourg.

L A C O U R D ' A P P E L :

Le litige a trait à la demande de la société de droit hongrois SOCIETE1.) Kft. (ci-après la société SOCIETE1.)) en obtention de dommages et intérêts pour préjudices matériel et moral dirigée à l'encontre de la société d'avocats, la société à responsabilité limitée SOCIETE2.) (ci-après le cabinet d'avocats luxembourgeois ou la société SOCIETE2.)).

Il est admis entre parties et il ressort des pièces versées en cause que conformément à la lettre d'engagement du 20 juillet 2020, la société SOCIETE1.) a mandaté la société SOCIETE2.) pour assurer sa défense dans le cadre d'une assignation de faillite, lancée en date du 10 juillet 2020 par la société de droit hongrois SOCIETE3.) (ci-après la société SOCIETE3.)) à l'encontre de la société anonyme de droit luxembourgeois SOCIETE4.) (ci-après la société SOCIETE4.)), filiale de la société-mère SOCIETE1.).

La société SOCIETE1.) était assistée en HONGRIE par un cabinet d'avocat hongrois, à savoir le cabinet SOCIETE5.), et notamment par l'avocat hongrois Maître PERSONNE1.) (ci-après Maître PERSONNE1.)).

Les interlocuteurs de la société SOCIETE1.) et du cabinet d'avocats hongrois auprès de la société SOCIETE2.) étaient Maîtres PERSONNE2.) et PERSONNE3.) (ci-après Maîtres PERSONNE2.) et PERSONNE3.)).

Dans le cadre de la procédure de faillite engagée par la société SOCIETE3.) devant le tribunal de commerce luxembourgeois, il a été convenu entre Maître PERSONNE1.) et Maître PERSONNE2.) que la société SOCIETE1.) consigne sur le compte tiers de la société SOCIETE2.) le montant réclamé de 1.050.000 EUR par la société SOCIETE3.) à la société SOCIETE4.), filiale de la société-mère SOCIETE1.), dans le but de démontrer au tribunal de commerce que les conditions de la mise en faillite de la société SOCIETE4.) n'étaient pas remplies.

Par jugement commercial du 2 septembre 2020, la demande de la mise en faillite de la filiale SOCIETE4.) a été rejetée.

Par courriel du 3 septembre 2020, Maître PERSONNE2.) a fait parvenir le jugement commercial à Maître PERSONNE1.), tout en l'informant ne pas avoir reçu le montant de 1.050.000 EUR sur le compte tiers du cabinet d'avocats luxembourgeois.

Après plusieurs échanges de courriels entre avocats, il s'est avéré que le montant de 1.050.000 EUR avait été transféré par trois virements, respectivement de 880.000, 137.000 et 33.000 EUR, sur un compte bancaire de la banque « SOCIETE6.) » au nom du bénéficiaire « CV SOCIETE2.) », ayant son adresse à « ADRESSE3.) »,

Ce compte bancaire a été indiqué par un ou plusieurs cybercriminels, qui s'étaient introduits dans les correspondances électroniques échangées entre les parties.

En date du 7 septembre 2020, la société SOCIETE1.) a déposé plainte pénale contre inconnu auprès des autorités hongroises.

En date du 8 septembre 2020, Maîtres PERSONNE2.) et PERSONNE3.) ont déposé plainte contre inconnu auprès du parquet du tribunal d'arrondissement de Luxembourg pour délits d'escroquerie, d'usurpation d'identité et d'accès à tout ou partie d'un système de traitement ou de transmission automatisé de données.

Par la suite, la société SOCIETE1.) a été informée que la société SOCIETE2.) avait déjà dénoncé à la police luxembourgeoise en date du 16 juillet 2020 des faits de piratage informatique concernant un client polonais.

Elle a alors estimé que la société SOCIETE2.) avait commis des fautes en n'adaptant pas sa pratique à la suite du piratage informatique antérieur afin de sécuriser son activité professionnelle et les transactions y liées et en ne faisant pas preuve de prudence.

Etant d'avis que la responsabilité du cabinet d'avocats luxembourgeois était engagée, la société SOCIETE1.) a, par exploit d'huissier de justice du 18 août 2021, fait donner assignation à la société SOCIETE2.) devant le tribunal d'arrondissement de Luxembourg pour la voir condamner à lui payer le montant de 1.065.000 EUR, avec les intérêts au taux légal à compter du 17 mai 2021, sinon à compter de la demande en justice jusqu'à solde.

Elle a encore demandé le montant de 10.000 EUR à titre d'indemnité de procédure.

Elle a basé sa demande principalement sur les articles 1147 et suivants du Code civil, sinon, subsidiairement sur les articles 1382 et suivants du Code civil.

Dans le cadre de ses dernières conclusions en première instance, la société SOCIETE1.) a encore sollicité de condamner la société SOCIETE2.) à lui payer le montant de 25.673,47 EUR à titre de frais d'avocat.

La société SOCIETE2.) a soulevé la nullité de l'exploit introductif d'instance du 18 août 2021 pour défaut d'indication de la personne ou de l'organe qualifié pour représenter la société SOCIETE1.) en justice.

Elle a contesté toute faute et toute responsabilité dans son chef et a demandé de condamner reconventionnellement la société SOCIETE1.) au paiement d'une indemnité pour procédure abusive et vexatoire du montant de 20.000 EUR et d'une indemnité de procédure du montant de 10.000 EUR.

Par jugement du 7 juin 2023, le tribunal a rejeté le moyen de nullité de l'exploit introductif d'instance du 18 août 2021 et a déclaré les demandes de la société SOCIETE1.) recevables, mais non fondées.

La demande reconventionnelle de la société SOCIETE2.) en obtention d'une indemnité pour procédure abusive et vexatoire a été rejetée.

La société SOCIETE1.) a été condamnée à payer à la société SOCIETE2.) une indemnité de procédure du montant de 2.000 EUR.

Du jugement du 7 juin 2023, lui signifié en date du 26 juin 2023, la société SOCIETE1.) a régulièrement relevé appel par exploit d'huissier de justice du 4 août 2023.

L'appelante demande, par réformation du jugement entrepris, de condamner la société SOCIETE2.) à lui payer le montant de 1.110.000 EUR, avec les intérêts au taux légal à partir de la demande en justice, sinon à compter de l'acte d'appel, sinon à partir de l'arrêt à intervenir, jusqu'à solde.

A titre subsidiaire, elle demande de voir nommer un expert judiciaire informatique avec la mission de « *se prononcer sur les causes et origines des deux attaques de piratage informatique survenues, pour la première en date des 15 et 16 juillet 2020, pour la seconde aux environs du 3 août 2020, sans préjudice quant à la date plus exacte, relativement au système informatique, aux comptes mails, au logo et à tous les noms et adresses, donc toute la signature des avocats du cabinet d'avocats SOCIETE2.), et ayant visé le détournement de fonds destiné à son compte tiers, et provoqué, lors de la seconde attaque, le détournement litigieux des fonds, à savoir 1.050.000 EUR, destinés au compte tiers dudit cabinet d'avocats, et de se prononcer sur la similitude du modus operandi entre les deux attaques* ».

En tout état de cause, elle demande d'être déchargée du paiement du montant de 2.000 EUR auquel elle a été condamnée à titre d'indemnité de procédure pour la première instance.

L'appelante demande encore une indemnité de procédure du montant de 10.000 EUR et de voir ordonner l'exécution provisoire de l'arrêt à intervenir.

Dans ses conclusions de synthèse du 13 décembre 2024, la société SOCIETE1.) précise demander à titre de dommages et intérêts pour préjudice matériel le montant de 1.050.000 EUR, pour préjudice moral le montant de 10.000 EUR, ainsi que pour les frais d'avocat le montant de 53.584,57 EUR, à augmenter des intérêts au taux légal tel que spécifié ci-avant.

La société SOCIETE2.) demande d'entériner le jugement entrepris.

A titre subsidiaire, elle demande de constater et dire que l'indemnité réparatrice pouvant revenir à la société SOCIETE1.) se trouve limitée à dix fois le montant des honoraires payés par elle pour les services rendus par le cabinet d'avocats luxembourgeois, soit le montant de 223.666,60 EUR.

Pour le surplus, elle conteste les demandes de la société SOCIETE1.) en leur principe et en leur quantum.

Elle demande une indemnité de procédure du montant de 10.000 EUR pour l'instance d'appel.

La société SOCIETE1.) critique le jugement entrepris pour ne pas avoir retenu que la responsabilité du cabinet d'avocats luxembourgeois était engagée.

Elle fait valoir que par courriel électronique du 20 juillet 2020, la société SOCIETE2.) lui a conseillé de consigner sur son compte tiers le montant de 1.050.000 EUR malgré le fait qu'en date du 15 juillet 2020, le système informatique, les comptes mails, ainsi que le logo du cabinet et toute la signature de la société SOCIETE2.) avaient fait l'objet d'un hacking informatique, tel que cela résulterait de la plainte déposée à cet effet.

La plainte pénale du 16 juillet 2020 ferait état du fait qu'un client polonais de la société SOCIETE2.) s'était adressé à celle-ci en date du 15 juillet 2020 par voie téléphonique aux fins de demander la confirmation que la banque du cabinet d'avocats luxembourgeois avait effectivement changé et se trouvait actuellement en Pologne.

A la suite de la réponse négative par la société SOCIETE2.), ce client aurait envoyé certains courriels prétendument reçus de la part de la société SOCIETE2.).

Lors de sa plainte pénale, la société SOCIETE2.) aurait été en aveu judiciaire que l'hacker avait copié le logo de l'entreprise, ainsi que tous les noms et l'adresse, donc toute la signature et que seulement l'adresse électronique (e-mail) était différente, étant donné que l'adresse e-mail du cabinet est composée comme suit : *prénomMAIL1.)* et que celle utilisée par l'hacker était composée comme suit : *prénomMAIL2.)*.

L'appelante fait valoir que le même modus operandi a été utilisé par le ou les cybercriminels lui ayant fait parvenir le faux numéro de compte sur lequel elle a viré le montant de 1.050.000 EUR.

Elle reproche à la société SOCIETE2.) de ne pas avoir pris des mesures conservatoires consistant pour le moins à ne plus émettre de demandes de virement sur son compte tiers par la voie de courriels après l'incident survenu et dénoncé en date du 16 juillet 2020.

Selon elle, la société SOCIETE2.) aurait dû prendre des mesures afin de garantir à ses futurs clients la sécurité absolue des correspondances, informer les nouveaux clients du piratage informatique survenu, rechercher d'autres solutions que le virement d'argent sur son compte tiers, et informer les nouveaux clients du modus operandi utilisé par les pirates.

L'appelante estime que la société SOCIETE2.) aurait dû avertir les futurs clients par téléphone.

La société SOCIETE1.) reproche à la société SOCIETE2.) de ne pas avoir pris au sérieux l'attaque informatique et d'avoir demandé et insisté par courriels électroniques de se voir virer plus d'un million d'euros sur son compte tiers, ayant fait l'objet d'un piratage.

Les deux attaques informatiques auraient visé les clients de la société SOCIETE2.), le détournement d'argent à destination du compte tiers de la société SOCIETE2.), les chaînes de courriels échangés par la société SOCIETE2.) avec ses clients, les adresses électroniques de la société SOCIETE2.), le logo de l'entreprise SOCIETE2.), ainsi que la signature des avocats de la société SOCIETE2.).

Le modus operandi des pirates informatiques, en tout point identique, balayerait toute coïncidence et accablerait lourdement le professionnel, qui n'aurait pas pris les mesures appropriées afin d'assurer la sécurité informatique et financière de ses clients profanes.

Le cabinet d'avocats luxembourgeois aurait violé ses obligations d'information, de conseil et de prudence. L'obligation d'information serait une obligation de résultat et il incomberait à la société SOCIETE2.) de prouver qu'elle l'a accomplie.

La société SOCIETE1.) fait encore valoir que la messagerie électronique du cabinet d'avocat hongrois SOCIETE5.) a été analysée par deux experts informatiques hongrois après l'escroquerie survenue et qu'aucun signe de violation du système de messagerie n'a pu être constaté.

Elle indique que les experts informatiques hongrois ont conclu que le système de filtrage des courriels du cabinet d'avocats luxembourgeois était faible et que le filtre des courriels n'a pas réussi à vérifier à partir du suffixe de zone si le courriel était bien arrivé de l'adresse électronique du cabinet d'avocats hongrois, ce qui n'avait pas été le cas.

La société SOCIETE1.) estime que la responsabilité contractuelle de la société SOCIETE2.) est engagée sur base des articles 1134 et 1147 du Code civil pour avoir commis des fautes graves tant par omissions que par actions.

En tant que fautes par omission, la société SOCIETE1.) reproche à la société SOCIETE2.) le fait d'avoir omis d'informer ses nouveaux clients de la cyberattaque subie, le fait de ne pas avoir adapté sa pratique professionnelle pour sécuriser les échanges avec ses clients et garantir la confidentialité de

l'identité de ses clients, le fait d'avoir émis des indications de paiement par courriels à destination de ses comptes bancaires et le fait de ne pas avoir indiqué à ses clients que toute indication de paiement sur son compte tiers devrait être vérifiée de vive voix par téléphone et /ou par un autre service sécurisé, du moins pour les paiements les plus importants.

En tant que fautes par commission, la société SOCIETE1.) reproche à la société SOCIETE2.) le fait d'avoir émis une indication de paiement par la voie de courriel concernant le montant important de 1.050.000 EUR, tout en connaissant le modus operandi utilisé par les pirates et le fait d'avoir prodigué un conseil désastreux et préjudiciable, étant donné que le transfert de l'argent sur le compte tiers n'était pas une condition à l'obtention d'une relâche dans le cadre de la procédure de faillite et qu'une mise à disposition des fonds sur un compte bancaire hongrois aurait été suffisante.

La société SOCIETE2.) aurait ainsi contrevenu aussi bien à ses obligations d'information et de conseil qu'à ses obligations générales de prudence et de diligence.

Ces obligations seraient des obligations de résultat et en l'absence de preuve de la part de la société SOCIETE2.) d'avoir rempli son obligation d'information et de conseil, sa responsabilité se trouverait engagée sans qu'elle puisse s'exonérer par la production d'une simple expertise informatique concluant de façon lacunaire que lors de l'incident avec le client polonais, aucun courriel n'était sorti ou entré des serveurs de l'étude.

Subsidiairement, la société SOCIETE1.) estime que la responsabilité du cabinet d'avocats luxembourgeois est à retenir sur base des articles 1382 et 1383 du Code civil.

La société SOCIETE2.) conteste toute faute dans son chef et tout lien causal entre une prétendue faute de sa part et le préjudice subi par SOCIETE1.).

Elle fait valoir que son conseil de consigner le montant de 1.050.000 EUR sur son compte tiers afin de démontrer au tribunal de commerce luxembourgeois que les conditions de la faillite n'étaient pas remplies ne constituait certainement pas une démarche fautive, étant donné qu'il s'agit d'une stratégie tout à fait courante.

Le dommage subi par la société SOCIETE1.) serait en relation causale avec des manœuvres informatiques criminelles, manœuvres auxquelles elle serait totalement étrangère et qui aurait amené la société SOCIETE1.) à effectuer trois virements du montant total de 1.050.000 EUR sur un compte bancaire en Indonésie pour un bénéficiaire dénommé CV SOCIETE2.) au lieu de les effectuer sur le compte tiers de la société SOCIETE2.) à Luxembourg.

Le cabinet d'avocats luxembourgeois explique avoir préparé et adressé à la société SOCIETE1.) une déclaration intégrant les coordonnées bancaires de son compte tiers auprès de la banque SOCIETE7.) à Luxembourg et que cette

déclaration lui est revenue avec la signature du représentant de la société SOCIETE1.).

Elle explique que les hackers ont fait parvenir à la société SOCIETE1.) des détails bancaires alternatifs à ceux communiqués par elle et que c'est sur base de ces communications frauduleuses que la société SOCIETE1.) a effectué les trois virements pour le montant total de 1.050.000 EUR sur le compte bancaire du ou des cybercriminels en Indonésie.

Pour le reste des échanges, les hackers auraient relayé par leur filtre les courriels de SOCIETE2.), respectivement ceux des avocats hongrois et ceux de la société SOCIETE1.), de sorte qu'en apparence tout progressait au mieux dans le cadre de la procédure de faillite.

Après s'être rendu compte des faits criminels, elle aurait immédiatement déposé plainte au pénal et averti son prestataire de services informatiques, la société SOCIETE8.).

La société SOCIETE8.) aurait conclu à une absence de piratage et à une absence de phishing du serveur de la société SOCIETE2.), suspectant un phishing auprès de Maître PERSONNE1.).

Ainsi, la société SOCIETE8.) aurait pu identifier sur le serveur mail de la société SOCIETE2.) un premier courriel avec des adresses frauduleuses expédié à partir de l'adresse électronique du cabinet d'avocats hongrois @hu.andersenlegal.com, ce qui permettrait de conclure que c'est le cabinet hongrois qui a été victime d'un phishing le 22 juillet 2020 ou à une date antérieure.

Ce serait ce phishing de la boîte mail de Maître PERSONNE1.) qui aurait permis à ou aux cybercriminels de s'introduire à travers la mise en place d'adresses électroniques frauduleuses dans les communications entre d'une part le cabinet d'avocats luxembourgeois et d'autre part le cabinet d'avocats hongrois et la société SOCIETE1.), selon la méthode du « *man in the middle* ».

Il résulterait du courriel frauduleux du 22 juillet 2020 que l'escroc aurait modifié l'adresse de réponse électronique « MAIL3.) » en « MAIL4.) » et que des changements comparables, très difficilement détectables auraient également été commis pour les adresses électroniques mises en copie.

La société SOCIETE8.) serait une société spécialisée en informatique et ses constatations seraient objectives.

La demande en institution d'une expertise judiciaire serait ni pertinente ni concluante et superfétatoire.

Le cabinet d'avocats luxembourgeois ne serait pour rien dans les agissements criminels de l'escroc et le piège mis en place par les hackers aurait été inévitable.

Sa mise en place aurait seulement été possible, parce que le cabinet d'avocats hongrois aurait fait l'objet d'un phishing ayant permis à ou aux cybercriminels d'accéder à la boîte mail de Maître PERSONNE1.).

Aucune faute ne pourrait lui être reproché.

La société SOCIETE2.) fait noter que s'il est exact qu'elle a été confrontée à une cyberattaque similaire en juillet 2020, toujours est-il que cette cyberattaque, impliquant un client polonais, n'avait aucun lien avec celle impliquant la société SOCIETE1.).

Lors de l'incident informatique avec le client polonais, elle aurait immédiatement informé son prestataire de services informatiques SOCIETE8.) aux fins de procéder aux vérifications de son système informatique.

La société SOCIETE8.) l'aurait informée du fait que l'attaque n'avait pas été perpétrée à partir de son système informatique qui ne présenterait aucune faille, de sorte qu'aucune action sur ses systèmes ne serait requise.

Selon la société SOCIETE8.), la cause de l'incident se serait trouvée exclusivement chez le client polonais.

La société SOCIETE2.) renvoie aux courriers des sociétés SOCIETE8.) et SOCIETE9.) des 15 juillet 2020 et 14 octobre 2021 desquels il ressort que le courriel frauduleux envoyé au client polonais n'était ni sorti ni reçu des serveurs du cabinet d'avocats luxembourgeois.

En ce qui concerne l'incident avec le client polonais, elle fait valoir avoir été rassurée par son prestataire de services informatiques, lui ayant assuré que ses systèmes informatiques n'avaient souffert d'aucune faille et qu'elle n'avait pas fait l'objet d'une introduction frauduleuse dans son système informatique.

La société SOCIETE2.) estime avoir réagi adéquatement à l'incident avec le client polonais et avoir pu, sans se rendre fautive, communiquer avec le cabinet d'avocats hongrois et la société SOCIETE1.) par courriels, y compris pour donner des indications de paiement.

La prétendue faute, tirée d'un défaut de précaution, reprochée par la société SOCIETE1.) serait dépourvue de toute réalité.

Elle aurait réagi de manière adéquate à l'incident avec le client polonais en faisant vérifier immédiatement son système informatique et en déposant plainte auprès de la police grand-ducale.

Elle relève que le client polonais n'a subi aucun dommage puisque ce dernier, en tant qu'homme normalement diligent, a eu le bon réflexe de la contacter pour demander la confirmation du prétendu changement de compte bancaire vers la Pologne.

Il y aurait absence du moindre lien entre les deux incidents, étant donné que ce serait Maître PERSONNE1.) qui se serait fait pirater et non pas le cabinet d'avocats luxembourgeois.

La société SOCIETE2.) fait encore valoir que même en admettant l'existence d'une quelconque faute dans son chef, celle-ci ne serait pas en relation causale directe et certaine avec le préjudice financier subi par la société SOCIETE1.).

La responsabilité du dommage subi incomberait aux cybercriminels et à la société SOCIETE1.), respectivement au cabinet d'avocats hongrois.

La société SOCIETE1.) et son avocat hongrois auraient été négligents en effectuant un premier paiement en date du 11 août 2020 sur un compte détenu auprès d'une banque en Indonésie par une entité dénommée « SOCIETE10.) », entité tout à fait distincte à la sienne.

Après avoir posé des questions quant au transfert de fonds en Indonésie, la société SOCIETE1.) et son avocat hongrois se seraient contentés d'une réponse abracadabrantesque, communiquée par les cybercriminels se faisant passer pour Maître PERSONNE2.).

Malgré le rejet des premiers virements par la banque du ou des cybercriminels, la société SOCIETE1.) et son avocat hongrois n'auraient pas hésité à effectuer des virements sur un compte d'une banque en Indonésie, ouvert cette fois-ci au nom d'une entité « CV SOCIETE2.) », avec une adresse à ADRESSE4.).

La société SOCIETE1.) et son avocat hongrois auraient fait preuve d'une négligence inouïe en faisant lesdits virements sans contacter le cabinet d'avocats luxembourgeois par téléphone pour recueillir des explications sur les modalités de paiement pour le moins extravagantes qui leur étaient proposées.

Ils auraient dû être interpellés par le fait qu'ils étaient invités à transférer l'argent sur un compte bancaire en Indonésie, ce d'autant plus que le titulaire fut dans un premier temps une entité dénommée « SOCIETE10.) », puis dans un deuxième temps un titulaire dénommé « CV SOCIETE2.) », avec une adresse à ADRESSE4.), étant rappelé que le transfert d'argent avait pour finalité de justifier devant le tribunal de commerce de Luxembourg l'existence de liquidités disponibles d'une société de droit luxembourgeois, assignée en faillite.

Le jugement de première instance serait donc à confirmer en ce qu'il a retenu que la société SOCIETE1.) reste en défaut de rapporter la preuve d'un comportement fautif dans le chef de la société SOCIETE2.), alors qu'au contraire, ses propres négligences et la violation de sa propre obligation de prudence seraient établies.

Il y aurait également lieu de rejeter la demande en institution d'une expertise pour déterminer les origines de l'acte de piratage, étant donné que la réponse à cette question ne serait pas pertinente pour l'issue du présent litige.

La société SOCIETE1.) conteste les allégations de la société SOCIETE2.) et de la société SOCIETE8.) consistant à dire qu'en l'espèce c'est le cabinet d'avocat hongrois qui a été victime d'un « phishing » le 22 juillet 2020 ou à une date antérieure.

L'avis de la société SOCIETE8.) serait unilatéral et critiquable, manquant d'impartialité.

En outre, il serait totalement contredit par les avis fournis par les experts informatiques hongrois, qui attestent que les services informatiques de l'étude d'avocats hongrois n'ont pas fait l'objet d'une intrusion et estiment que l'interception frauduleuse s'est manifestement effectuée auprès de Maître PERSONNE3.).

Appréciation de la Cour d'appel

Les parties étaient contractuellement liées, de sorte que la demande de la société SOCIETE1.) en obtention de dommages et intérêts pour préjudices matériel et moral est à analyser sur base de la responsabilité contractuelle.

Afin de prospérer dans sa demande, il appartient à la société SOCIETE1.) de rapporter la preuve que son dommage trouve sa cause dans une inexécution contractuelle commise par la société SOCIETE2.).

Les moyens développés par la société SOCIETE1.) quant à la charge de la preuve des inexécutions contractuelles qui, pour l'obligation d'information et de conseil seraient de résultat, de sorte qu'il incomberait à la société SOCIETE2.) de s'exonérer de la responsabilité pesant sur elle, sont à rejeter.

En effet, les inexécutions contractuelles reprochées par l'appelante ne constituent pas des manquements aux obligations d'information ou de précaution usuelles et accessoires au contrat de mandat entre parties, mais des manquements à des obligations supplémentaires d'information et de précaution que la société SOCIETE1.) estime avoir été, en l'espèce, à la charge de la société SOCIETE2.) à la suite de l'incident avec le client polonais.

Il incombe dès lors à la société SOCIETE1.) de rapporter la preuve que la société SOCIETE2.) a adopté un comportement fautif après l'incident avec le client polonais et que ce comportement est en relation causale avec le dommage subi.

La société SOCIETE1.) ne fait aucun reproche à la société SOCIETE2.) en ce qui concerne la cyberattaque elle-même.

La Cour d'appel rejoint dès lors les juges de première instance et retient que dans la mesure où la cyberattaque en soi n'est pas reprochée à la société SOCIETE2.), il n'y a pas lieu de s'attarder sur la question de savoir où se trouve l'origine de la faille informatique.

Les développements des parties en relation avec l'intrusion des hackers sont ainsi sans pertinence et il n'y a pas lieu de faire droit à la demande en institution d'une expertise informatique.

Il ressort des pièces versées en cause qu'après l'incident avec le client polonais, la société SOCIETE2.) a immédiatement pris contact avec son prestataire informatique qui l'a rassurée qu'après vérification, le courriel incitant le client polonais à virer l'argent sur un compte bancaire polonais n'était pas sorti de ces serveurs et qu'aucune action n'était à faire sur le système informatique du cabinet.

Le prestataire informatique a encore conseillé à la société SOCIETE2.) de s'adresser au client polonais pour que ce dernier vérifie son système antispam avec son service informatique.

Lors de l'incident avec le client polonais, il n'a pas été question d'une interception et d'un relayage des courriels électroniques entre parties par un ou des cybercriminels, faisant usage de la pratique du « man in the middle ».

La société SOCIETE2.) fut seulement mise au courant que le client polonais avait reçu des courriels de la boîte mail « prénomMAIL2.) » et que ces courriels n'étaient pas sortis de ses serveurs.

S'il est exact que la société SOCIETE2.) savait que le cybercriminel avait copié son logo et sa signature, toujours est-il qu'un tel copiage est extrêmement facile compte tenu des publications officielles concernant les études d'avocats et qu'aucune mesure efficace aux fins d'éviter un tel copiage n'est dès lors possible.

Il suit de ce qui précède que la société SOCIETE2.) a pu légitimement croire que le problème résidait du côté du client polonais, qu'il s'agissait d'un évènement isolé et que son système informatique n'était pas en cause.

Ainsi, la société SOCIETE2.) ne pouvait pas soupçonner que l'évènement allait se reproduire auprès d'un autre client.

La Cour d'appel rejoint les juges de première instance pour avoir retenu que la société SOCIETE2.) n'avait aucune raison de mettre en doute la sécurité de son système informatique et pouvait dès lors légitimement continuer à correspondre par courriels électroniques, qui sont devenus le moyen de communication usuel en la matière.

Il s'ensuit que le cabinet d'avocats luxembourgeois n'a pas adopté un comportement fautif en n'informant pas tous ses clients présents et futurs de l'incident qui s'était produit avec le client polonais.

Le reproche que la société SOCIETE2.) n'a pas pris au sérieux l'incident avec le client polonais tombe à faux, étant donné qu'elle a réagi en s'adressant à son prestataire informatique et en déposant plainte.

Face au fait que la société SOCIETE2.) a été rassurée qu'aucune intrusion n'avait eu lieu et qu'aucune action n'était à faire sur son système informatique, il ne peut être reproché à la société SOCIETE2.) d'avoir continué à demander par voie de courriels de se voir transférer de l'argent sur son compte tiers, ce qui constitue une pratique courante.

Pour les mêmes raisons, il ne saurait être retenu que la société SOCIETE2.) a commis une faute en omettant de se faire confirmer tous les éléments sensibles par téléphone ou autre.

La société SOCIETE8.) est formelle pour dire qu'il n'y a pas de lien entre les événements analysés en juillet 2020 et ceux analysés en septembre 2020 et la preuve d'un tel lien, en dehors des affirmations de la société SOCIETE1.) consistant à dire qu'il ne peut pas s'agir d'une coïncidence, fait défaut.

La société SOCIETE2.) a pris les précautions d'usage en ce qui concerne sa demande de virement du montant de 1.050.000 EUR sur son compte tiers, en rédigeant une déclaration avec indication de son compte bancaire, tout en demandant de se voir retourner ladite déclaration après signature, déclaration qui fut cependant interceptée par les hackers et lui retournée par courriel avec la signature contrefaite de la société SOCIETE1.).

Le dommage trouve sa cause dans l'escroquerie commise par le ou les cybercriminels, ensemble avec le manque de prudence de la société SOCIETE1.), assistée du cabinet d'avocats hongrois, qui a viré le montant de 1.050.000 EUR d'abord sur un compte détenu auprès d'une banque en Indonésie par une entité dénommée « SOCIETE10.) », entité tout à fait distincte de la société SOCIETE2.), et ce malgré une explication manifestement incompréhensible du ou des cybercriminels, écrivant au nom de Maître PERSONNE2.).

Ensuite, après un premier rejet par la banque des hackers, la société SOCIETE1.) a encore viré le montant de 1.050.000 EUR auprès d'une banque en Indonésie au nom d'une entité « CV SOCIETE2.) », ayant son adresse à ADRESSE4.), et ce malgré le fait qu'elle avait des suspicions tel qu'il ressort d'un courriel versé en cause, intercepté par le ou les cybercriminels.

Malgré l'incident avec le client polonais, qui n'avait conduit à aucun dommage, il ne peut être reproché à la société SOCIETE2.) de ne pas avoir prévu que la société SOCIETE1.), représentée par un avocat, était susceptible de se laisser convaincre à effectuer un virement sur un compte bancaire en Indonésie au nom d'une entité différente que la sienne, avec une adresse à ADRESSE4.) en relation avec un litige au Luxembourg et lors duquel il s'agissait de virer de l'argent sur le compte bancaire de la société SOCIETE2.), ayant son siège social au Luxembourg, aux fins de démontrer que les conditions de la faillite de la filiale luxembourgeoise SOCIETE4.) n'étaient pas remplies.

Il suit de tout ce qui précède que la société SOCIETE1.) reste en défaut de prouver une inexécution contractuelle à charge de la société SOCIETE2.) en relation causale avec le dommage réclamé.

Le jugement entrepris est dès lors à confirmer pour avoir débouté la société SOCIETE1.) de sa demande en obtention de dommages et intérêts pour préjudices matériel et moral.

Au vu de l'issue du litige, c'est à bon droit que la société SOCIETE1.) a été déboutée de sa demande en obtention de frais d'avocat pour la première instance.

Pour la même raison, sa demande en obtention de remboursement de frais d'avocat pour l'instance d'appel n'est également pas fondée.

C'est cependant à tort que la société SOCIETE1.) a été condamnée au paiement d'une indemnité de procédure pour la première instance, comme il n'est pas inéquitable de laisser à la charge de la société SOCIETE2.) toutes les sommes par elle exposées et non comprises dans les dépens.

Pour les mêmes motifs, il y a lieu de débouter la société SOCIETE2.) de sa demande en paiement d'une indemnité de procédure pour l'instance d'appel.

Au vu de l'issue du litige, c'est à bon droit que la société SOCIETE1.) a été déboutée de sa demande en obtention d'une indemnité de procédure pour la première instance et elle est à débouter de sa demande afférente pour l'instance d'appel.

La demande en exécution provisoire de l'arrêt est sans objet, les arrêts ne faisant pas l'objet de recours suspensif.

PAR CES MOTIFS

la Cour d'appel, deuxième chambre, siégeant en matière civile, statuant contradictoirement,

reçoit l'appel,

le déclare partiellement fondé,

réformant,

dit la demande de la société à responsabilité limitée SOCIETE2.) en obtention d'une indemnité de procédure pour la première instance non fondée,

décharge la société de droit hongrois SOCIETE1.) de la condamnation de payer à la société à responsabilité limitée SOCIETE2.) le montant de 2.000 EUR à titre d'indemnité de procédure pour la première instance,

confirme le jugement entrepris pour le surplus,

déboute la société de droit hongrois SOCIETE1.) de sa demande en obtention de frais d'avocat pour l'instance d'appel,

déboute les parties de leur demande respective en obtention d'une indemnité de procédure pour l'instance d'appel,

dit la demande en exécution provisoire de l'arrêt sans objet,

condamne la société de droit hongrois SOCIETE1.) aux frais et dépens de l'instance d'appel avec distraction au profit de Maître Jean MINDEN qui la demande, affirmant en avoir fait l'avance .

La lecture du présent arrêt a été faite en la susdite audience publique par Danielle SCHWEITZER, président de chambre, en présence du greffier Alexandra NICOLAS.