CYBER-ATTAQUE : LE PRESTATAIRE RESPONSABLE POUR DEFAUT DE CONSEIL !

Les jurisprudences sur la responsabilité en cas de cyber attaque sont (encore) rares et l'arrêt de la Cour d'appel de Rennes du 19 novembre 2024 ([1]) mérite déjà, pour cette simple raison, une lecture attentive.

Nous en ferons volontairement de nombreuses citations, pour envisager dans quelle mesure la Cour (i) répond aux demandes d'une société cyber attaquée par la faute (?) de son prestataire et (ii) statue sur la demande d'indemnisation du préjudice subi.

Des faits aujourd'hui tristement classiques…

La société [cyber-attaquée] *"fabrique des portails". "Elle n'est pas un professionnel de l'informatique"* bien qu'elle dispose d'un *"service informatique… constitué de trois personnes".*

En 2019, la société [cyber-attaquée] a *"établi [un] projet de remplacement des serveurs et de la baie SAN"*.

"Sur la base du cahier des charges … établi" [par la société future cyber attaquée], le prestataire *"qui s'affiche spécialiste en matière de cybersécurité"* a *"proposé le renouvellement [des] infrastructures"* IT incluant une *"phase de gestion de projet"* et *"la rédaction… d'un plan de sauvegarde".*

La proposition commerciale du prestataire comportait *"un schéma des montages techniques nécessaires à l'installation d'une nouvelle architecture"* [IT] qui *"illustre la complexité informatique du projet".* Point essentiel du litige à venir, les *"travaux"* du prestataire *"ne comportaient pas l'installation de sauvegardes déconnectées".*

"L'offre de prix du 25 juillet 2019" du prestataire s'élevait à 161.000 euros HT. La société [future cyber-attaquée] accepte l'offre, signe apparemment les "CGV" du prestataire et le prestataire installe le matériel en novembre 2019.

Le 25 février 2020, le prestataire transmet à la société [cyber-attaquée] un *"projet de contrat d'assistance"* (de gestion des sauvegardes des données ?) qui ne sera jamais formellement ni accepté, ni rejeté par la société [cyber-attaquée].

Suite à un *"fishing"* [sic] *"durant la nuit du mercredi 17 juin 2020, [le fabricant de portail] a été victime d'une cyberattaque par rançongiciel. Les [attaquants] ont procédé au chiffrement complet de son système d'information, dont les systèmes de sauvegarde".*

"L'activité de la société [cyber-attaquée] a été intégralement à l'arrêt durant une semaine".

Une rançon a-t-elle été demandée ? Payée ? L'arrêt de la Cour n'évoque aucun de ces deux points.

Le 30 juillet 2020, la société [cyber-attaquée] met en demeure le prestataire pour indemnisation de son préjudice puis l'assigne sur le fondement de *"manquements à son obligation d'information, de conseil et de délivrance".*

Le 19 novembre 2024, la Cour d'appel de Rennes décide que *"le [prestataire] a manqué à ses obligations en matière d'information et de conseils"* et le condamne à indemniser son client cyber-attaqué.

Le "devoir d'information et de conseil" du prestataire

Le devoir d'information et de conseil à la charge des prestataires informatiques fait l'objet de nombreuses jurisprudences depuis des années.

1 Cour d'appel de Rennes 3ème chambre commerciale 19 novembre 2024 RG n°23/04627
https://www.courdecassation.fr/decision/673d7ce6d666990c113dbf0c

Depuis la réforme du Code civil de 2016, l'obligation de conseil des prestataires est un impératif légal imposé par l'article 1112-1 ([2]) dont aucun prestataire ne peut s'exonérer, de quelque manière que ce soit. Il s'agit d'une obligation *"pré-contractuelle"* nous précise une jurisprudence de 2022 ([3]).

Dans un monde idéal, en cas de mise en chantier d'un projet de refonte de l'infrastructure IT d'une entreprise, cette entreprise doit d'abord rédiger un cahier des charges, ce qui est le cas de notre société cyber-attaquée.

Le prestataire pour sa part avait effectivement répondu aux demandes de son futur client, mais sans remettre en cause ni lui rappeler l'oubli des *"sauvegardes non connectées".*

Or, la cyber-attaque au cryptolocker de juin 2020 avait chiffré tout le système d'information de la société cyber attaquée, dont la totalité des sauvegardes qui étaient toutes connectées. Ne restaient donc plus aucune donnée accessible à notre fabricant de portail.

Manifestement, le cahier des charges n'était pas pertinent sur ce point. Et le prestataire n'avait rien écrit en ce sens à son client. Pire, au mois de février 2020, le prestataire avait proposé à son client des prestations additionnelles sous la forme d'un *"projet de contrat d'assistance"*. Et le client n'avait alors formellement ni accepté, ni rejeté ce contrat et le prestataire n'avait pas insisté. A tort…

Que disent les CGV du prestataire ? "les normes standards et les usages internationaux" (soupirs)

Le prestataire écrivait dans ses CGV *"mettre en œuvre les mesures de sécurité techniques et d'organisation de systèmes de services* [sic] *se conformant aux normes standards et aux usages internationaux"*. Difficile d'écrire une clause plus bidon que celle-ci !

La question qu'aurait dû se poser la Cour de Rennes est la suivante : ne proposer que des sauvegardes déconnectées est-il conforme *"aux normes standards et aux usages internationaux"* ? Et la réponse de la Cour aurait dû être "non".

Tout juriste normalement consciencieux aurait dû vérifier ce point en recherchant les normes et usages techniques en matière de cyber-sécurité connus à l'époque des faits : (i) le *"guide d'hygiène informatique"* de l'ANSSI de 2017 ([4]) et (ii) la norme ISO 27001 version 2013 (5).

Le guide de l'ANSSI est *on-ne-peut-plus* clair sur la nécessité de mettre en place des sauvegardes non-connectées ([6]) : *"Les données vitales au bon fonctionnement de l'entité que détiennent les postes utilisateurs et les serveurs doivent faire l'objet de sauvegardes régulières et stockées sur des équipements déconnectés, et leur restauration doit être vérifiée de manière périodique".*

Vous doutez encore ? La mesure 37 du même guide de l'ANSSI recommande de *"formaliser une politique de sauvegarde régulièrement mise à jour"* en y intégrant *"au moins … les différents types de sauvegarde (par exemple le mode hors ligne)".*

Coupons - tout de suite - court à la remarque selon laquelle une *"recommandation"* (de l'ANSSI ou de la CNIL) *"n'a pas de caractère normatif"* (ne serait pas juridiquement obligatoire). Le rôle des autorités de contrôle est précisément de définir "l'état de l'art". C'est ce que rappelle systématiquement l'ANSSI dans ses *"référentiels d'exigences"* qui comportent aujourd'hui une définition de "l'état de l'art" ([7]) : *"ensemble des bonnes pratiques,*

---

2 Article 1112-1 Code civil : "*Celle des parties qui connaît une information dont l'importance est déterminante pour le consentement de l'autre doit l'en informer dès lors que, légitimement, cette dernière ignore cette information ou fait confiance à son cocontractant. Néanmoins, ce devoir d'information ne porte pas sur l'estimation de la valeur de la prestation. Ont une importance déterminante les informations qui ont un lien direct et nécessaire avec le contenu du contrat ou la qualité des parties. Il incombe à celui qui prétend qu'une information lui était due de prouver que l'autre partie la lui devait, à charge pour cette autre partie de prouver qu'elle l'a fournie. Les parties ne peuvent ni limiter, ni exclure ce devoir…*"

3 CA Versailles 25 octobre 2022 n° RG 21/02882
https://www.courdecassation.fr/decision/export/6358ce0cc40aa805a7864e01/0

4 ANSSI "*guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures*" version 2.0 septembre 2017 https://cyber.gouv.fr/publications/guide-dhygiene-informatique

5 Hélas encore, les normes ISO sont protégées par le droit d'auteur et il n'est pas possible d'y accéder librement, sauf à en payer une copie… https://www.iso.org/fr/standard/27001

6 Mesure renforcée n°14 " *Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique*" ANSSI Guide d'hygiène informatique précité

7 Voir par exemple l'article I.3.2 du référentiel d'exigences ANSSI "PVID v1.1" du 1er mars 2021 https://cyber.gouv.fr/sites/default/files/document/PVID_referentiel-exigences_v1.1.pdf ou l'article 1.3.2 du référentiel d'exigences ANSSI "SecNumCloud v3.2" du 8 mars 2022 https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf

des technologies et des documents de référence relatifs à la sécurité des systèmes d'information… publiquement accessibles, et des informations qui en découlent de manière évidente". Pour le dire en mots simples, si c'est "recommandé" par l'ANSSI dans une publication officielle, c'est obligatoire !

La CNIL dit exactement la même chose sur l'état de l'art en matière de mot de passe ([8]) : *"Les dispositions de cette recommandation, qui n'ont pas un caractère normatif, correspondent à l'état de l'art auquel tout responsable de traitement devrait se conformer, a minima".*

Coté norme ISO27001 version 2013, les sauvegardes non connectées ne sont pas évoquées du tout (ni dans la version 2022 d'ailleurs), ce qui conduit à s'interroger sur la pertinence de cette norme et des certifications délivrées mais c'est là un autre débat.

Au final, si un prestataire ne respecte pas les *"normes standards et [les] usages internationaux"* en matière de cyber-sécurité, ce prestataire est fautif par négligence au sens du Code civil ! Et qui dit *négligence qui cause un dommage* dit *responsabilité.*

Rappelons ici le texte de l'article 1241 du Code civil : *"Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence".*

Hélas, comme souvent, la Cour d'appel de Rennes n'évoque aucunement dans sa décision le manquement contractuel - pourtant évident - du prestataire aux règles de base de cyber-sécurité évoquées *si pudiquement* dans les "CGV" du prestataire…

Le redimensionnement du "devoir de conseil"

En revanche et de manière très pragmatique, la Cour retient que *"si le prestataire estimait que le document [cahier des charges] transmis par la société [cyber-attaquée] n'était pas suffisamment précis sur la définition des attentes, le prestataire devait la solliciter pour faire préciser sa commande. Au besoin elle devait la conseiller sur l'architecture nécessaire à la sécurisation de ses données et lui signaler que ses travaux ne comportaient pas l'installation de sauvegardes déconnectées".*

Le prestataire ne doit donc pas se cantonner à insérer une clause franchement vague dans ses CGV ni se cantonner à répondre par écrit point par point aux demandes exprimées par son client. Au contraire, le prestataire doit pousser son conseil jusqu'à remettre en cause les postulats techniques erronés ou incomplets retenus par son client, voire le conseiller de manière pro-active vers "l'état de l'art", en l'espèce, la mise en place *en plus* de sauvegardes non connectées.

Les arguments de la défense judiciaire du prestataire

Voyons maintenant les arguments (infructueux) de la défense du prestataire devant la Cour d'appel (alors qu'il avait tout gagné devant le Tribunal de commerce de Nantes).

Le client disposait d'un service informatique : c'était donc à lui de prévoir ces sauvegardes déconnectées. Non ! répond la Cour d'appel en précisant que la société [cyber-attaquée] *"fabrique des portails"* et n'est donc *"pas un professionnel de l'informatique"* bien qu'elle dispose d'un *"service informatique… constitué de trois personnes".* La Cour ajoute que ces trois personnes *"ne peuvent se voir attribuer les mêmes compétences expertales que celles qui sont revendiquées par [le prestataire]"* (ce qui parait de bon sens).

La mission contractuelle du prestataire ne prévoyait pas de *"maitre d'œuvre pour piloter le projet"* ? Tant pis ! répond encore la Cour d'appel : vu le *"coût de son intervention",* c'était au prestataire d'assumer ce rôle de maitre d'œuvre. Sur ce point, nous conclurons donc que, selon la Cour d'appel de Rennes, *plus un projet est cher, plus le prestataire assure un rôle prépondérant de conseil à l'égard de son client,* allant jusqu'à la maitrise d'œuvre du projet dans son ensemble. Voilà bien une décision qui devrait faire trembler les prestataires !

Autre argument du prestataire en défense : il avait proposé un *"projet de contrat d'assistance"* mais le client n'avait pas donné suite. Si *pas de contrat signé*, pas d'obligation contractuelle ! Et la solution de sauvegardes connectées aurait, selon le prestataire, entrainée un cout supplémentaire à la charge du client. Donc le prestataire trouvait normal de n'avoir pas évoqué cette option avec son client.

8 Voir l'article 1.5 Délibération [CNIL] n°2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation-2022-100-du-21-juillet-2022_recommandation-aux-mots-de-passe.pdf

La charge de la preuve de la bonne exécution du devoir de conseil et ses conséquences

Alors, à qui la faute ? Qui doit prouver quoi pour l'emporter ? La Cour d'appel tranche net ce point : *"Le [prestataire] ne démontre pas [qu'il] a proposé cette solution à sa cliente [la société cyber-attaquée] ni que dans ce cas la société [cyber-attaquée] a refusé".* Cette preuve incombe donc au prestataire.

Circonstance aggravante ([9]) dans le défaut de conseil, notre prestataire s'affichait (apparemment publiquement) *"spécialiste en matière de cybersécurité"* ! Et, comme le relève la Cour dans une sorte de deuxième *effet Kiss Cool*, le "*sinistre [la cyber-attaque] [n'avait] même pas été anticipé par le prestataire*"… Est-on un professionnel "*raisonnable*" ([10]) (*comprendre "normalement compétent" ?*) lorsque l'on n'anticipe pas un problème que tout professionnel "*raisonnable*" connait ? Pour les professionnels de la cyber-sécurité, la Cour d'appel répond juste "non".

Et la conclusion de la Cour d'appel tombe alors : *"Il est donc établi que le [prestataire] a manqué à ses obligations en matière d'information et de conseils vis à vis de la société [cyber-attaquée]"*.

Et voici les conséquences pratiques que retient la Cour d'appel : *"En matière de prestations informatiques comprenant l'installation d'une nouvelle architecture, considérées comme un produit complexe, le [prestataire] a l'obligation de s'assurer que ses prestations répondent aux besoins de son client, qu'il aura analysés". Pour y parvenir [le prestataire] doit s'informer sur ses besoins pour lui présenter une proposition commerciale adaptée".*

En synthèse, le prestataire commet une faute pour ne pas avoir proposé à son client une option payante supplémentaire qui ne répondait à aucune demande du cahier des charges. Si vous êtes prestataire, vous devriez jeter un coup d'œil sur ce que prévoient vos "CGV" / CGU / contrats, *des fois que* vos documents contractuels disent (par hasard) le contraire…

La disparition de l'argument de la "délivrance" non conforme

Devant le Tribunal de commerce de Nantes, la société cyber-attaquée avait soulevé l'argument de la *"délivrance non conforme"* des prestations livrées. La Cour n'en dit pas un mot dans son arrêt, ce qui se comprend aisément.

Le défaut de délivrance conforme nécessite la démonstration d'engagements contractuels pris par le prestataire qui n'auraient pas été respectés. Comme ni le cahier des charges, ni la proposition du prestaire n'évoquaient la délivrance de sauvegardes non connectés, il est légitime de ne pas juger la prestation livrée "non conforme". L'argument ne pouvait donc pas prospérer.

La disparition de l'argument de la "faute lourde"

La Cour ne retient pas la faute lourde du prestataire pour manquement à ses obligations contractuelles. En réalité, l'arrêt n'en parle tout simplement pas !

Cette notion de faute "lourde" est pourtant explicitement prévue en matière contractuelle dans notre Code civil à l'Article 1231-3 ([11]) lorsque l'inexécution concerne une condition substantielle du contrat ([12]). Si une "simple" faute ([13]) permet de prononcer la résiliation d'un contrat, l'intérêt de la faute lourde est d'échapper aux clauses limitatives de responsabilité prévue au contrat, donc d'obtenir une plus large indemnisation du préjudice subi ([14]). Hélas, plutôt que d'analyser contractuellement les obligations des parties, sur ce point encore, la Cour botte en touche et ne répond que sur le fondement du devoir de conseil qui aurait entrainé la *"perte d'une chance d'éviter un sinistre".*

La "perte d'une chance d'éviter un sinistre" ?

La jurisprudence retient que *"seule constitue une perte de chance réparable, la disparition actuelle et certaine d'une éventualité favorable"* ([15]) qui cause un préjudice. Dans notre arrêt du 19 novembre 2024, la perte d'une chance pour notre entreprise cyber-attaquée est la conséquence directe du manquement du prestataire à son

9 Principe légal dans notre Code pénal seulement
10 Article 1188 du Code civil version 2016 qui remplace la notion de "*bon père de famille*" (utilisée depuis 1804) par celle de "*personne raisonnable*"
11 Article 1231-3 du Code civil : "*Le débiteur n'est tenu que des dommages et intérêts qui ont été prévus ou qui pouvaient être prévus lors de la conclusion du contrat, sauf lorsque l'inexécution est due à une faute lourde ou dolosive*"
12 Cass. Civ. 1re, 2 décembre 1997, no 95-21.907 - D. 1998. Somm. 200, obs. D. Mazeaud - JCP 1998. I. 144, nos 10 s., obs. Viney - LPA 24 juill. 1998, note Briton
13 Les juristes les plus pointu(e)s rappelleront qu'en matière contractuelle, il n'est pas besoin de "faute" au sens de la responsabilité délictuelle mais seulement d'un "manquement" (non-respect) à une obligation prévue dans le contrat.
14 … pour autant que le préjudice allégué soit prouvé pour le Tribunal (ce qui pose un véritable problème à la lecture de cet arrêt)
15 1ère Civ., 8 mars 2012, n°11-14.234)

devoir de conseil. Si le client avait été bien conseillé, il aurait eu la chance (???) de limiter les effets de la cyber-attaque.

Sur le principe, la Cour d'appel applique les critères classiques de la jurisprudence en la matière : le demandeur doit démontrer qu'une chance a été perdue ([16]), même si la chance perdue est statistiquement faible ([17]). La Cour d'appel nous précise que *"l'indemnité doit être mesurée à la chance perdue d'éviter le fishing* [sic] ([18]) *mais ne peut être égale au dommage résultant de ce sinistre*", ce qui est parfaitement logique en droit.

Techniquement, l'argument est bancal dans la mesure où, si l'origine de la cyber-attaque était un phishing, les "credentials" (login + mot de passe) volées à *l'insu du plein gré* d'un(e) salarié(e) de l'entreprise cyber-attaquée ne sont pas la cause du chiffrement du système d'information, mais seulement un moyen pour l'attaquant d'y pénétrer. Une fois le SI *compromis*, l'attaquant a eu beau jeu de chiffrer l'ensemble, sauvegardes connectées comprises. Juridiquement, la chance perdue aurait dû être celle de restaurer les données du système d'information, et partant, de redémarrer rapidement et sans trop de dommage le système d'information. Mais bon…

Alors, quelle indemnisation pour quels préjudices ? Les juristes s'intéressent aux fondements légaux des décisions judiciaires (ici, le devoir de conseil) mais beaucoup plus rarement à la nature et à la preuve des préjudices indemnisables. C'est pourtant l'unique raison des actions judiciaires pour les justiciables, consommateurs comme professionnels.

Le sujet n'est pas drôle, mais il est central lorsqu'on vient à mener une action judiciaire : quels sont les principes permettant d'obtenir des dommages-intérêts ? Et que fournir à un tribunal pour justifier de ses demandes d'indemnisation en cas de dommages causés par une cyber-attaque ?

<u>Les préjudices à indemniser, parents pauvres de l'arrêt du 19 novembre 2024</u>

Les principes du Code civil sont inchangés depuis 1804 en France : ils sont tout entier contenus dans l'article 1231-2 du Code civil : *"Les dommages et intérêts dus au créancier sont, en général, de la perte qu'il a faite et du gain dont il a été privé, sauf les exceptions et modifications ci-après".*

Pas de besoin de faire de longues recherches de jurisprudence, la Cour de cassation a exposé publiquement sa doctrine (inchangée à ce jour) en 2013 ([19]). Retenons-en deux citations :

La perte éprouvée *"est la perte effectivement subie par le créancier du fait de l'inexécution d'une obligation contractuelle, d'un délit ou quasi-délit… Il s'agit de constater la réalité des biens détruits ou des frais engagés… (devis, commandes, factures, contrats) … la réparation doit être égale au montant nécessaire à la remise en état de la chose… Les dépenses induites, enfin, sont purement matérielles".*

Le gain manqué *"est un manque à gagner certain (le gain était dû et aurait dû être perçu) … correspond à la marge bénéficiaire manquée. Celle-ci ne saurait être assimilée purement et simplement au chiffre d'affaires ni au bénéfice net, mais correspond à la marge sur coûts variables, c'est-à-dire un chiffre d'affaires diminué de toutes les charges variables… Les gains manqués devraient s'analyser comme la différence entre les revenus manqués et les coûts économisés".*

Alors, que dire de l'attribution des dommages-intérêts par la Cour de Rennes à notre entreprise cyber-attaquée ?

L'arrêt commence bien puisque la Cour d'appel relève que *"la société [cyber attaquée] … a supporté des charges considérables liées à l'intervention de plusieurs prestataires extérieurs et au travail réalisé par ses salariés pour la récupération et la réorganisation des données nécessaires [à son] fonctionnement".*

Les choses se compliquent avec la démonstration de la réalité des préjudices. Trois postes de préjudices sont allégués : (i) les coûts externes de la remise en état du système d'information, (ii) les frais internes et (iii) une atteinte à l'image de l'entreprise cyber attaquée.

Sur les coûts externes de remise en état de fonctionnement du système d'information, la Cour d'appel constate la réalité du préjudice subi par la production des factures des prestataires intervenus *post-attaque*. La somme totale de 62 680,03 € HT "est donc justifiée" précise la Cour au regard des diligences accomplies par ces

16 Cass. Crim. 25 octobre 2000, n°00-80.433
17 Cass. Civ. 1re, 16 janvier 2013
18 Lire "phising" ou hameçonnage : rien à voir avec la pêche…
19 Bulletin d'information de la Cour de cassation n°781 mai 2013 "*Le préjudice économique des entreprises*"

prestataires. Pourtant, dans son *par ces motifs*, la Cour *"condamne le prestataire à verser à la société [cyber-attaquée] la somme de 50.000 euros".* Comprenne qui pourra…

Concernant les coûts internes, la société cyber-attaquée communique un tableau des heures passées par ses salarié(e)s pour la récupération des données perdues, tableau attesté par expert-comptable. Concrètement, les salarié(e)s ont dû délaisser leurs taches habituelles pour s'occuper exclusivement (on comprend bien pourquoi) de la récupération des données *cryptolockées* par l'attaquant.

Sur ce point, la Cour d'appel rejette d'un revers de main toute demande d'indemnisation fondée sur le paiement des salariés au motif "qu'il appartient à l'employeur de régler ses salariés" ! Les motivations de l'arrêt nous semblent particulièrement critiquables et l'envie nous prend de répliquer à la Cour "*c'est un peu court, jeune homme*" ([20]). Refuser cette indemnisation nous paraît incohérent dès lors que les salarié(e)s de l'entreprise cyber-attaquée n'ont pas pu remplir leurs missions pendant toute la durée de l'interruption de fonctionnement du système d'information. L'entreprise victime de la cyber-attaque n'avait pourtant d'autre solution que de mobiliser ses propres ressources humaines pour restaurer le fonctionnement normal de son système d'information.

L'arrêt est d'autant plus surprenant que la même Cour de Rennes avait jugé en 2023 *"qu'il est acquis que lorsqu'une entreprise modifie son architecture informatique ses salariés consacrent du temps à l'appréhension des nouveaux systèmes. […] Ces salariés qui ont été employés à d'autres tâches liées aux dysfonctionnements du système informatique n'a pas permis que leur force de travail soit utilement utilisée pour augmenter les performances de l'entreprise"* ([21]). Et la Cour d'accorder une indemnisation du préjudice subi par *la victime*. De la même manière, la Cour d'appel de Lyon avait validé une demande d'indemnisation similaire en décembre 2023 en précisant *"qu'il n'apparaît cependant pas contestable que les difficultés connues avec le système informatique ont nécessairement mobilisé les salariés au-delà de ce qu'aurait requis la mise en place d'un système adapté"* ([22]).

Il aurait fallu, prend le soin de préciser la Cour, *"que la société [cyber-attaquée] ait versé des salaires au titre d'heures supplémentaires et/ou fait appel à des recrutements dans le cadre de cette surcharge de travail"* ([23]) pour que la demande d'indemnisation de ce préjudice précis puisse prospérer. La décision de la Cour de Rennes est d'autant plus paradoxale que le recours à des dispositifs alternatifs, tels que le chômage partiel imposé aux salarié(e)s aurait très probablement conduit à une indemnisation de l'entreprise cyber-attaquée. Cette décision semble donc ignorer la réalité des conséquences matérielles subies par notre entreprise cyber-attaquée.

Le dernier poste d'indemnisation examiné par la Cour de Rennes concerne l'atteinte à l'image de la société cyber-attaquée. Ce point est traité de manière expéditive par la Cour, qui reconnaît toutefois – à juste titre – que *"la société [cyber-attaquée] n'a pas été en mesure de répondre dans les délais à ses partenaires"*. *"Sa réputation a donc été ternie"* retient sobrement la Cour, qui (*au doigt mouillé ?*) accorde à notre entreprise cyber-attaquée la somme de 5.000 euros de dommages-intérêts. Sur ce point, outre le caractère parfaitement arbitraire (et largement sous-évalué) de la somme attribuée, la Cour confond l'indemnisation d'un préjudice de type "gain manqué et perte subie" avec le préjudice d'image, très difficile à chiffrer. Il n'y a donc rien d'intéressant à retenir de cette décision sur ce point.

<u>Que retenir de cet arrêt de la Cour de Rennes ?</u>

Premier constat : plutôt que de faire une analyse contractuelle et argumentée des manquements du prestataire, la Cour a préféré fonder sa décision sur cette notion fluctuante de devoir de conseil. Sur ce point, l'arrêt du 19 novembre 2024 est pour les "prestataires informatiques" un véritable tremblement de terre (i) qui élargit considérablement leur obligation en cas de réponse à appel d'offre et (ii) qu'il sera extrêmement difficile d'encadrer contractuellement.

En matière de cyber-sécurité, chaque proposition de réponse à un appel d'offre avec cahier des charges devrait prévoir un engagement clair du prestataire à assistance à maitrise d'œuvre du projet du maitre d'ouvrage (le client) comportant (i) analyse (pour de vrai…) du cahiers des charges et des demandes du client et (ii) engagement de compléter, même avec des options payantes supplémentaires, l'ensemble des problématiques relevant de l'état de l'art (par exemple: des sauvegardes déconnectées).

---

20 "ha ! non ! c'est un peu court, jeune homme !" Acte Ier scène IV du "Cyrano de Bergerac" d'Edmond Rostand
21 Rennes, 3e chambre commerciale, 19 Septembre 2023, RG : 21/03352
22 Cour d'appel, Lyon, 3e chambre A, 7 Décembre 2023 – n° 20/03688
23 Voir sur ce point Cour d'appel de Versailles - 13e chambre 26 juillet 2022 / n° 21/03036

Ce qui est certain, à l'avenir, notamment en matière de conseil en cyber sécurité, c'est qu'il ne suffira pas à un prestataire de simplement répondre point par point à un cahier des charges pour prétendre *"avoir fait le job"*. Il est dorénavant nécessaire, pour qui se prétend prestataire, de faire une lecture "intelligente" des appels d'offre reçus, au point d'avoir le devoir légal d'en critiquer par écrit les manquements / oublis / erreurs…

Chers prestataires, vous devriez aussi arrêter de vous prétendre professionnel ou *"spécialiste de la cyber-sécurité"* ([24]) lorsque vous ne l'êtes pas : votre responsabilité sera alors aggravée comme le retient la Cour d'appel de Rennes.

Le second constat est celui de l'indemnisation judiciaire du préjudice. Les plaideurs et leurs conseils ont tendance à espérer beaucoup et au final à n'obtenir que bien peu. Le plus souvent, les preuves des préjudices sont oubliées, voire bâclées. Parfois, comme c'est le cas de cet arrêt, ce sont les juges qui semblent voir les choses *d'un peu loin* et ne pas comprendre la réalité des situations qui leur sont soumises.

A retenir pour celles et ceux qui placent leurs espoirs dans une décision de justice : faire un procès, c'est bien. Obtenir une réelle indemnisation de son préjudice, c'est tout de même mieux. Et - regrettons le - nos juges sont rarement sensibles à cette logique économique, qui est pourtant la raison d'être de la procédure judiciaire menée ici par notre entreprise cyber-attaquée.

Marc-Antoine LEDIEU Avocat au barreau de Paris - **Ledieu-Avocats**

Jean-Nicolas ROBIN Avocat au barreau de Rennes - **Avoxa Avocats**

24 Dans vos contrats, dans vos propositions commerciales, dans votre marketing…