L'indemnisation consécutive à une perte de données

les faits **Blocage de l'activité, atteinte à la réputation, temps passé à la reconstitution de fichiers, frais juridiques… Qu'elle soit accidentelle ou la conséquence d'une cyberattaque, une perte de données engendre des coûts considérables pour l'entreprise. Un jugement du Tribunal de commerce de Nanterre en date du 23 avril 2019 apporte un éclairage sur la question de l'évaluation et de l'indemnisation du préjudice subséquent.**

Dans cette affaire, une société industrielle dans le secteur des travaux publics avait conclu un contrat d'infogérance avec un prestataire, ayant pour objet l'externalisation de son système d'information et notamment la sécurisation et la mise en place de sauvegardes et de restauration. Suite à un problème informatique sur l'un des serveurs, la reconstitution de certains fichiers aboutit à la perte de plusieurs centaines de milliers de données non sauvegardées. L'expert judiciaire désigné pour établir la nature et le volume des fichiers disparus distingue toutefois le nombre de fichiers «perdus» et celui de fichiers dits «perdus et utiles» pour l'activité de la société. Faute pour la société victime de réussir à justifier la valeur réelle des données manquantes depuis sa création, les juges ont estimé que les dommages et intérêts alloués devaient être limités «*au coût du préjudice matériel des fichiers estimés perdus et utiles*» pour la poursuite de son activité, à savoir le coût de vérification et de reconstitution des fichiers concernés. Ce jugement apparaît contestable dans la mesure où comme dans le cas d'espèce, certaines données sans utilité immédiate ont néanmoins une valeur considérable, notamment les données relatives au fond documentaire d'une entreprise, son historique de construction ou sa veille concurrentielle, davantage inscrits dans un cadre normatif

Me Pierre-Randolph Dufau
Avocat à la cour
Fondateur de la SELAS
PRD avocats

qu'économique, à des fins probatoires par exemple, et qu'il faut prendre en compte dans l'évaluation des dommages et intérêts. Cette question de l'évaluation du préjudice posée, il convient de revenir sur les démarches à entreprendre pour se prémunir de toute nouvelle perte et obtenir réparation. Le premier réflexe en cas de cyberattaque ou de vol de données peut ainsi être de déposer plainte, le cas échéant auprès de brigades d'enquête spécialisées dans les technologies informatiques et se constituer partie civile. Vient ensuite la question de l'engagement éventuel de la responsabilité contractuelle du prestataire de services, si les données étaient hébergées, sauvegardées ou archivées dans le cadre d'un contrat d'infogérance comme en l'espèce. Là encore, la responsabilité est souvent limitée par l'insertion dans le contrat d'une clause limitative fixant un montant maximal d'indemnités, voire excluant certains dommages du champ de la responsabilité. L'application de cette clause peut toutefois être écartée par le juge en cas de faute lourde du prestataire. Ce ne fut pas le cas en l'espèce, les juges ayant considéré, alors même que l'objet du contrat était notamment la mise en place de sauvegardes sécurisées, que le prestataire avait agi avec diligence pour tenter de mettre un terme aux problèmes constatés et ayant donc appliqué le plafond d'indemnisation contractuellement fixé. D'où l'importance de la formulation des obligations, de moyens ou de résultat, mises à la charge des parties. Entre temps, l'entreprise peut tenter de mobiliser ses assurances, même si nombreuses sont celles qui excluent les cyber-risques.

ce qu'il faut retenir **Le préjudice lié à la perte de données est immatériel et donc difficile à évaluer. L'aménagement contractuel de la responsabilité du prestataire et la rédaction précise et détaillée de la nature des obligations à sa charge sont essentiels pour anticiper tout litige lié à la prise en charge des coûts de reconstitution des données perdues.**

Parcoursup ne communique pas son algorithme à un syndicat étudiant

Par une décision en date du 12 juin 2019, le Conseil d'État a rappelé que si la Loi pour une République numérique est venue consacrer le droit d'accès aux traitements algorithmiques et aux codes sources des documents administratifs, seuls les candidats inscrits sur Parcoursup peuvent toutefois se voir communiquer les critères d'examen de leurs candidatures et les codes des logiciels utilisés pour leur sélection. D'où le refus de communication de l'algorithme à un syndicat d'étudiants.

Nature juridique des messageries électroniques

La CJUE a estimé le 13 juin 2019 que l'activité d'un service de messagerie électronique sur Internet comme Gmail, qui utilise les services de fournisseurs d'accès internet tiers «ne consiste pas en la transmission de signaux sur des réseaux de communications électroniques» et n'est donc pas un «service de communications électroniques» au sens du droit européen.

Sanction confirmée pour faille de sécurité

Par une délibération du 28 mai 2019, la Cnil a prononcé une amende de 400000 euros à l'encontre d'une société spécialisée dans l'immobilier. Cette dernière avait par erreur laissé en libre accès sur son site des documents transmis par les candidats à la location, dont la copie de cartes d'identité et de cartes vitales. Informée de la faille, la société a mis dix jours à la corriger, délai interprété comme un manque de diligence.