Infogérance : maîtriser les risques contractuels

les faits **Si les avantages de l'infogérance sont indéniables – réduction des coûts, flexibilité, performance, technologie évolutive –, la décision de la Cour d'appel de Paris du 8 mars dernier rappelle que les risques le sont tout autant. Dans ce litige, une banque s'est trouvée sans accès à son système d'information pendant un mois. L'occasion de revenir sur les mécanismes contractuels à maîtriser pour éviter une telle situation.**

L'infogérant détecte une faille de sécurité chez sa cliente : les clés du système informatique et de l'attribution des droits d'administration ont été transmises à des employés non agréés. Soumis à une obligation de sécurité de résultat, il s'expose à être tenu responsable en cas de fuite de données, même d'origine interne et ce d'autant plus aujourd'hui à l'aulne de la directive NSI et du RGPD. En conséquence, le prestataire décide de mettre en place de nouveaux mots de passe et de ne pas les communiquer immédiatement à sa cliente. Cette dernière perd alors la maîtrise de son système d'information pendant presque un mois, remettant en cause la gouvernance de ses données. Pour ne pas restituer les mots de passe, l'infogérant se fonde sur une disposition du contrat d'infogérance : la clause de réversibilité. En effet cette clause, qui permet traditionnellement d'organiser la reprise en main du système par le client, était conditionnée à un délai de trois mois à partir du moment où le client en faisait la demande. Le prestataire refuse donc de redonner les accès avant l'expiration des trois mois. La banque a alors fini par reprendre d'autorité le contrôle de son système d'information, mettant, de fait, fin au contrat et plaçant les parties dans une situation d'insécurité

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

juridique totale. Qui était en tort ? L'infogérant qui avait refusé de communiquer les mots de passe avant trois mois ou la banque qui a résilié le contrat sans attendre ? Les décisions – Tribunal de commerce, Cour d'appel, Cour de cassation et renvoi – se sont enchaînées, prenant tour à tour le parti de l'une puis de l'autre. Après dix ans de procédure, la Cour d'appel de Paris les a finalement toutes les deux estimées fautives, l'une pour ne pas avoir rendu les accès et l'autre pour avoir résilié sans préavis.

Une si longue et coûteuse procédure aurait pu être évitée aux deux parties si elles n'avaient pas négligé les points de vigilance propres au contrat d'infogérance : la clause de réversibilité et la clause résolutoire. L'attention doit porter non seulement sur leurs contenus respectifs, mais également sur leur articulation. En l'espèce, le délai de trois mois avant la réversibilité est problématique en cas de manquements du prestataire rendant intenable la poursuite du contrat. Le délai est-il toujours requis alors même que la société d'informatique aurait manqué à ses obligations essentielles ? C'est ce doute d'interprétation qui a mis les parties dans une situation de blocage et a conduit à cette saga judiciaire. D'où la nécessité de prévoir toutes les situations : en cas de défaillance à ses obligations principales, l'application de la clause résolutoire devrait obliger le prestataire à organiser la reprise de l'exploitation du système d'information par son client sans délai. ■

ce qu'il faut retenir **La clause de réversibilité est indispensable car elle permet d'éviter une situation de dépendance et d'organiser la réappropriation du système d'information. Cependant, il est crucial qu'elle définisse clairement la durée de réversibilité et ses étapes, et ce même en cas de résolution du contrat.**

Clauses abusives de Facebook

Par un jugement du 9 avril 2019, le TGI de Paris a déclaré abusives et illicites 430 clauses des conditions générales d'utilisation (CGU) du réseau social Facebook. Les clauses figuraient dans les CGU de 2013, 2015 et 2016 et visaient tant la responsabilité du réseau et les droits des utilisateurs que sa politique de données. Ce jugement suit deux autres jugements du TGI de Paris déclarant comme abusives les CGU de Twitter, puis Google. Le TGI exige désormais de la part de ces sociétés des termes moins vagues et des CGU plus contraignantes.

Le « Cybersecurity Act »

Les députés européens ont adopté le 12 mars 2019 un règlement «Cybersecurity Act», visant à renforcer la cybersécurité à l'échelle européenne par une harmonisation des certifications nationales en matière de sécurité des TIC. Un prestataire souhaitant exporter ses services dans plusieurs États de l'Union européenne ne serait donc plus soumis qu'à une certification unique. Trois niveaux de certification sont prévus. Le règlement doit encore être approuvé par le Conseil européen.

Hébergeur de site et gestion des données

Par un arrêt du 1er mars 2019, la Cour d'appel de Paris a rappelé que l'hébergeur d'un site internet n'est pas responsable du traitement des données à caractère personnel présentes sur le site et qu'il ne lui incombe pas d'effectuer les démarches de mise en conformité, telles que les formalités auprès de la Cnil, le recueil de consentement ou l'information de l'internaute. L'hébergeur ne peut donc être poursuivi pour faire cesser le trouble manifestement illicite allégué.