https://www.observatoire-collectivites.org/spip.php?article9868

Mots de passe faibles, sécurité négligée : qui est responsable en cas de piratage ?

- Jurisprudence -

Publication date: vendredi 29 mai 2026

Piratage d’un système téléphonique communal : la responsabilité des prestataires peut-elle être engagée, y compris après la fin du contrat ?

Oui. Même après la fin de son contrat, un prestataire peut voir sa responsabilité engagée si ses manquements antérieurs (notamment en matière de sécurité et de conseil) ont directement contribué à la survenance du dommage. Le juge administratif retient ainsi la responsabilité contractuelle de plusieurs intervenants lorsque leurs fautes respectives ont concouru à maintenir un système vulnérable. L’absence d’audit, de sécurisation et de conseil constitue ici des manquements déterminants. Les prestataires successifs sont condamnés à indemniser la collectivité victime d'un piratage.

Une commune avait confié la maintenance de son système téléphonique (PABX) à un premier prestataire jusqu’à la fin de février 2015, avant de conclure un nouveau contrat d’entretien avec une autre société à compter de mars 2015. Quelques semaines plus tard, le système fait l’objet d’un piratage d’une ampleur significative, générant des communications frauduleuses et des coûts importants.

À la suite d’une expertise judiciaire, la collectivité engage la responsabilité contractuelle des deux prestataires.

La première société (ancien titulaire du marché) fait valoir que son contrat avait pris fin avant la survenance du piratage et qu’aucun incident n’était survenu durant son intervention. Elle conteste donc tout lien de causalité.

La seconde société (nouveau titulaire du marché), en liquidation judiciaire au moment du litige, contestait également sa responsabilité en soutenant notamment qu’elle n’était intervenue que sur une période très courte et que la preuve de ses manquements n’était pas rapportée.

Le tribunal écarte ces arguments et retient la responsabilité des deux sociétés.

D’une part, le premier prestataire a manqué à son devoir de conseil et de sécurité. L’expertise met en évidence une gestion défaillante des mots de passe du système (mots de passe faibles, absence de renouvellement), ainsi que l’absence de préconisations en matière de sécurisation. Ces manquements ont laissé persister une vulnérabilité structurelle du système. Le juge en déduit l’existence d’un lien de causalité direct entre ces carences et la possibilité du piratage, peu important que celui-ci se soit produit après la fin du contrat :

Il résulte de l’instruction, et notamment des conclusions de l’expert judiciaire, que la société S... a fait preuve d’un manque de vigilance caractérisé en ne prêtant pas attention à la sécurité des mots de passe, ceux-ci, composés uniquement de quatre chiffres, étant aisés à pirater. Elle n’avait par ailleurs pas procédé au changement des mots de passe, ce qui constitue « une pratique extrêmement dangereuse en ce qui concerne la sécurité du PABX », ces mots de passe facilement piratables étant toujours selon l’expert une source de vulnérabilité ayant rendu le piratage « facile et possible ». La société S... n’a également pas été en mesure d’apporter la preuve qu’elle avait conseillé à la commune d’Antony de commander une prestation de mise en sécurité du PABX, de sorte que l’entreprise a manqué à son devoir de conseil envers l’administration. L’expert conclut en affirmant qu’il existe « un lien de causalité directe et certain entre le défaut de conseil de la société S... et l’état vulnérable du PABX qui a rendu le piratage possible ». Si la société S... fait valoir en défense qu’elle n’était plus titulaire du contrat de maintenance depuis le 28 février 2015 et qu’elle ne peut être tenue responsable d’un piratage survenu au cours du mois de mai 2015, il n’en demeure pas moins qu’elle est directement à l’origine de faits ayant rendu ce piratage possible, du fait notamment de l’absence de sécurisation des mots de passe, de sorte que sa responsabilité est engagée à raison d’une faute caractérisée, quand

bien même ce piratage a eu lieu à une date où elle n'était effectivement plus titulaire du contrat de maintenance.

Si la faiblesse des mots de passe a permis, en l'espèce, à la collectivité d'engager la responsabilité de ses prestataires, elle pourrait, dans d'autres configurations, être analysée comme une négligence imputable à la collectivité elle-même.
Ainsi, en février 2021, une cyberattaque survenue en Floride (États-Unis) a conduit à la manipulation de la composition chimique de l'eau distribuée. Le pirate est parvenu à augmenter de manière significative le taux de soude caustique, multipliant par dix sa concentration. Les conséquences auraient pu être particulièrement graves en l'absence de réaction rapide des agents de la station de traitement.
Or, cette attaque reposait sur des failles élémentaires plutôt que sur des procédés sophistiqués. L'enquête a mis en évidence plusieurs défaillances majeures :
– l'utilisation d'un mot de passe unique et partagé sur l'ensemble des postes ;
– l'absence de pare-feu entre Internet et le système d'information ;
– le maintien d'un système d'exploitation obsolète (Windows 7), dont les mises à jour de sécurité avaient cessé depuis janvier 2020, en dépit des alertes des autorités.
Transposée au contexte français, une telle accumulation de manquements pourrait caractériser une faute de la collectivité en cas de dommage, notamment si celle-ci n'a pas pris les mesures élémentaires de sécurisation pourtant connues et recommandées. Une action en responsabilité pourrait alors être engagée contre la collectivité, voire, dans certaines hypothèses, conduire à rechercher la responsabilité personnelle des décideurs (élus et/ou responsables des systèmes d'information) en cas de carence manifeste face à un risque prévisible.

D'autre part, le second prestataire a également manqué à ses obligations. Il n'a pas réalisé d'audit initial du système, pourtant indispensable compte tenu de la reprise des installations, ni formulé de recommandations de sécurité adéquates. En outre, il n'a pas transmis à la collectivité un rapport d'audit mettant en évidence de nombreuses vulnérabilités et n'a pas efficacement mis fin à l'attaque. Ces défaillances caractérisent également un manquement au devoir de conseil et de diligence.

Le tribunal retient ainsi que les fautes respectives des deux sociétés ont concouru à la réalisation du dommage et engage leur responsabilité solidaire.

Cybersécurité : une formation en ligne proposée pour préparer les élus et leurs agents aux crises cyber

Face à la montée en puissance des cybermenaces, les communes et intercommunalités se retrouvent en première ligne. En 2025, 293 revendications d'attaques cybercriminelles ciblant des collectivités territoriales ont été recensées. Les conséquences peuvent être lourdes : interruption des services publics, captations de données sensibles ou encore pertes financières significatives.

C'est dans ce contexte préoccupant que l'AMF et le Commandement du ministère de l'Intérieur dans le cyberespace ont lancé « CapCyber : crises & collectivités », un exercice de simulation en ligne innovant pour accompagner les élus locaux et leurs agents dans la prévention et la gestion du risque cyber. Conçu pour anticiper les crises avant qu'elles ne surviennent, ce programme propose une immersion pédagogique dans une situation de cyberattaque simulée, afin de mieux comprendre les enjeux et adopter les bons réflexes.

Sur le plan indemnitaire, le juge opère une appréciation stricte des chefs de préjudice :
certains postes sont écartés (notamment les frais d'avocat déjà couverts par les règles propres aux frais de justice), d'autres sont admis comme directement liés au dommage (frais d'assistance technique lors de l'expertise, surcroît de

travail d’un agent). Les sociétés sont ainsi condamnées à indemniser partiellement la collectivité, ainsi qu’à supporter solidairement les frais d’expertise.

Tribunal Administratif de Cergy-Pontoise, 19 février 2026, NÂ° 2214074