INCENDIES À RÉPÉTITION CHEZ OVH : LES PREMIÈRES ACTIONS À MENER PAR LES ENTREPRISES IMPACTÉES

Le 19 mars dernier, un nouvel incendie s'est déclaré au sein du datacenter de Strasbourg du géant informatique français OVH. Le 10 mars 2021, une semaine auparavant, un violent incendie avait déjà détruit une partie des serveurs de ce même datacenter affectant les sites et les données de « *12 à 16 000 clients* ».

Dans ce contexte, quelles sont les conséquences de cet incendie pour les sociétés impactées ? Quelles actions doivent-elles mettre en place de toute urgence ?

En tout premier lieu, elles doivent impérativement **consulter les contrats qu'elles ont conclu soit directement avec OVH soit avec un sous-traitant prestataire d'hébergement pour le compte de leurs clients**. Sachant que des options pouvaient être souscrites, celles qui directement ou par l'intermédiaire d'un prestataire avaient souscrit un hébergement avec sauvegarde auprès d'OVH sont logiquement censées être plus à l'abri que celles ayant écarté une telle option.

Il semblerait toutefois que certains clients ayant souscrit en direct ou par l'intermédiaire de leur prestataire l'option de sauvegarde aient néanmoins perdu tout ou partie de leurs données, les serveurs incluant l'offre de sauvegarde et ceux ne l'incluant pas se trouvant dans les mêmes salles ou à proximité.

Bien entendu, les clients ayant souscrit l'option de sauvegarde auprès d'OVH disposent d'une action en responsabilité à l'encontre de l'hébergeur. Il leur sera plus facile de démontrer les manquements d'OVH dans cette hypothèse.

Pour les clients ayant souscrit un hébergement simple (sans option de sauvegarde), la question se pose de l'étendue des obligations d'OVH et du caractère essentiel de la prestation de sauvegarde attachée à l'hébergement.

Bien sûr, OVH peut tenter d'opposer à ses clients l'article 7.7 de ses Conditions Générales de Service qui exclue sa responsabilité en cas d'incendie, ce dernier constituant un cas de force majeure.

Pourtant si l'incendie a déjà été retenu comme cas de force majeure (évènement imprévisible et irrésistible) par la jurisprudence, cette qualification n'est pas automatique. Dans le cas d'OVH, les juges pourraient considérer qu'un incendie dans un datacenter n'est pas imprévisible compte tenu de la concentration en un même lieu de nombreux serveurs, baies informatiques, fils électriques et branchements.

Ils pourraient également s'interroger pour savoir si toutes les mesures de sécurité nécessaires pour éviter l'incendie ont été prises.

Il est donc loin d'être certain que la responsabilité d'OVH puisse être écartée sur le fondement de la force majeure.

Les clients ayant souscrit les prestations d'hébergement auprès d'un sous-traitant vont, quant à eux, pouvoir se retourner contre ce dernier et l'appeler en garantie (celui-ci se chargeant ensuite de porter l'action à l'encontre d'OVH).

En tout état de cause, il est conseillé aux entreprises impactées de commencer à **calculer leur préjudice, de déclarer le sinistre à leur assurance et de faire le point sur leur contrat d'assurance** notamment quant à l'indemnisation de la perte de données et quant aux moyens mis en œuvre pour leur reconstitution.

Enfin, les sociétés impactées par l'incendie OVH doivent **penser aux actions à effectuer au regard du RGPD**. Le 22 mars dernier la CNIL a publié sur son site une page intitulée « *Incendie OVH : faut-il notifier à la CNIL ?* » afin de rappeler les obligations des entreprises impactées en matière de notification de violation en cas d'indisponibilité ou de destruction de données personnelles.

Les responsables de traitement qui hébergeaient des données personnelles au sein du datacenter sont tenus de documenter la violation dans un registre tenu en interne.

Selon la CNIL, une notification à cette dernière est nécessaire :

- Si des données personnelles ont été définitivement perdues ;
- Si elles sont restées indisponibles suffisamment longtemps, de telle sorte que cela a engendré un risque pour les personnes.

En conclusion, cette affaire rappelle l'importance pour les sociétés de lire attentivement les contrats informatiques souscrits, de vérifier en cas de sous-traitance la chaîne des obligations (contrats miroirs) avant de s'engager à fournir à leurs clients des prestations informatiques qu'elles ne maitrisent pas, et de vérifier les modalités des contrats d'assurance dont elles disposent notamment en matière de cyber risques (incluant spécifiquement la perte et la reconstitution de données).