FIDAL

INSUFFISANCE DES MESURES DE SECURITE DES DONNEES CLIENTS : BOUYGUES TELECOM CONDAMNE PAR LA CNIL

La société Bouygues Télécom a notamment pour activité d'éditer et de gérer son site web www.bouyguestelecom.fr et de mettre sur cette plateforme à disposition de ses clients un accès à leur espace personnel en vue d'éditer des documents administratifs liés à leur contrat.

En mars 2018, la CNIL est informée de l'existence d'une faille de sécurité sur son site web concernant plus de deux millions de personnes permettant d'accéder aux données à caractère personnel de ses clients au moyen d'adresses URL ayant une structure identique.
En effet, n'importe quel internaute pouvait en inscrivant l'adresse URL https://www.bouyguestelecom.fr/archived/index/printcontract/archived_id/X et en remplaçant « X » par différents nombres entiers, accéder aux données personnelles renseignées par les clients sur leur contrat de souscription (par exemple, leur nom, prénom, date de naissance, adresse de courrier électronique etc.).

Selon la société Bouygues Télécom, cette faille de sécurité avait pour origine la fusion des systèmes informatiques des sociétés Bouygues Télécom et B&You, à cette occasion, le code informatique rendant nécessaire l'authentification lors de l'accès au site web de Bouygues Télécom n'avait pas été réactivé.

La formation restreinte de la CNIL se prononce alors sur le manquement de Bouygues Télécom à son obligation d'assurer la sécurité et la confidentialité des données personnelles de ses clients en sa qualité de responsable de traitement.

En premier lieu, elle estime que Bouygues Télécom a fait le choix de ne pas mettre en place des mesures complémentaires à l'authentification de ses clients de son site web, ce choix a fait peser sur elle une obligation particulièrement renforcée de vigilance à l'égard de cette unique mesure de sécurité par authentification.

En second lieu, selon la formation restreinte, si une revue manuelle de l'ensemble des logins de codes informatique du site web aurait été disproportionnée au regard du nombre de lignes le composant, la revue manuelle du code uniquement sur sa partie relative au mécanisme d'authentification aurait, dans ce cas précis, été nécessaire.

De ce fait, la formation restreinte estime que le fait de ne pas avoir mis en œuvre, pendant plus de deux ans et trois mois, des mesures efficaces permettant de découvrir l'erreur humaine à l'origine de la faille de sécurité constitue une violation de l'obligation de sécurité à la charge de Bouygues Télécom au sens de l'article 34 de la loi Informatique et Libertés n°78-17 du 6 janvier 1978. En effet, Bouygues Télécom aurait dû prévoir, d'une part, des mesures de revue

automatisées du code informatique adaptées au système d'information tel qu'hérité suite à la fusion de Bouygues Télécom et B&You et, d'autre part, une revue manuelle de la partie du code portant sur l'authentification de ses clients.

Partant, la formation restreinte, au regard de la gravité du manquement caractérisé par le nombre de personnes concernées (plus de deux millions), des données personnelles y afférentes et de la durée de la faille de sécurité (plus de deux ans et trois mois), condamne Bouygues Télécom à une amende pécuniaire de 250 000 euros et décide de rendre publique sa décision.

Notons que cette décision est rendue pour des faits soumis dans leur intégralité à la législation applicable avant l'entrée en application du Règlement Général sur la Protection des Données (RGPD). Désormais, rappelons que le nouveau règlement européen porte le montant maximum des amendes pécuniaires pour un manquement à une telle obligation de sécurité des données par un responsable de traitement (ou par un sous-traitant) à 10 000 000 euros ou 2 % du chiffre d'affaires annuel mondial de l'entreprise, le montant le plus élevé étant retenu.