Phishing et négligence de la victime

Par un arrêt du 25 octobre 2017, la Cour de cassation sanctionne les juges du fond de ne pas avoir recherché si, compte-tenu des circonstances, la « victime » ne pouvait pas avoir conscience du caractère frauduleux de l'e-mail reçu et si le fait d'avoir communiqué les informations relatives à sa carte bancaire ne constituait pas une négligence grave, exonérant la banque de son obligation de remboursement. Il convient donc désormais d'être prudent au risque de devoir supporter les débits liés à une opération de paiement réalisée à la suite d'une pratique de phishing.

Sanction de la Cnil pour atteinte à la sécurité des données

Le 16 novembre 2017, la Cnil a prononcé une sanction d'un montant de 25 000 € à l'encontre de la société Web Éditions pour manquement à son obligation d'assurer la sécurité et la confidentialité des données de ses clients sur quatre sites internet de démarches administratives. Elle a en effet constaté qu'une fois le formulaire en ligne renseigné, la simple modification d'un numéro dans l'adresse URL de la page récapitulative permettait d'accéder aux pages d'autres utilisateurs des différents sites.

Licenciement et utilisation du matériel de l'entreprise

Par un arrêt du 25 octobre 2017, la Cour de cassation confirme la décision des juges du fond jugeant que l'utilisation parfois abusive de la carte de télépéage mise à la disposition d'un(e) salarié(e) et le téléchargement sur l'ordinateur portable de fichiers personnels volumineux n'étaient pas constitutifs d'une faute grave et que le licenciement était sans cause réelle et sérieuse.

Comment se mettre rapidement en conformité avec le RGPD ?

LES FAITS

Le Règlement européen général sur la Protection des données (RGPD) auquel toutes les entreprises, peu importe leur taille, privées ou publiques, devront se conformer s'appliquera dès le 25 mai 2018. Ce règlement qui pose un nouveau cadre et renforce les droits des personnes objets de traitements de données impose un grand nombre de chantiers, techniques et organisationnels. Tour d'horizon des 5 grandes étapes à mettre en place dans les 5 prochains mois.

NOMMER UN DATA PROTECTION OFFICER (DPO)

Obligatoire pour les organismes privés, dès lors que les entreprises opèrent des traitements à grande échelle de suivi régulier et systématique des personnes ou de données sensibles (religion, condamnations, santé, etc.) et dans le secteur public, à l'exception des juridictions, quelle que soit la nature du traitement. Il sera le coordinateur de la conformité des dispositifs internes au RGPD. Alliant des compétences juridiques et techniques, rattaché directement à la direction générale, il délivrera en toute indépendance des recommandations sur toutes les problématiques liées à la protection des données à caractère personnel. Les entreprises qui ont déjà nommé un Correspondant informatique et libertés pourront faire monter ce dernier en compétences, ou même externaliser cette fonction auprès de prestataires spécialisés (avocat par exemple).

CARTOGRAPHIER LES TRAITEMENTS DE DONNÉES

La deuxième étape consiste à passer en revue l'ensemble des traitements de données personnelles, informatisés ou non, et de les recenser dans un registre qui pourra être demandé à tout moment par la Cnil. Pour dresser cette cartographie, il convient notamment de lister pour chaque traitement : la finalité poursuivie, la nature des données traitées, leur localisation, les flux amont et aval (l'origine et la destination), les acteurs internes et externes qui traitent ces données, le temps de conservation, etc.

ÉTABLIR UN PLAN D'ACTIONS

Sur la base de ce registre, il s'agira d'identifier les actions à mener pour se conformer aux obligations actuelles et à venir, actions à privilégier au regard des risques que font peser les traitements sur les droits et les libertés des personnes concernées. Une fois les traitements à risque identifiés, il s'agira de les soumettre à une étude d'impact sur la vie privée (« *Privacy Impact Assessment* ») afin d'identifier les risques probables d'atteinte aux droits des personnes, leur gravité, et les mesures adoptées ou devant être adoptées pour sécuriser le traitement ou corriger les défauts constatés.

DR

Me Pierre-Randolph Dufau, avocat à la cour, fondateur de la SELAS PRD avocats.

POSER LE CADRE DE GOUVERNANCE INTERNE

Pour inscrire ce plan d'actions dans la durée, il conviendra de mettre en place des procédures internes visant à garantir l'intégrité de la donnée tout au long de sa vie, de la collecte à sa suppression (par exemple, organiser la gestion des failles de sécurité, des demandes de rectification, d'accès ou de modification des données collectées, changement de prestataire, etc.). Organiser les process implique également de prendre en compte la protection des données personnelles dès la conception d'une application ou d'un traitement (« *privacy by design* »).

DOCUMENTER LA CONFORMITÉ

En application du principe d'« *accountability* », on passe d'une logique déclarative (suppression des déclarations préalables auprès de la Cnil) à une logique de conformité. Ainsi, en cas de contrôle, l'entreprise devra être à même de démontrer qu'elle a mis en œuvre l'ensemble des mesures organisationnelles pour respecter le RGPD via la tenue d'une documentation complète, actualisée et exportable facilement.

CE QU'IL FAUT RETENIR

En cas de non-respect de cette réglementation, les sanctions sont lourdes, celles-ci pouvant aller jusqu'à 20 millions d'euros ou, pour les entreprises, à 4 % du chiffre d'affaires annuel mondial.