La Tribune de l'assurance

Date : 07/05/2020
Heure : 08:00:42
Journaliste : Nessim Ben Gharbia

www.tribune-assurance.fr
Pays : France
Dynamisme : 3

Visualiser l'article

« Fuites et détournements de données se multiplient »

Mélanie Erber, avocate associée, **Coblence avocats**

Comment les entreprises peuvent-elles se mettre en conformité avec le RGPD et quelles sont les repsonsabilités en cas de fuite de données ? Eléments de réponse avec Maître Mélanie Erber.

L'assurance garantit-elle une fuite de données personnelles ?
Cela dépend des assurances RC souscrites par les responsables de traitements. Compte tenu de l'accroissement de ces fuites, des compagnies proposent des assurances spécifiques aux risques liés à la cybercriminalité (et notamment aux fuites et/ou aux détournements de données personnelles). Ces polices d'assurance prennent en charge les frais d'avocats, les frais engendrés par la notification à la Cnil et aux personnes concernées et éventuellement les réparations qui seraient allouées aux personnes ayant subi la violation des données. Si une personne physique demande réparation au titre de préjudice de la fuite des données, cela peut être pris en charge.
Les victimes peuvent également engager la responsabilité civile du responsable de traitement au sens de l'article 1240 du Code civil pour obtenir réparation du préjudice moral subi, sous réserve d'en justifier. Le préjudice moral peut résulter de la divulgation d'informations sur les revenus, de données de santé ou de données relatives à la situation familiale. S'agissant des données bancaires, aujourd'hui quand un client bancaire est piraté, la plupart des contrats d'assurance cartes bleues prennent en charge ces risques et procèdent au remboursement, avec des délais et des formes spécifiques.

Qui peut être tenu responsable dans la fuite massive des données personnelles et bancaires de quelque 130 000 clients détenues par une filiale d'AccorHotels ?
Dans cette affaire, le responsable de traitement est Accor ou une de ses filiales. C'est donc sur elle que pèse la responsabilité de la fuite. Cependant, il y a aussi la responsabilité potentielle des sous-traitants d'Accor (en l'espèce Zelko). De ce fait, si la Cnil sanctionne Accor, il est fort probable que l'hôtelier recherchera

la responsabilité de son sous-traitant qui se devait de respecter ses obligations contractuelles relatives aux données personnelles qui lui étaient transmises par Accor. C'est justement afin de pouvoir engager la responsabilité contractuelle des sous-traitants que nous conseillons toujours aux entreprises de veiller à la rédaction de leurs contrats avec les sous-traitants auxquels elles donnent accès aux données personnelles de leurs clients. S'agissant des sanctions, elles sont plafonnées par la Cnil à 10 M€, ou 2 % du chiffre d'affaires annuel mondial de l'entreprise concernée étant précisé que la Cnil retient le montant le plus élevé.

Que prévoit la réglementation concernant la protection des données personnelles en cas de fuite ?
Le responsable de traitement des données personnelles a plusieurs obligations. Dans un document récapitulatif, il doit déterminer la nature de la violation, le nombre approximatif des personnes dont les données ont été violées et les conséquences probables de la violation des données. Par ailleurs, il doit énumérer les mesures qu'il a prises ou qu'il a l'intention de prendre pour atténuer les conséquences d'une telle faille et éviter que la violation des données ne se reproduise. La deuxième chose à faire, s'il y a un risque pour les personnes dont les données ont été violées, c'est de notifier la violation à la Cnil (article 33 du RGPD) soixante-douze heures après en avoir pris connaissance (article 33 RGPD). Enfin, s'il considère que le risque est élevé pour la vie privée des personnes concernées, il doit immédiatement les informer de la fuite.
En tout état de cause, la procédure devant la Cnil n'empêche pas une action pénale en parallèle (saisie du procureur de la République).

Les entreprises sont-elles désormais en conformité avec le RGPD ?
Au sein de notre cabinet, nous accompagnons les clients en amont pour les aider à se mettre en conformité. Nous avons constaté que 75 % des effectifs des sociétés n'ont pas conscience de ce qu'est une fuite de données. En conséquence et dans la mesure où le périmètre d'une fuite de données est très vaste, nous recommandons, en plus de la mise en place des outils préconisés par le RGPD, de former les salariés en interne afin de les sensibiliser et qu'ils aient conscience, par exemple, que quand ils perdent leur téléphone ou leur ordinateur portable, cela peut donner lieu à une fuite de données. Le respect des exigences du RGPD est d'autant plus important pour les pure players s'adressant essentiellement à des consommateurs.