Protection des données personnelles : la conformité à la loi ne suffit plus !SOLUCOMINSIGHT

Raphaël Brun | Consultant senior

Protection des données personnelles : la conformité à la loi ne suffit plus !

[Article rédigé en collaboration avec **Ahmed Sanhaji**, **consultant**]

Toutes les organisations sont aujourd'hui susceptibles d'être concernées pas des failles, voire des attaques, liées aux données à caractère personnel qu'elles manipulent. Les multiples exemples relayés ces dernières années par les médias l'illustrent : condamnation de la CNIL, failles révélées dans le SI, plaintes d'utilisateurs,... Même si une application scrupuleuse de la loi participe à la diminution du risque, elle ne peut garantir l'absence d'incident.

De ce fait, **les organisations manipulant des données personnelles ne doivent plus se demander si ce type d'incident pourrait arriver, mais plutôt quand il va survenir et quels en seront les impacts**.

La crise « données personnelles » doit être anticipée et préparée

Le récent « bug Facebook » l'illustre bien, les impacts seront d'autant plus importants aujourd'hui que le grand public est attentif à ces problématiques.

Pour rappel, lors de l'activation de la nouvelle page Timeline, certains utilisateurs se sont plaints de la publication de messages privés sur leur mur. Une faille a d'abord été soupçonnée.. Après enquête de la CNIL, il s'agit d'anciennes publications de mur à mur quela Timelinea fait ressortir. Quelle que soit la cause, la réaction démesurée des utilisateurs à la possible publication non maîtrisée de données qu'ils considèrent comme privées montre bien la sensibilité quasi-épidermique du public sur le sujet.

Les multiples prises de position des utilisateurs, de la presse, ainsi que de la classe politique illustrent à quel point cette problématique est devenue médiatique. La ministre déléguée à l'économie numérique, Fleur Pellerin, a conseillé hâtivement de porter plainte si la faille était avérée. De son côtéla CNIL, considérant que la confusion des utilisateurs est sans doute liée aux changements unilatéraux et récurrents des paramètres de vie privée en 2009 et2010, ademandé à Facebook de lui transmettre les mesures que l'entreprise américaine comptait mettre en œuvre afin de respecter ses recommandations.

Facebook s'est bien entendu défendu de toute « atteinte à la vie privée », expliquant avant la CNIL l'origine de la confusion. La rapidité de la prise de parole n'a cependant pas empêché que l'image du site et la confiance de certains utilisateurs ne soient écornées.

Cet exemple a permis de mettre en lumière que **l'incident de confidentialité (fuite, mauvais traitements) de données personnelles est devenu un type de crise à traiter par les organisations**. Elles doivent dès lors amender leurs dispositifs de gestion de crise afin d'y intégrer les dispositions propres à ce type de sujet (processus de détection et de qualification spécifique, experts juridique mobi-

Protection des données personnelles : la conformité à la loi ne suffit plus !SOLUCOMINSIGHT

lisables, …). En particulier, au regard de la nouvelle, et forte sensibilité du public, **une attention toute particulière devra être portée à la maitrise de la communication de crise**. Le « bug Facebook » l'a montré, la crise peut davantage être liée à la communication autour de l'évènement que de la faille en elle-même.

Il reviendra alors au Correspondant Informatique et Libertés de mobiliser les différents acteurs concernés (responsable du processus de crise, département relation client, service juridique, experts sécurité) au sein de groupes de travail afin de définir les processus et dispositifs à mettre en place le jour « J » (moyens d'alertes, plan de communication, …).

Le projet de règlement européen relatif] à la protection des données personnelles rendra d'ailleurs ces aspects d'autant plus essentiels, l'obligation de notification de toute fuite de données personnelles devant se traiter au sein d'un dispositif ad-hoc impliquant l'entreprise mais aussi des acteurs externes, afin d'éviter que la crise prenne une ampleur préjudiciable pour les personnes concernées et l'entreprise.

Seule une analyse de risques permettra d'anticiper au mieux la crise

Pour anticiper et traiter au mieux ces crises, l'organisme devra se poser la question des risques afférents à la manipulation des données personnelles, et construire des plans d'actions proportionnels aux impacts anticipés.

Cette démarche, en ligne avec les exigences de la loi informatique et libertés (cf. article 34 : *Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et* des risques présentés par le traitement) et certainement du futur règlement européen, pourra être menée à l'aide des méthodes classiques d'analyse de risques bien connues des Responsable dela Sécurité des SI (les guides « Gérer les risques » et « Mesures pour traiter les risques » publiés parla CNIL pourront également être utilisés).

L'enjeu vis-à-vis de ces données personnelles ne sera donc plus uniquement de se conformer aux exigences de la loi mais bien **d'identifier les risques potentiels et les crises probables**. Il reviendra alors à l'organisme de traiter en priorité les traitements comportant le plus de risques, notamment ceux pouvant la mettre en péril en cas de fuite de données personnelles.