Données personnelles

Moins de trois mois pour se préparer au tsunami UE

L'entrée en vigueur du Règlement européen sur la protection des données personnelles est prévu pour ce 25 mai 2018. Moins de trois mois nous séparent de cette échéance qui suscite l'inquiétude des opérateurs. Particulièrement ceux de l'offshoring. L'autorité chargée de la protection de la vie privée (CNDP) joue à l'éclaireur en mettant en ligne un guide à disposition de ses usagers (voir page 5 et www.cndp.ma). «C'est un texte complexe qui nécessite un apprentissage qui prend un peu de temps, notamment au niveau de ses nouveaux outils. Donc, c'est un investissement», reconnaît la présidente de la Commission nationale de l'informatique et des Libertés (Cnil), Isabelle Falque-Pierrotin fin février 2018 à Casablanca.

Le nouveau règlement sur la protection des données privées a été adopté le 27 avril 2016 par le Parlement et le Conseil européens (Ph. Faquihi)

■ Une réglementation applicable hors frontières

Le Règlement européen n°2016/679 a un caractère extraterritorial. C'est à dire qu'il s'applique aussi bien dans l'Union qu'à l'étranger. Le législateur a retenu deux critères pour son application. Le premier est dit «d'établissement». Il induit que le traitement des données «est effectué dans le cadre d'activités» d'opérateurs établis sur le sol de l'UE. Peu importe que ce traitement «ait lieu ou pas» dans un Etat-membre. Seule compte l'origine de la donnée et le lien physique qu'elle a avec un citoyen européen: patronyme, coordonnées, groupe sanguin, numéro de compte bancaire... D'où la raison d'être du second critère, dit de «ciblage». Bruxelles cible tout opérateur «dès lors qu'il traite des données» de ses citoyens. Que ce traitement consiste à proposer des offres de biens et services ou à pister «les comportements» d'une personne.

■ Qu'est-ce qui change pour les sous-traitants?

«Il faut des garanties techniques et organisationnelles suffisantes pour traiter les données transférées depuis l'Union européenne», précise la Commission nationale pour le contrôle de la protection des donnés à caractère personnel (CNDP). Le traitement assuré par un sous-traitant du sud doit être conforme aux pratiques

➡➡➡

Moins de trois mois pour se préparer au tsunami UE

en vigueur au nord de la Méditerranée. Une activité où le sous-traitant ne peut faire appel à un autre prestataire qu'après autorisation du responsable de traitement. Entendez la société européenne. Et qui demeure juridiquement la première responsable en cas d'abus. Le Règlement de l'UE induit donc une responsabilité civile en cascade: donneur d'ordre, sous-traitant, prestataires connexes...

C'est pourquoi il faut bien lire le contrat qui «définit les caractéristiques du traitement», conseille la CNDP. Reste à savoir si dans les faits, un sous-traitant africain a vraiment le choix de négocier sur l'étendue de sa responsabilité.

■ Un registre et un délégué à la protection des données

La loi veut aussi qu'un opérateur dispose de son registre de traitement. C'est là où devront êtres consignés les plus petits détails relatifs au traitement des données: identité du responsable du traitement, types des données, nature du traitement, incidents... Une entreprise, y compris sous-traitante, doit notifier les violations des données personnelles dans les meilleurs délais à ses clients: donneur d'ordre, personne... Le vol des données et l'intrusion au système d'information sont des cas types.

Le délégué à la protection des données est une sorte d'officier chargé de veiller sur la bonne application des règles et de la procédure. Il peut être informaticien, juriste ou administrateur. L'essentiel pour une entreprise est d'agir en équipe dans ce chantier. Avec un comité qui se réunit régulièrement avec le top management pour mettre à plat les difficultés notamment. Le délégué à la protection est un ambassadeur aussi. C'est lui le porte-parole de l'entreprise en matière de traitement. Le correspondant aussi avec l'autorité de contrôle.

■ Une sanction qui peut atteindre 223 millions de DH

«Les anciennes sanctions de la directive 95/46 changeaient d'un Etat européen à un autre. L'amende était plafonnée en cas de récidive à 300.000 euros chez notre premier partenaire commercial, la France», précise, en septembre 2017, Mounim Zaghloul, DG du cabinet de conseil Consilium. Le nouveau règlement «a unifié et alourdi» les sanctions pécuniaires qui peuvent aller jusqu'à 20 millions d'euros (un peu plus de 223 millions de DH) ou 4% du chiffre d'affaires mondial de l'entreprise contrevenante. Ce dispositif répressif peut être décidé en complément ou à la place d'autres sanctions. On peut citer à titre d'exemple la suspension de flux de données vers un pays tiers comme le Maroc. L'autorité de contrôle peut décider aussi d'effacer des données ou encore d'en limiter le traitement.

■ Les six règles à suivre pour se préparer

La CNDP préconise plusieurs démarches pour se préparer à la mise en conformité. L'entreprise doit d'abord constituer un comité de pilotage. Puis faire un inventaire des traitements de données personnelles. Ce data mapping va déterminer le type des données traitées, les chantiers à entamer, leur ampleur et un agenda. Ensuite, le management identifie les actions prioritaires. Ce qui suppose aussi de «manager le risque» de gestion avec son volet juridique. Il faut aussi être pointilleux sur l'organisation de la mise en conformité en instaurant un processus interne de réalisation des objectifs. Finalement, l'entreprise doit «actualiser ses documents» conformément aux nouvelles règles. ❑

Faiçal FAQUIHI

Les bienfaits d'un «impérialisme juridique»

CE nouveau Règlement peut être perçu comme une forme d'impérialisme juridique. Et qui, reconnaissons-le, a ses bienfaits y compris pour la vie privée des non-européens.

Des Etats africains, comme la Tunisie et le Maroc, devraient aligner leurs lois aux standards de protection de leur premier partenaire commercial. L'Afrique francophone, qui compte aussi le Sénégal, en est convaincue. La révision de leurs législations n'est qu'une question de temps. Rabat, Tunis et Dakar font la course. Le premier arrivé des sous-traitants sera le plus avantagé pour garder ses marchés et capter d'autres investissements étrangers.

Outre les droits traditionnels (information, accès aux données personnelles, rectification, opposition, restriction du profilage automatisé...), le règlement adopté en 2016 a introduit de nouveaux droits pour les personnes. Figure d'abord le renforcement des conditions applicables au consentement, notamment celui des enfants, et le droit à l'oubli (cf. L'Economiste n°5102 du 8 septembre 2017).❑

Des outils pour consolider la conformité de l'entreprise

• Règles internes, clauses types, code de conduite et certifications

• Un business face à l'obligation d'une protection adéquate

• Une aubaine pour les conseils en compliance

LE transfert de données d'un pays à un autre obéit à une procédure stricte. Un opérateur doit obtenir le feu vert du régulateur de son pays avant toute opération. De 2011 à 2016, la Commission nationale pour le contrôle de la protection des données à caractère personnel (CNDP) a autorisé 388 transferts vers l'Europe en majorité (voir illustration). Le pays destinataire doit donc assurer «une protection suffisante et conforme à la loi 09-08 relative à la protection des données». Toute une procédure qui est importée de... l'Union européenne.

Sauf que le droit des 28 Etats-membres change de règles à partir de ce 25 mai 2018. Celles-ci seront applicables aussi bien sur le sol de l'UE qu'aux entreprises qui manipulent les données de ses citoyens (voir page 3). D'où l'intérêt économique de se mettre en adéquation avec la norme européenne. C'est un exemple type de «convergence réglementaire». En matière de données personnelles, il est question de «procédure d'adéquation». Elle induit que le transfert transfrontalier est possible vers le pays destinataire. Car son Etat dispose d'une législation qui assure une protection conforme aux standards exigés par Bruxelles.

La présidente de la Commission nationale de l'informatique et des Libertés (Cnil), Isabelle Falque-Pierrotin, est rassurante vis-à-vis du nouveau Règlement européen. «Nous avons accompagné les opérateurs durant la période précédant son entrée en vigueur et continuerons à le faire. Ce n'est pas le couperet et la guillotine pour les acteurs qui ne seront pas prêts», confiait, fin février à Casablanca, la présidente de la Cnil (cf. L'Economiste n°5217 du 26 février 2017).

Une société qui sous-traite les données d'un client basé à l'UE a d'autres moyens pour consolider ses standards en matière de protection de données personnelles. Il y a par exemple les règles internes de l'entreprise ou Binding Corporate Rules (BCR). Notons aussi l'existence des clauses contractuelles types approuvées par la Commission européenne. Sans oublier les codes de conduite et mécanisme de certification qui font le bonheur des conseils en compliance. «Le Règlement européen a engendré un gros marché en Amérique du Nord, particulièrement aux USA. Les avocats notamment en font leur miel. Il faut espérer que le même effet se produit au Maroc», déclare le secrétaire général de la CNDP, Lahousseine Anis.❑

F.F.

La France premier destinataire des transferts

Base légale des transferts autorisés	2015		2016		Cumul 2011-2016	
Transferts effectués vers des pays ayant une protection suffisante	98	85,96%	42	82,35%	351	90,46%
Transferts effectués sur la base du consentement des personnes concernées	15	13,16%	8	15,69%	33	7,42
Transferts effectués sur la base des clauses contractuelles ou BCR	1	0,88%	1	1,96%	4	0,89
Total	114		51		388	

Source: CNDP

Entre 2011 et 2016, ce sont 388 transferts de données personnelles qui ont été autorisés à partir du Maroc. Ils s'effectuent principalement vers l'Europe (79,3%) suivie de l'Amérique du Nord avec un peu plus de 13%, surtout aux USA. Ces transferts transfrontaliers sont effectués sur autorisation préalable de l'autorité de contrôle (CNDP)