ACTUALITÉS

Un changement de paradigme

Entretien avec Édouard Geffray Secrétaire général de la CNIL.

Semaine sociale Lamy : Quels sont les grands changements portés par le règlement ?

Édouard Geffray : Premier grand changement : le droit sera désormais le même pour tous, dans tous les États membres de l'Union européenne. La réforme est en effet portée par un règlement, ce qui signifie que le texte est d'application directe dans l'ordre juridique des États membres de l'UE, sans transposition nationale contrairement à la directive du 24 octobre 1995. C'est donc un instrument d'harmonisation extrêmement puissant. Par exemple, aujourd'hui, la durée de conservation des données fait l'objet d'exigences nationales différentes. Autre exemple, pour engager une procédure répressive, il existe des procédures nationales spécifiques. Certaines reposent sur le juge (la Belgique), d'autres nécessitent qu'il y ait une atteinte ou un risque d'atteinte élevé aux droits fondamentaux des personnes (l'Angleterre), ou encore un manquement à la loi Informatique et Libertés (la France). Demain, c'est un manquement au règlement qui pourra justifier une sanction administrative, comme c'est déjà le cas en France.

Le champ d'application évolue également. La directive de 1995 s'appliquait aux entreprises ayant un établissement ou des moyens de collecte de données en Europe. Le règlement européen ajoute à ces deux critères celui du « ciblage ». Concrètement, dès lors qu'un citoyen européen sera « ciblé » par un système de traitement de données à caractère personnel, le règlement européen s'appliquera. C'est donc un changement de paradigme : le champ d'application du droit n'est plus seulement construit autour de l'entreprise. Il combine ce critère à celui du citoyen. Par conséquent, une entreprise installée en dehors de l'UE et n'y disposant pas de moyens de traitement des données, qui crée un site Internet dédié aux ressortissants européens (ex. : langue, monnaie de paiement), devra respecter le règlement européen lorsqu'elle traitera leurs données personnelles.

Quel est l'impact du règlement européen sur les droits des citoyens ?

É. G. : Les droits des personnes sont globalement renforcés, notamment le consentement. Ce dernier est érigé en « clé de voûte », ce qui peut avoir des conséquences particulières en matière de droit du travail lié à la relation de subordination juridique. De plus, les personnes ont des droits nouveaux. Le droit d'accès déjà existant, permettant à un particulier de connaître les données détenues par une entreprise, est complété par un droit à la portabilité, c'est-à-dire le droit de récupérer ces données sous un format lisible et réutilisable et de les transférer à un tiers.

Et pour les entreprises ?

É. G. : C'est sans doute là que le changement est le plus important. On passe d'une logique de conformité à l'instant T de l'entreprise à une logique dynamique consistant à se demander si la protection maximale des données est assurée en continu, compte tenu des évolutions technologiques. L'idée étant de responsabiliser l'entreprise. Conséquence : les déclarations préalables à la CNIL disparaîtront à compter de mai 2018, même si un système de demande d'avis ou d'autorisation subsistera dans certains cas, et notamment pour les traitements de données sensibles.
Autre grand changement, par l'effet combiné de la loi Informatique et Libertés et de la directive de 1995, l'essentiel de la responsabilité est aujourd'hui supporté par le responsable de traitement. La loi s'applique peu aux sous-traitants qui pèsent parfois davantage que les entreprises responsables de traitement, notamment s'il s'agit de TPE/PME. Grâce au règlement européen, les obligations seront harmonisées et la responsabilité pourra être conjointe. L'ensemble de la chaîne pourra être saisi, quel que soit le type de traitement, et attrait dans la procédure de conformité ou de sanction.

Comment cette nouvelle logique de responsabilisation va-t-elle modifier les démarches de mise en conformité des entreprises ?

É. G. : Pour les traitements les plus sensibles, l'entreprise devra effectuer des études d'impact sur la vie privée (Privacy Impact Assessment) préalablement à la mise en œuvre des traitements et prendre les mesures nécessaires pour protéger les données personnelles des salariés. Cette étude sera soumise à la CNIL qui pourra, le cas échéant, s'opposer au traitement. Pour le reste des traitements, nous serons dans une logique d'accountability (détection des responsabilités) ou de compliance (mise en conformité). Les entreprises devront internaliser le contrôle et vérifier, en temps réel, qu'elles assurent une protection optimale des données. L'entreprise ne pourra plus se réfugier derrière la déclaration faite à la CNIL, qui ne vaut d'ores et déjà pas certificat de conformité mais qui est parfois vécue comme telle.

Que devient le CIL ?

É. G. : La désignation d'un correspondant Informatique et Libertés (CIL), aujourd'hui facultative, devient obligatoire dans de nombreux cas. Tous les organismes publics (collectivités locales, État, établissements publics, etc.) devront s'en doter ainsi que toutes les entreprises traitant de données à caractère personnel de manière régulière, assurant un suivi régulier de leurs clients ou ayant recours au profilage. Sont soumises à cette obligation les entreprises dont l'activité de base implique le traitement de données sensibles.
Le CIL change également de dénomination. Il reste l'acteur de la mise en conformité de l'entreprise mais s'appelera désormais délégué de la protection des données (DPO). La logique est la même, avec des compétences renforcées et une exigence nouvelle de qualification, cette dernière n'étant pas encore déterminée. Il a une obligation de documentation technique et juridique et doit tenir les documents à disposition de la CNIL dès lors que celle-ci souhaite effectuer un contrôle. Il est véritablement le « chef d'orchestre de la conformité » de son entreprise.

AUTEURS : Propos recueillis par Sabine Izard et Marine Corbères