Quels changements anticiper ? Le règlement européen sur les données personnelles annoncé pour le printemps :

	Quels changements anticiper Le règlement européen sur les données personnelles annoncé pour le printemps : ?

Ce règlement, dont le premier projet remonte à 2012, est appelé à remplacer la directive de 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ». Son objectif est d'uniformiser les règles en matière de protection des données personnelles en Europe, de garantir la libre circulation de ces données sur le territoire de l'Union et de simplifier l'exercice de leurs droits par les citoyens européens.

Après des débats parfois acharnés entre les acteurs en présence, que ce soit les CNIL européennes, les acteurs de l'internet et du Big-Data ou encore les représentants des consommateurs, une version consolidée a été arrêtée et diffusée le 15 décembre 2015.
De la loi du 6 janvier 1978 au futur règlement, la législation en matière de protection des données personnelles est allée dans le sens d'une complexité et d'une incertitude toujours plus grande. Les entreprises peuvent-elles attendre plus de sécurité juridique du futur règlement ? La réponse est contrastée.

Un projet de texte stabilisé… mais pas encore adopté
Il convient tout d'abord de tempérer l'enthousiasme affiché des institutions européennes : le texte définitif n'est pas encore adopté. Après un premier vote du Parlement européen en mars 2014, le Conseil de l'Union européenne donnait mandat au Luxembourg en juin 2015, dans le cadre de la présidence tournante de l'Union européenne, pour parvenir à un consensus sur le projet de règlement au plus tard fin décembre de la même année. Au terme de discussions intenses, Parlement et Conseil sont parvenus à un accord *in extremis* avant la trêve des confiseurs sur un document de pas moins de 200 pages…
Cet accord n'est pour le moment que politique, et la prochaine étape est un vote en deuxième lecture par le Parlement européen pour adoption définitive.
Le règlement européen sera ensuite applicable dans un délai de deux ans après son adoption. La différence essentielle par rapport à la directive de 1995 est que ce texte sera directement applicable au sein de l'Union européenne, sans que chacun des 27 états ne doive adopter des lois nationales de transposition, ce qui aurait nécessairement nui à l'objectif d'harmonisation. Les règles européennes nouvelles remplaceront donc automatiquement les règles nationales existantes incompatibles. Ainsi, pour ses 40 ans, la Loi française du 6 janvier 1978 dite « Informatique et Libertés » va se retrouver fortement vidée de sa substance.
Les entreprises ont donc encore un peu de temps devant elles pour se préparer à la mise en œuvre des nouvelles règles. Quels sont les changements majeurs à anticiper ?

***« Accountability »* et « *Privacy by Design* » sont des termes qui doivent devenir familiers**
Quelles données pourront être traitées ? Quelle durée de conservation appliquer ? Quels outils techniques installer ? Quelles formalités accomplir ?
Si le règlement uniformise la réponse à ses questions au sein de l'Union européenne… il ne les simplifie par nécessairement. Une large place sera faite à l'interprétation des dispositions nouvelles.

La **définition des données personnelles** ne change pas fondamentalement. Le règlement s'applique aux traitements des données identifiantes ou permettant d'identifier une personne, que ce soit directement ou indirectement. Le projet de règlement ajoute toutefois une série d'exemples de données qui permettent d'identifier une personne : son nom, mais également un numéro d'identification, une donnée de localisation, un identifiant d'un compte en ligne, ainsi que des références à des informations relatives à l'identité physique, génétique, mentale, économique, sociale ou culturelle d'une personne. Ces précisions sont dans la logique de la position actuelle des juridictions européennes et françaises.
S'agissant des **modalités de traitement** des données personnelles, il est abondamment fait référence dans le texte à la notion de *Privacy by Design*.
Qu'est-ce que cela signifie concrètement ? Les entreprises seront désormais tenues d'anticiper les sujets relatifs aux traitements de données dès les premières étapes de leurs projets informatiques, afin qu'il soit vérifié en amont que les développements à intervenir, où les logiciels à implémenter, seront conformes aux exigences imposées par le règlement.
Le responsable du traitement devra ainsi « *implémenter les mesures techniques et organisationnelles appropriées, telles que l'anonymisation, qui sont conçues pour mettre en œuvre les principes de protection des données, […] d'une manière effective et d'intégrer les protections nécessaires dans les traitements de manière à respecter les exigences du règlement et à protéger les droits des intéressés.* »
Une pondération devra en effet être faite entre coûts, état de l'art, contexte, finalités des traitements concernés, risques pour les droits et libertés des individus, etc. Autant de concepts dont la cohabitation laissera une grande place à une appréciation au cas par cas. Le règlement envisage qu'un mécanisme de certification soit mis en place, probablement afin de faciliter cette appréciation, bien que les procédures de certifications pèchent parfois par leur complexité.
Comme en l'état actuel de la législation, le règlement ne prévoit pas expressément de **durée de conservation des données**, et l'on peut le regretter. L'appréciation d'une durée de conservation des données sous une forme identifiante « *qui n'excède pas la durée nécessaire aux finalités pour lesquelles [les données] sont collectées et traitées* », place souvent le responsable de traitement dans une situation d'insécurité juridique. En revanche, dans sa dernière version, le projet de règlement prévoit que cette durée de conservation, ou *a minima* les critères retenus pour fixer cette durée, devront être portés à l'attention de la personne concernée dès la collecte. Les responsables de traitements devront donc apporter une attention particulière à ce sujet avant la mise en œuvre du traitement.
Les **formalités administratives** seront allégées : moins de notifications préalables aux autorités nationales, moins d'interlocuteurs. Un des objectifs principaux de ce texte est de garantir la libre circulation des données au sein de l'Union européenne. Ainsi, pour les groupes ayant des établissements dans plusieurs pays d'Europe, ou une activité ciblant plusieurs Etats-Membres, le principe du « guichet unique » permettra que les formalités requises ne soient effectuées qu'auprès de l'autorité de l'Etat Membre dans lequel le groupe a son établissement principal, les autorités des différents Etats Membres devant ensuite coopérer entre elles.
Les sociétés établies en dehors de l'Union européenne, mais ayant une activité ciblant le public européen, devront quant à elles désigner un représentant sur le territoire de l'Union, qui agira comme point de contact unique, tant pour les autorités que pour les personnes dont la société en question traite les données. A l'instar des pratiques en matière de fiscalité, cette dernière exigence incitera très probablement les grands acteurs du numérique non établis en Europe à désigner un représentant dans un Etat Membre dont l'autorité nationale de protection des données aura des règles réputées plus souples, ou disposera de moins de moyens pour diligenter des contrôles ou engager des procédures de sanction. Ces disparités devraient toutefois être tempérées par la coordination qu'assurera la nouvelle autorité européenne instaurée par le règlement.
En revanche, les **procédures internes seront quant à elles décuplées…** Un contrôleur à la protection des données devra être désigné dans les entités publiques et dans les entreprises traitant des données personnelles à une échelle importante. Il convient de souligner qu'il n'y a pas de seuil chiffré permettant à une entreprise de déterminer si elle doit ou non désigner une telle personne. Sa désignation est requise lorsque l'activité de l'entreprise implique le traitement de données personnelles de manière régulière et systématique sur une large échelle…
Le contrôleur pourra alternativement être salarié ou prestataire de service. Le responsable de traitement devra également tenir à jour des registres des traitements mis en œuvre sur le même modèle que ce qui existe actuellement pour les CIL. Dans la logique du principe d'« *accountability* », ces mesures devront permettre au responsable de traitement de démontrer que les traitements qu'il met en œuvre se font en conformité avec le règlement.
Afin de faciliter aux entreprises la mise en œuvre de telles procédures, et la démonstration de conformité du responsable de traitement à ses obligations, le règlement renvoie ici encore à un mécanisme de certification ou à des codes de conduite.

Et côté personnes physiques, quels droits ? Quelles protections nouvelles ?
Les personnes dont les données sont traitées devront bénéficier d'une **information plus large** sur les traitements qui les concernent. Outre les informations qui doivent déjà être fournies lors de la collecte de données en application de la Loi Informatique et Libertés, le responsable de traitement doit notamment préciser le fondement juridique du traitement, ainsi que la possibilité de déposer plainte auprès d'une autorité compétente d'un Etat Membre. Les mentions d'informations fournies par les responsables de traitement devront donc être ajustées.
Les personnes dont les données sont traitées bénéficieront d'un **droit à la portabilité de leurs données**. Les responsables de traitement devront donc être en mesure de restituer aux personnes dont les données sont traitées lesdites données, et ce dans un format standard et exploitable, afin qu'elles puissent être communiquées à un autre prestataire de services. Cette communication de données pourra même se faire directement au nouveau prestataire sur demande de la personne concernée.
Le projet de règlement prévoit des règles nouvelles encadrant **les traitements de données relatives aux enfants**. Ainsi, l'article 8 du projet de règlement prévoit une disposition visant à interdire aux services de la société de l'information destinés aux mineurs de 16 ans de recueillir leurs données personnelles sans autorisation préalable d'un titulaire de l'autorité parentale. Les Etats Membres pourront décider d'abaisser cette limite d'âge jusqu'à 13 ans. Le texte ajoute que le responsable de traitement devra fournir des efforts raisonnables, au regard des technologies disponibles, pour vérifier que le consentement est bien fourni par le titulaire de l'autorité parentale.
Les éléments détaillés ci-dessus ne sont que quelques points d'attention extraits parmi les 209 pages du projet de règlement dans sa dernière version. Les subtilités se cachent dans les détails et les 4 années de modifications et de reformulations du texte depuis sa première mouture ont pu altérer sa cohérence. Les deux années avant l'entrée en vigueur des dispositions nouvelles ne seront pas de trop pour permettre aux entreprises de se mettre en conformité. D'autant qu'en cas de manquement, les sanctions administratives pourront désormais aller jusqu'à 20 000 000 d'euros ou 4% du chiffre d'affaires mondial… ce qui est sans commune mesure avec les 150 000 euros d'amende que peut à ce jour prononcer la CNIL.

Réagissez à cet article

Source : *Le règlement européen sur les données personnelles annoncé pour le printemps : Quels changements anticiper ? – Féral-Schuhl Sainte-Marie*