Lire cet article en ligne

Nouveau règlement européen sur la protection des données (Partie I)

Le très attendu Règlement n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (autrement appelé le « Règlement général sur la protection des données » ou « RGPD ») vient de paraître au Journal officiel de l'Union européenne (JO, L 119, 4 mai 2016).

Sur proposition de la Commission européenne en date du 25 janvier 2012, ce Règlement adopté conjointement par le Parlement européen et le Conseil remplace la directive 95/46/CE et instaure un cadre général et unique pour la protection des données en Europe.

Le présent article (Partie I ; Partie II à paraître le mois prochain) se propose d'identifier les principales innovations apportées par le Règlement.

Contexte

Le Règlement général sur la protection des données (ci-après le « Règlement ») s'inscrit dans le cadre d'une réforme complète des dispositions européennes relatives à la protection des données.

Cette réforme comporte également une Directive n°2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données. La directive s'appliquera aux transferts de données à travers les frontières de l'Union Européenne (ci-après « l'UE ») et fixera, pour la première fois, des normes minimales pour le traitement des données à des fins policières et judiciaires au sein de chaque État membre. Les Etats membres ont jusqu'au 6 mai 2018 pour adopter les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la directive.

Le Règlement, qui lui est entré en vigueur le 25 mai 2016, sera obligatoire dans tous ses éléments et

directement applicable dans tout État membre deux ans après cette date, soit à partir du 25 mai 2018 (article 99).

Rappelons en effet qu'à l'inverse de la directive qui « *lie tout État membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens* », le règlement a « *une portée générale* », et « *est obligatoire dans tous ses éléments (et) directement applicable dans tout État membre* »[1].

Avec l'application de ce Règlement, à compter donc du 25 mai 2018, les Etats membres de l'UE disposeront d'une législation uniforme et actualisée en matière de protection des données.

La directive 95/46/CE précitée de 1995 (ci-après la « Directive »), qu'il abroge, était l'instrument législatif principal de la protection des données à caractère personnel en Europe. Ses objectifs et les mesures nationales qui les transposaient demeurent d'actualité jusqu'à ce que le Règlement s'applique.

Le besoin d'adapter l'encadrement juridique actuel à notre environnement numérique et l'octroi de compétences à l'UE en matière de protection des données à caractère personnel[2] sont à l'origine de la proposition et de l'adoption, après 4 années de discussions cependant, de ce nouveau Règlement.

Champ d'application territorial (article 3)

Les règles actuelles pour déterminer la loi nationale applicable au traitement de données résultent de la Directive et permettent l'application cumulative et simultanée de plusieurs législations nationales à un seul responsable de traitement établi dans plusieurs Etats Membres (article 4, 1, a), ce qui peut être source à la fois de complexité et de coûts pour ce responsable de traitement. Selon la Commission européenne, ce n'est pas moins de 2,3 milliards d'euros par an qui pourraient être économisés par les entreprises avec le Règlement.

Sachant que la notion d'« *établissement* », qui n'est pas définie dans la Directive, a été globalement interprétée largement par les autorités nationales (en pratique, même un cabinet d'avocat, un bureau d'une personne et même un simple agent dans un Etat membre peuvent être considérés comme un « établissement »), ces règles peuvent en effet conduire à l'application au même responsable de traitement des différentes législations nationales de chaque Etat membre concerné par chaque établissement.[3]

Plus subtil encore, ces règles permettent à un Etat membre d'appliquer sa législation à un traitement de données dont le responsable du traitement n'est pas établi sur le territoire de l'Union européenne mais « *recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur (c)e territoire.* » (article 4, 1, c).

Ici encore, la notion de « *moyens, automatisés ou non, situés sur le territoire* », qui n'est pas définie dans la Directive, prête à discussion et est interprétée de façon très large et différemment entre les Etats membres.

Elle englobe ainsi les intermédiaires humains ou techniques, voire même les activités externalisées, auprès de sous-traitants notamment.[4]

L'application du Règlement devrait régler ce problème d'insécurité juridique et de surcoût dans la mesure où il est directement et immédiatement applicable dans tous les Etats membres. Les mêmes règles s'appliqueront, sans que des mesures nationales de transposition soient nécessaires. En cas de pluralité d'établissements, c'est l'établissement principal qui sera pris en compte.

Si le critère de l'établissement du responsable de traitement, mais également celui du sous-traitant, continuera de s'appliquer, le Règlement conserve l'idée que les règles européennes de protection des données personnelles doivent s'appliquer à un responsable de traitement même si celui-ci n'est pas établi en Europe. Sauf qu'à la place de la localisation des « *moyens* » qu'il utilise pour traiter les données, le Règlement recherchera le contexte dans lequel il les traite : si le responsable de traitement, ou un sous-traitant, sans être établi dans l'Union, a des « *activités de traitement liées a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* », le Règlement s'appliquera également (article 3).

Reste à voir comment les autorités nationales des Etats membres vont appliquer cette disposition et en contrôler l'application, mais elle aura vraisemblablement pour effet de soumettre tous les acteurs économiques opérant sur le marché européen aux nouvelles règles européennes en matière de protection des données.

Il suffit de lire le préambule du Règlement pour s'en convaincre :

- s'agissant de l'offre de biens et de services, « *Alors que la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention, des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union, peuvent indiquer clairement que le responsable du traitement envisage d'offrir des biens ou des services à des personnes concernées dans l'Union*» (considérant n°23) ;
- et, s'agissant du comportement des personnes, *« Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit. »* (considérant n°24).

Consentement (articles 4, 11°, 6 et 7)

Il est indéniable que les règles européennes, et les législations nationales les transposant, ne permettent pas toujours de s'assurer que le consentement de la personne concernée au traitement est libre et éclairé.[5]

Le consentement est pour l'instant défini par la Directive comme « *toute manifestation de volonté, libre, spécifique et informée* » par laquelle la personne concernée accepte « *indubitablement* » que des données à caractère personnel la concernant fassent l'objet d'un traitement (Combinaison des articles 2, h et 7, a).

Les Etats membres ont transposé ce concept de façon très différente dans leurs droits nationaux. En particulier, et puisqu'aucune forme n'est prescrite, certains Etats membres acceptent le consentement implicite alors que d'autres exigent un consentement explicite, voire écrit.[6]

Par exemple, en France, la loi Informatique et Libertés ne donne aucune définition du consentement (article 7) et précise seulement les cas dans lesquels il doit être exprès (articles 8, 33 et 56). C'est seulement pour la prospection commerciale, en particulier au moyen de courriers électroniques et de SMS, que la loi définit le consentement (conformément à l'article 2, f de la Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, qui a le même sens que celui de la Directive 95/46), lequel doit être considéré comme exprès d'après le Conseil d'Etat[7].

Le Règlement prend clairement position : il s'agira désormais de « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* » (article 4, 11°).

Ainsi, le consentement devra nécessairement se faire « *par une déclaration ou par un acte positif clair* ».

Ici encore, le préambule nous renseigne sur ce que constitue et ne constitue pas une « *déclaration* » ou un « *acte positif clair* » : « *Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité* » (considérant n°32).

Il est précisé que la charge de la preuve du consentement pèse sur le responsable de traitement (article 7, 1°).

Par contre, le règlement ne révolutionne pas le champ d'application de ce principe. Si le traitement de données reste basé sur le consentement (article 6, a), les cas de traitements licites sans le consentement de la personne concernée demeurent quasiment inchangés (article 6, b à f).

Enfin, le Règlement établit clairement que « *La personne concernée a le droit de retirer son consentement à tout moment* » et qu'elle doit « *en (être) informée avant de donner son consentement. Il est aussi simple de*

retirer que de donner son consentement » (article 7, 3°).

[1] Article 288 TFUE, ex-article 249 TCE.

[2] Article 16 TFUE, ex-article 286 TCE.

[3] Voir Opinion 8/2010 sur le droit applicable du groupe de travail de l'article 29, p. 10 (en anglais : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf). Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE

[4] Idem., p. 20 et suiv.

[5] Voir Opinion 15/2011 sur la définition du consentement du groupe de travail de l'article 29 (en anglais : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf).

[6] Analyse d'impact de la Commission européenne sur le projet de règlement en date du 25 janvier 2012, SEC (2012) 72 final, p. 15 (en anglais seulement : http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf)

[7] Article L. 34-5 du code des postes et des communications électroniques, et arrêt du Conseil d'Etat en date du 11 mars 2015, Société TUTO4PC, n°368624.