Par Prudence Cadio,
avocat counsel,

et Eva Naudon,
avocat collaborateur,
LPA-CGR avocats

Sociétés établies en dehors de l'Union européenne : pourquoi il faut s'intéresser au nouveau règlement européen en matière de protection des données à caractère personnel

Après de nombreuses années de négociations, l'Union européenne («UE», «Union») se dote enfin d'une réglementation homogène en matière de protection des données à caractère personnel, matérialisée par le règlement 2016/679 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, adopté le 27 avril 2016 par le Parlement européen («RGPD», «Règlement»).

Pour rappel, les données à caractère personnel désignent toutes les informations se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement. Quant au responsable de traitement, il s'agit de l'entité qui détermine les moyens et finalités du traitement mis en œuvre, tandis que le sous-traitant renvoie à l'entité qui traite les données à caractère personnel pour le compte du premier (articles 2 et 3 de la loi Informatique et libertés, article 4 du RGDP).
L'application du RGDP, judicieusement repoussée au 25 mai 2018, a permis d'appréhender pendant deux années les nouvelles dispositions qu'il contient, dont les caractéristiques principales peuvent se résumer comme (i) le renforcement considérable des obligations imposées aux responsables de traitement de données à caractère personnel et, nouveauté du texte, à leurs sous-traitants, ainsi que (ii) l'accent mis sur le volet répressif, les sanctions applicables en cas de non-conformité aux dispositions du RGDP ayant été significativement durcies.
Si l'objectif poursuivi par le Règlement est l'harmonisation des législations au sein de l'Union, son rayonnement dépasse de toute évidence la frontière des vingt-sept Etats membres. Certes, les entreprises établies sur le territoire de l'Union, agissant tant en qualité de responsable de traitement que de sous-traitant, sont les premières intéressées par le RGDP. Cette simplicité apparente s'efface toutefois devant la définition du champ d'application territorial du Règlement, qui lui offre un spectre beaucoup plus large.

1. Les critères d'application du Règlement à double détente pour une entreprise établie hors UE

Pour se voir appliquer les dispositions du Règlement, le critère premier est l'établissement au sein de l'Union de l'entité collectant ou traitant les données que celle-ci agisse en qualité de responsable de traitement ou de sous-traitant. Guidé par un esprit plus universaliste, le texte prévoit de nouveaux critères. On observe ainsi un phénomène de capillarité qui implique, de jure, une hausse du nombre d'entreprises potentiellement concernées par le RGPD.
Deux cas de figure impliqueront l'application des dispositions du Règlement à des sociétés établies en dehors de l'Union, il s'agit d'une part du cas de l'entité entrant dans le périmètre du Règlement et, d'autre part, celui-ci de l'application par ricochet imposée au sous-traitant.

1.1. L'application directe du Règlement

L'application directe du Règlement vise deux situations expressément énoncées, dont le tronc commun est celui d'un responsable de traitement ou de son sous-traitant situé en dehors de l'UE, qui met en œuvre un traitement visant les données à caractère personnel d'individus se trouvant dans l'UE.

• L'offre de biens ou de services à distance
Cette hypothèse a, à l'évidence, vocation à intéresser un grand nombre d'entreprises. Elle couvre tous les traitements des sociétés de l'e-commerce offrant leurs produits et services à des personnes établies dans l'Union, ainsi que les sous-traitants de ces sociétés, tels que les SSII (hébergement du site Internet, service après-vente).
L'offre de bien ou le service ne doit, cependant, pas seulement être consultable par une personne située dans l'UE, elle doit lui être destinée. Le critère de destination est rempli par un faisceau d'indices, et notamment la possibilité de se faire livrer dans l'UE, l'affichage des prix en euros ou l'utilisation d'une langue du pays de l'UE.

• Le suivi du comportement, ou profilage
Moins visible mais tout aussi importante, cette hypothèse s'adresse aux sociétés étrangères qui utilisent des techniques de traçage des comportements sur Internet des utilisateurs situés en UE afin notamment d'enrichir des outils de statistique ou de publicité ciblée.
Dans les deux situations précitées, le responsable de traitement et le sous-traitant sont visés indifféremment, allongeant ainsi notablement la chaîne des entreprises concernées par le Règlement. Partant, le lien avec le RGDP peut apparaître dilué mais reste pourtant bien présent, justifiant une attention toute particulière à ces schémas. A titre d'illustration, sera soumise au Règlement la société (sous-traitante) offrant un service d'hébergement d'un site d'e-commerce d'une entreprise taïwanaise (responsable de traitement) offrant ses produits au public allemand et autrichien.

1.2. L'application du Règlement par ricochet

Le Règlement, dans son entreprise de responsabilisation du responsable de traitement, lui impose de prendre toutes les mesures appropriées afin de s'assurer que le traitement qu'il met en œuvre est conforme au RGPD (article 24). Cette disposition contraint en pratique le responsable de traitement à exiger de son sous-traitant le respect des mêmes règles que celles qui s'imposent à lui en application du Règlement. L'outil contractuel s'avérera le plus adapté pour faire peser sur le sous-traitant cette obligation de conformité et engager sa responsabilité en cas de défaut. L'entreprise sous-traitante se verra notamment imposer, contractuellement, des exigences strictes de sécurité, telles que la notification des failles ou l'interdiction de recruter un autre sous-traitant sans l'autorisation écrite préalable du responsable de traitement (article 28).
Les entreprises dont l'activité est de répondre aux besoins d'externalisation d'autres sociétés (système de fiche de paye, édition de compte bancaire, maintenance informatique, hébergement de données, etc.) doivent ainsi, en tant que sous-traitants, se préparer à respecter les exigences du Règlement alors même qu'elles sont situées hors UE, qu'elles n'offrent pas de service à distance ni ne pratiquent le profilage de ressortissants européens.

2. Obligations et sanctions

L'entreprise soumise au RGDP devra respecter de nombreuses obligations pour attester de sa conformité lesquelles ne font pas l'objet des présents développements. Il est toutefois utile de rappeler l'obligation spécifique incombant aux entités situées hors UE visées par le RGPD, à savoir celle de désigner un représentant.

2.1. Désignation d'un représentant

La contrainte la plus pragmatique vise à ne pas isoler les entreprises soumises au Règlement, quand bien même elles seraient territorialement éloignées de l'Union. Le RGDP tend ainsi à garantir une mise en œuvre effective des obligations pesant sur les responsables en imposant aux entreprises ou sous-traitants situés hors UE de désigner un représentant au sein de ce territoire (article 27). Désignée par écrit, cette personne physique ou morale sera un point de contact et un relais, tant pour les autorités de contrôle que pour les personnes concernées.
Dès lors, le représentant sera considéré comme l'interlocuteur privilégié des autorités pour toutes les questions relatives au traitement des données à caractère personnel traitées depuis le pays hors UE. Ce représentant aura notamment la charge de tenir un registre – lorsque la tenue de ce registre est prescrite par le Règlement – de toutes les catégories d'activités de traitement de données à caractère personnel mises en œuvre sous leur responsabilité. L'existence et la présence de ce représentant dans un Etat membre n'exonèrent néanmoins nullement le responsable du traitement ou le sous-traitant de leur responsabilité à l'égard ni des autorités de contrôle, ni des personnes concernées.
Certains aspects du rôle du représentant et l'articulation de ses obligations avec l'entité responsable du traitement restent encore à clarifier, notamment sa responsabilité propre dans sa fonction de relais entre l'entité responsable hors UE et l'autorité de contrôle.

2.2. Sanctions

L'intérêt de l'Europe pour la protection des données à caractère personnel se manifeste par un durcissement, remarqué, des sanctions applicables. Le Règlement augmente ainsi substantiellement le montant des sanctions en cas de non-conformité avec ses dispositions, à savoir, jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial ou 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, selon les cas, pour les amendes administratives. ■