PROJET DE RÈGLEMENT EUROPÉEN

Les données à caractère personnel au cœur de la sécurité et des libertés numériques

Pour compléter notre dossier sur les enjeux des données personnelles, Maître Eric Caprioli et Isabelle Cantero, du cabinet Caprioli & Associés, livrent leur analyse du règlement européen [1] sur le traitement des données à caractère personnel.

Eric A. Caprioli,
Avocat à la Cour de Paris,
Docteur en droit et membre de la délégation française aux Nations Unies.

Isabelle Cantero,
Juriste sénior, responsable du Pôle « Données personnelles et vie privée », Caprioli & Associés - société d'avocats.
www.caprioli-avocats.com
contact@caprioli-avocats.com

Le 25 janvier 2012, la Commission européenne a présenté un projet de règlement communautaire visant à encadrer la protection des données à caractère personnel. Le recours à cette forme de législation plutôt qu'à une directive se justifie par le fait qu'un règlement, d'application directe dans tous les Etats membres, permet une meilleure uniformisation qu'une directive (qui laisse aux Etats une marge de manœuvre dans la transposition du texte, ce qui crée des disparités entre les Etats). Force est de constater que les principes fondateurs de la directive 95/46/CE ne sont pas remis en cause par le projet qui met à jour et complète un certain nombre d'innovations dues aux nouveaux usages numériques, à la globalisation et, plus généralement, au développement des technologies de communication et à la sécurité numérique qui en découle. Il était urgent de prendre en compte les activités des nouveaux business models tels que les moteurs de recherche, les réseaux sociaux, les blogs ou les techniques de profilage numérique qui ne garantissent pas une protection suffisante des données à caractère personnel.

L'objectif de cette réforme est de renforcer les droits des citoyens, d'effectuer une adaptation aux nouveaux services et usages de l'internet et de faciliter la circulation des données à caractère personnel au sein de l'Union européenne. Dans ce contexte, de par l'aggravation des sanctions financières qu'il prévoit, le futur règlement aura un impact non négligeable sur la compétitivité de l'ensemble des entreprises européennes procédant aux traitements des données personnelles. Dans cette perspective, les manquements au projet seront susceptibles d'entraîner des sanctions pénales dans chaque Etat membre, ainsi que des sanctions administratives par les différentes autorités nationales de contrôle (les amendes peuvent aller jusqu'à 1 000 000 d'euros et 2 % du CA annuel mondial).

Des mesures de simplification

En ce qui concerne les transferts des données hors de l'Union européenne, le projet prévoit de modifier les conditions de mise en œuvre des **Binding Corporate Rules** (BCR, règles contraignantes internes). Ainsi, il ne serait plus nécessaire d'obtenir des autorisations subséquentes pour les transferts s'appuyant sur les BCR, ne subsisteraient que les demandes d'autorisation pour des traitements particuliers (ex : données de santé). Il est envisagé d'élargir le périmètre des BCR en permettant d'encadrer les transferts entre un groupe et ses sous-traitants.

Dans le cadre de la simplification des procédures, **un guichet unique pour les entreprises** établies dans plusieurs Etats membres est prévu. Dans ce contexte, une seule autorité de contrôle du pays du principal lieu d'établissement de l'entreprise serait compétente pour contrôler ses activités pour l'ensemble des entités (filiales, succursales) établies dans les autres Etats membres. Un des risques inhérent à ce type de mesure réside dans le « forum shopping », par le biais duquel les entreprises pourraient être tentées de s'établir dans les pays où le contrôle est le moins restrictif. Soulignons que la CNIL s'oppose fermement à une telle

(1) Règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), 25 janvier 2012, COM(2012) 11 final).

réforme en considérant qu'elle limiterait le rôle des autorités nationales à une simple boîte aux lettres, renforçant l'image bureaucratique et lointaine des institutions communautaires, voire privant largement les citoyens de la protection offerte par leur autorité nationale.

Droit à l'oubli et consentement préalable

S'agissant du **droit à l'oubli**, tel que prévu par l'article 17 du projet de règlement, il consisterait notamment en l'obligation faite au responsable du traitement d'effacer, sur demande de la personne concernée, ses données à caractère personnel et de cesser la diffusion de ces données, principe étendu aux données à caractère personnel que la personne avait rendues disponibles lorsqu'elle était enfant.

Le droit à l'oubli, initialement présenté par la Commission européenne comme une véritable avancée au titre de la protection des données en ligne a récemment été remis en cause et jugé irréaliste. En effet, les informations étant instantanément dupliquées sans que le prestataire garde le contrôle des données reproduites, il semble techniquement impossible de les retirer ou de les bloquer systématiquement, outre les risques d'atteintes à la liberté d'expression, au droit à l'information et à la liberté d'entreprendre.

L'article 7 précise les conditions relatives au **consentement préalable** au traitement de données. Ainsi, celui-ci devrait être donné de manière explicite, selon toute modalité appropriée permettant une manifestation de volonté libre, spécifique et informée. Cette manifestation peut être constituée par une déclaration ou par tout acte non équivoque de la personne concernée, garantissant qu'elle consent bien en toute connaissance de cause au traitement de ses données à caractère personnel (par exemple en cochant une case lorsqu'elle consulte un site internet ou par le biais de toute déclaration ou tout comportement indiquant clairement dans ce contexte qu'elle accepte le traitement proposé de ses données à caractère personnel). **Il ne saurait y avoir de consentement tacite ou passif.** En outre, le consentement ne serait plus un motif valable de collecte de données en cas de déséquilibre significatif entre la personne concernée et le responsable de traitement (ce qui n'était pas précisé par la loi « Informatique et libertés » du 6 janvier 1978. Enfin, la personne concernée a le droit de retirer son consentement à tout moment, ledit retrait devant être porté à la connaissance des différents acteurs de la chaîne de traitement des données.

(2) Ordonnance n° 2011-1012 du 24 août 2011, (JO du 26 août 2011) ; Décrets n°2012-436 du 30 mars 2012 (JO du 31 mars 2012) et n°2012-488 du 13 avril 2012 (JO du 15 avril 2012 et 10 mai 2012).

Obligations en matière de conformité au Règlement

D'une part, le projet impose aux responsables de traitement d'adopter des règles internes et de mettre en œuvre les mesures nécessaires pour garantir la conformité desdites mesures au règlement (obligation d' « accountability »), notamment eu égard à l'obligation de sécurité, l'accomplissement des formalités préalables et la désignation d'un Délégué à la protection des données (article 22). Il ne suffira plus au responsable de traitement de respecter la loi, il devra également documenter et étayer le dispositif opérationnel mis en œuvre pour ce faire, la documentation pouvant à tout moment faire l'objet d'un audit par l'autorité de contrôle.

Parallèlement aux obligations strictes en matière de sécurité des données, le projet soumet à l'accomplissement des formalités déclaratives de traitement, la réalisation d'une étude d'impact relative à la protection des données. L'étude doit être finement menée en particulier pour les traitements présentant des risques particuliers au regard des droits et libertés des personnes concernées du fait de leurs nature, portée ou finalité.

D'autre part, l'obligation de désigner un Délégué à la protection des données s'applique au responsable de traitement et au sous-traitant. Elle sera obligatoire dans 3 hypothèses :
Lorsque le traitement est effectué par une autorité ou un organisme public.

Lorsque le traitement est effectué par une entreprise de 250 personnes ou plus.

Lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique des personnes concernées.

Notification des violations de données

L'obligation de notifier toute violation de données à caractère personnel, imposée aux fournisseurs d'accès à Internet et aux prestataires de communications électroniques (opérateurs de télécoms)[2], devrait être étendue désormais à tous les responsables de traitement, quel que soit le secteur d'activité.

Une violation de données se définit comme *« une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière »*.

Dans ce contexte, le responsable de traitement devrait informer l'autorité de contrôle de la violation *« sans retard injustifié et, si possible, 24 heures au plus tard après en avoir pris connaissance »*. Si le délai de 24 heures est dépassé, la notification devra comporter une justification à cet égard. Il est, par ailleurs, précisé que la notification doit être réalisée dans les formes documentaires prévues à cet effet de façon à contenir notamment les renseignements sur la nature de la violation, les coordonnées des personnes auprès desquelles des renseignements peuvent être obtenus, les mesures à prendre pour atténuer les éventuelles conséquences négatives, les conséquences de la violation, etc. **De même, une notification est due par chaque sous-traitant** qui doit immédiatement informer le responsable du traitement de toute violation de données. Il est également prévu que le responsable du traitement informe toute personne concernée par la violation dès lors que celle-ci est *« susceptible de porter atteinte à la protection des données à caractère personnel ou à la vie privée »*, à l'exclusion de l'hypothèse où il serait capable de démontrer qu'il avait mis en œuvre des mesures technologiques rendant les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès (c'est-à-dire des mesures de chiffrement).

Au titre des sanctions administratives et conformément à l'article 79-6-h) du projet :

« L'autorité de contrôle [en France, la CNIL] *inflige une amende pouvant s'élever à 1 000 000 EUR ou, dans le cas d'une entreprise, à 2 % de son chiffre d'affaires annuel mondial, à quiconque, de propos délibéré ou par négligence :*

(…)

h) omet de signaler ou de notifier une violation de données à caractère personnel, ou omet de notifier la violation en temps utile ou de façon complète à l'autorité de contrôle ou à la personne concernée conformément aux articles 31 et 32 ; ».

S'agissant des sanctions pénales, chaque État membre doit prévoir des sanctions effectives, proportionnées et dissuasives. Ces dispositions législatives devront être notifiées à la Commission au plus tard au moment de l'entrée en vigueur du texte. Il est à noter qu'actuellement, dans le cadre de l'ordonnance du 24 août 2011, les peines encourues en matière de violations des données à caractère personnel par le fournisseur de service de communications électroniques qui ne procède pas à la notification prévue sont de 5 ans d'emprisonnement et 300 000 euros d'amende (article 226-17-1 du code pénal).

Notions de « responsable du traitement »

Les notions de responsable de traitement des données et de sous-traitant des données jouent un rôle central dans l'application du projet de règlement, car elles déterminent la ou les personnes chargées de faire respecter les règles de protection des données, la manière dont les personnes concernées peuvent exercer leurs droits, le degré d'efficacité des autorités chargées de la protection des données, le droit national applicable, etc. Sur ce dernier point, le texte précise, en effet, que chaque État membre applique ses dispositions nationales aux *« traitements de données à caractère personnel, lorsque* […] *le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre »*. Au surplus, *« si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable »*.

Dans ce prolongement, le projet de règlement consacre également la notion de co-responsables du traitement si les obligations mutuelles des parties, vis-à-vis des dispositions du règlement, n'ont pas été préalablement définies contractuellement. Un principe de responsabilité solidaire des parties est défini sur la totalité du dommage éventuellement subi par la personne concernée (art. 77), ainsi qu'une cause exonératoire partielle ou totale pour le responsable du traitement ou le sous-traitant s'ils apportent la preuve que le fait qui a provoqué le dommage ne leur est pas imputable.

En définitive, il apparaît que le projet de règlement modifie en substance les obligations des entreprises ou organismes qui traitent directement des données à caractère personnel (responsables de traitement) ou indirectement (celles qui agissent en qualité de sous-traitant). Si les données à caractère personnel présentent un caractère stratégique dans le cadre des activités numériques des entreprises et des autorités administratives, leur sécurité juridique et technique doit être assurée afin de garantir les droits fondamentaux des individus, et cela demain encore plus qu'aujourd'hui. ■