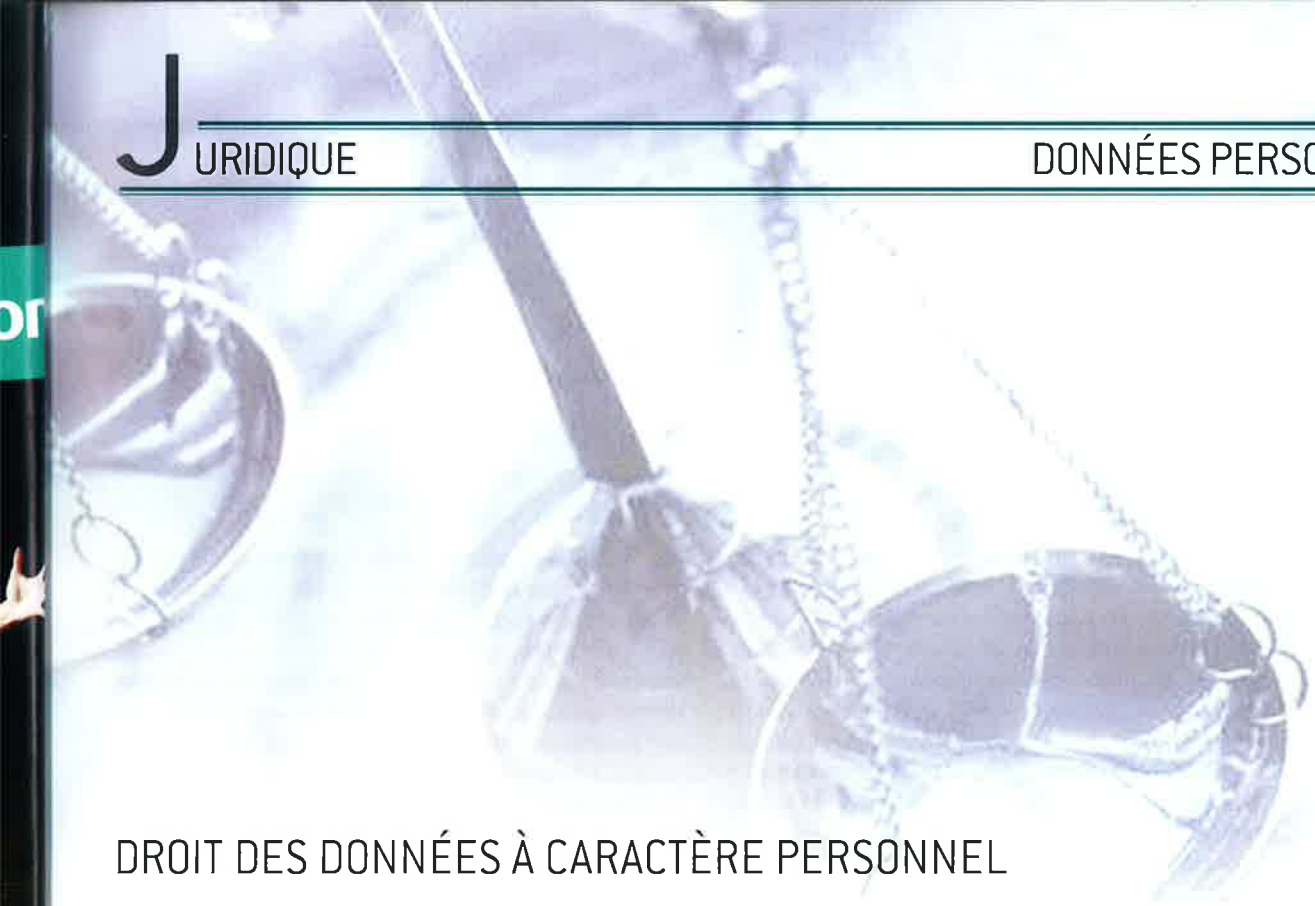

DROIT DES DONNÉES À CARACTÈRE PERSONNEL

De la sécurité de l'information à la mise en œuvre du principe d'accountability

L'évolution des technologies de l'information (Cloud computing, Big Data, médias sociaux,...), la prolifération et la puissance des outils technologiques, le succès de l'internet et la multiplication des acteurs du secteur ont pour conséquence un foisonnement exponentiel des collectes et des traitements de données à caractère personnel. Les systèmes d'information des entreprises ou organisation ont une incidence directe sur l'exploitation des données personnelles. Un projet de règlement européen envisage une responsabilisation des acteurs.

Eric A. Caprioli, Avocat à la Cour de Paris, Docteur en droit.

Isabelle Cantero, Juriste sénior, Responsable du Pôle Données personnes et vie privée (Caprioli & Associés, société d'avocats).

La valeur économique des données personnelles croît de façon proportionnelle, augmentation qui ne doit pas occulter les risques encourus (divulgation, atteinte à la réputation, altération/perte de données). Au vu de la complexité de l'environnement numérique, le renforcement de la protection des données s'est imposé à l'Union européenne qui a travaillé sur une Proposition de Règlement en la matière (ci-après « proposition de Règlement ») publié le 25 janvier 2012 [1], toujours en cours de discussion et destiné à remplacer la Directive 95/46/CE du 24 octobre 1995 actuellement en vigueur.

Partons d'un constat négatif selon lequel les principes de protection des données prévus par les dispositions légales actuelles, et spécifiquement eu égard aux obligations relatives à la sécurité, ne paraissent plus suffisants. Ainsi, le texte européen à l'étude prévoit-il une véritable responsabilisation des acteurs et en particulier du responsable de traitement, quant à la protection des données à caractère personnel.

Les obligations de sécurité en vigueur

A l'instar du dispositif européen actuel, la loi française « Informatique et Libertés » n°78-17 du 6 janvier

(1) COM(2012) 11 final 2012/0011 (COD). Eric A. Caprioli et Isabelle Cantero, «Les données à caractère personnel au cœur de la sécurité et des libertés numériques», Mag-Securs, n°36, pp. 29-31.

1978 modifiée pose un principe général de sécurité des données personnelles. L'article 34 de la loi impose en effet au responsable de traitement *« de prendre toutes les précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données »*. La jurisprudence considère traditionnellement qu'il s'agit d'une obligation de moyens aux termes de laquelle le responsable de traitement est tenu de veiller à *« empêcher que les données soient déformées, endommagées, ou que des tiers non autorisés y aient accès »*. Les politiques et les procédures à mettre en œuvre en vue de garantir la sécurité et la confidentialité des données sont donc laissées à la libre appréciation des responsables, selon l'état de l'art et proportionnées au niveau de sensibilité des données concernées.

Un libre arbitre mesuré, toutefois, depuis la transposition du Paquet télécoms en droit français par l'Ordonnance n°2011-1012 du 24 août 2011 relative aux communications électroniques et l'introduction d'un article 34 bis au sein de la loi « Informatique et libertés ». Cet article consacre la notion de violation de données à caractère personnel, définie en tant que *« violation de sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques »*. Ces violations doivent être signalées à la CNIL sans délai, étant précisé que l'obligation de notification s'applique aux fournisseurs de services de communications électroniques ouverts au public, qui sont, selon la CNIL les opérateurs enregistrés auprès de l'ARCEP (prestataires de télécoms, Fournisseurs d'accès à l'internet). Mais on peut s'interroger sur l'application de ces dispositions à des entreprises ou organismes qui fournissent des accès WiFi gratuits au public.

Or, la proposition de Règlement européen sur la protection des données personnelles a vocation à étendre cette obligation à tous les responsables de traitement, quel que soit le secteur d'activités ou la taille de l'entreprise/organisme. L'accent est résolument mis sur la nécessité d'assurer la sécurité des données traitées qui devient quasiment une obligation de résultat. En tout état de cause, les responsables de traitement devront notifier la violation des données personnelles qu'ils traitent à la CNIL et assumer les conséquences d'une défaillance, fût-elle par négligence ou par absence d'efficacité des mesures prises ou encore en raison de leur insuffisance. Mais cette notification pourra également s'effectuer auprès des personnes concernées par la violation, sauf si le responsable de traitement prouve à l'autorité de contrôle qu'il a mis en œuvre des solutions rendant les données incompréhensibles aux personnes non autorisées.

Pendant du principe de sécurité des données, l'exigence de transparence quant aux mesures adoptées à cette fin figure également dans l'obligation générale de déclaration préalable des traitements de données personnelles auprès de la CNIL (articles 22 et suivants). Plusieurs types de formalités sont prévus selon le degré de « sensibilité » du traitement concerné et/ou des données traitées, étant noté que le contrôle de la sécurité est à ce stade toujours ex ante. Partant, les risques de « décalage » entre la formalité accomplie auprès de la CNIL et la réalité du traitement ne peuvent jamais être totalement exclus.
Dès lors, la mise en œuvre effective de la sécurité des données personnelles est une nécessité. Dans cette perspective, la proposition de Règlement européen érige le principe de responsabilité (« accountability ») en nouvelle pierre angulaire de la protection des données à caractère personnel.

Le principe d'« accountability » dans la proposition de Règlement européen

Si le terme « accountability », d'origine anglo-saxonne, ne reçoit pas de traduction unique (par exemple : « principe de responsabilité » dans la proposition de règlement alors qu'il est question d'« engagement responsable » pour la CNIL), il se dégage néanmoins un large consensus sur son acception. Le concept renvoie ainsi à la façon dont la responsabilité à l'égard des données est assumée par le responsable de traitement et peut être prouvée. Dans cette perspective, les responsables de traitement seront contraints de mettre en œuvre des mesures de protection efficaces des données, au moyen d'outils et de procédures et de garantir la conformité de leurs traitements au Règlement dans la durée. Ils devront en justifier auprès de la CNIL et ne pas simplement présenter un dispositif de conformité de façade. L'objectif du législateur européen est d'obliger les responsables de traitement à s'inscrire dans une bonne gouvernance en la matière, à partir de mécanismes fondés sur la responsabilité.

Le cadre juridique de l'« accountability » est posé par l'article 22 de la proposition de Règlement. Au titre des mesures considérées comme appropriées, figurent la tenue d'une documentation dédiée, la mise en œuvre des obligations en matière de sécurité des données, la réalisation d'une analyse d'impact sur la protection des données (« Privacy Impact Assesment »), le respect des obligations relatives aux demandes d'autorisation ou de consultation, la désignation d'un délégué à la protection des données.

La documentation (détaillée à l'article 28) est au cœur du dispositif ; elle doit être mise à jour, son objectif premier étant d'assurer une trace de tous les traitements par le responsable de traitement. La documentation a vocation à démontrer la réalité des mesures prises et doit être tenue à la disposition de l'autorité de contrôle (la CNIL pour la France).

S'agissant spécifiquement de l'obligation de sécurité (article 30 de la proposition de règlement), des mesures techniques et organisationnelles doivent être adoptées et consignées dans la documentation sur les traitements. L'obligation de sécurité est substantiellement renforcée par rapport à l'obligation actuellement en vigueur. La pertinence des mesures à mettre en place doit être appréciée au regard d'une évaluation des risques encourus par le traitement en cause.
Dans le même sens, le responsable de traitement doit déterminer et recenser les mesures pratiques pour la réalisation des analyses d'impact sur la protection des données (imposées par l'article 33 pour les traitements susceptibles de comporter ou de générer des risques particuliers).

Des mesures concrètes de mise en œuvre concernent également les formalités à accomplir auprès de l'autorité de contrôle (autorisation et consultation préalables telles que prévues par l'article 34 de la proposition de Règlement).

En amont, les responsables de traitement devront recourir à des technologies permettant de garantir la protection des données (« privacy by design ou par défaut»). Cela induira nécessairement une collaboration entre les services informatiques/sécurité, conformité et achats.
Dans tous les cas, le responsable de traitement doit rendre des comptes quant à l'efficacité de ces mesures en mettant en œuvre des mécanismes de vérification, dont le recours à des auditeurs indépendants internes ou externes (article 22.3 de la proposition de Règlement). Dans cette optique, on peut estimer que ces audits devraient se fonder sur des référentiels prenant en compte les dimensions juridiques, techniques/sécurité et organisationnelles. Enfin, l'orientation concrète du principe de responsabilité, tout en procédant au renforcement des obligations existantes, va de pair avec la désignation obligatoire d'un délégué à la protection des données (DPD) (article 35 de la proposition de Règlement). Peu d'entreprises devraient y échapper.

Le RSSI aura un rôle important dans l'élaboration des outils et des procédures associées à «l'accountability»

Ces mesures sont susceptibles d'être complétées par des procédures spécifiques telles que celles visant à garantir la gestion des demandes d'accès, la gestion des plaintes, la formation des personnes responsables de la conformité légale (interlocuteurs du DPD en interne). Autant de mesures qui attesteront de la responsabilisation de l'entreprise quant à la définition du niveau de protection le mieux adapté à sa situation, sous réserve qu'elle puisse en rapporter la preuve aux autorités de contrôle ainsi qu'aux personnes concernées.
Pour conclure, on peut constater que la sécurité de l'information et du numérique est au centre de ces dispositions relatives à la protection des données à caractère personnel (ex : avec la norme ISO 27001 et la mise en place d'un système de management de la sécurité de l'information qui couvre la protection des données à caractère personnel) ; et par voie de conséquence, le Responsable de la sécurité des systèmes d'information aura un rôle important à jouer dans l'élaboration des outils et des procédures associées à « l'accountability ».

Pour autant, ces nouveautés ne seront pas une révolution dans les grandes entreprises qui ont déjà adopté des mesures de sécurité appropriées. C'est le principe de documentation qui risque d'être plus problématique en terme de ressources humaines et financières.

Finalement, il reste que le travail de mise en conformité des traitements en interne pourrait être non seulement considéré comme une aide substantielle apportée aux autorités de contrôle dans leur mission de surveillance, mais aussi comme une pierre à l'édification de la responsabilité sociale de l'entreprise. ■