JURIDIQUE

Quelle sécurité de l'information en matière de protection des données personnelles ?

Jamais, avec le règlement européen, la protection des données n'aura été autant au centre des préoccupations des responsables SSI. Nature des risques, étendue de la responsabilité juridique, responsabilité des sous-traitants… Le point avec deux de nos fidèles chroniqueurs.

Les auteurs

Eric A. CAPRIOLI,
Avocat à la Cour,
Docteur en droit,
Vice-Président du CESIN.

Isabelle CANTERO, Juriste senior, Responsable du Pôle Données personnelles et vie privée (Caprioli & Associés, société d'avocats).

Selon les articles 34 et 35 de la loi « Informatique et Libertés », l'obligation de sécurité et de confidentialité des données s'impose d'une part au responsable de traitement et, d'autre part, à son (ses) sous-traitant(s). Toutefois, en cas de manquement à cette obligation, le responsable de traitement est passible de sanctions administratives[1] (de la Cnil) ou pénales[2] alors que le sous-traitant engagera sa responsabilité exclusivement sur la base du contrat conclu avec le responsable de traitement.

La sécurité actuellement

La règle posée est que le niveau de sécurité doit être déterminé compte tenu des risques présentés par le traitement et de la nature des données. Pour rappel, les risques identifiés sont *« la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite »*. Il s'agit pour le responsable de traitement et pour le sous-traitant d'adopter « toutes précautions utiles », c'est-à-dire concrètement, un ensemble de mesures techniques et organisationnelles en tenant compte de l'état de l'art et des coûts y afférents. Il s'agit aussi et surtout, en cas de sous-traitance, de veiller à consigner dans le contrat les exigences requises au titre de la sécurité et de la confidentialité des données personnelles traitées et de veiller au respect des mesures adoptées.

Ce qu'il faut retenir : le responsable de traitement n'est jamais déchargé de son obligation de sécurité et de confidentialité des données personnelles, y compris en cas de sous-traitance. Il est donc tenu de vérifier, d'un point de vue technique et organisationnel, l'efficience des garanties mises en œuvre … L'audit de sécurité parait incontournable nonobstant le soin particulier qui doit être apporté aux clauses relatives à la protection des données personnelles dans le contrat de sous-traitance ainsi que le suivi, le cas échéant, des dispositions contractuelles des sous-traitances ultérieures.

Sanctions du manquement à l'obligation de sécurité

Il convient tout d'abord de préciser que le seul manquement à l'obligation de *« mettre en œuvre les mesures prescrites à l'article 34 de la loi* « Informatique et Libertés » » est constitutif d'un délit sans que soit requise la preuve d'un préjudice quelconque. On constate que la jurisprudence en la matière est peu fournie.

En revanche, de nombreuses informations quant à la teneur de l'obligation peuvent être tirées des diverses mises en demeure et sanctions adoptées par la Cnil avertissement et sanction pécuniaire) à l'encontre des responsables de traitements défaillants. De fait, la Cnil a déjà considéré que le manquement à l'obligation de sécurité était caractérisé par la faiblesse des mots de passe (5 chiffres au lieu de 16) et par l'absence de politique de sécurité (sanction pécuniaire de 10 000 euros[3] confirmé par le Conseil d'État[4]). Elle a également sanctionné en tant que défaut de sécurité des données (sanction pécuniaire de 50 000 euros)[5] l'absence de politique de gestion des mots de passe (accès aux comptes clients et aux postes des salariés), leur vulnérabilité (robustesse insuffisante) et les lacunes du contrat de sous-traitance (aucune clause sur la sécurité).

Donc des sanctions à l'encontre du responsable de traitement pour ses propres manquements.

Mais la Cnil est aussi intervenue pour sanctionner les défauts de sécurité imputables au sous-traitant. Ainsi, le recours à des sous-traitants ne décharge pas le responsable de traitement de ses obligations et il est tenu de s'assurer de l'effectivité de la sécurité des données personnelles qui doit être garantie par ses sous-traitants. La Cnil a ainsi sanctionné le fait que la société DHL[6] n'avait pas cherché à vérifier la sécurité de l'ensemble de l'application qui avait été créée par un sous-traitant des années auparavant, le défaut de conception du logiciel développé par

[1] Sanctions de la CNIL en application de l'article 45 de la Loi de 1978 - avertissement, sanction pécuniaire, injonction de cesser le traitement – qui peuvent faire l'objet d'une publicité.

[2] Article 226-17 du code pénal : 5 ans d'emprisonnement et 300.000 euros d'amende pour les personnes physiques et 1.500.000 euros d'amende pour les personnes morales.

[3] Décision n° 2013-139 du 30 mai 2013 prononçant une sanction pécuniaire à l'encontre de la société PS Consulting.

[4] Conseil d'État, 10ème / 9ème SSR, décision du 18 novembre 2015.

[5] Délibération de la formation restreinte n° 2015-379 du 5 novembre 2015 prononçant une sanction pécuniaire à l'encontre de la société OPTICAL CENTER.

[6] Délibération de la formation restreinte n°2014-238 du 12 juin 2014 prononçant un avertissement rendu public à l'encontre de la société DHL INTERNATIONAL EXPRESS France

le sous-traitant n'ayant pas permis de sécuriser les adresses IP des clients et donc à l'origine de la diffusion de leurs données sur l'internet.
Dans le même sens, en décembre 2015, le Conseil d'État[7] a confirmé l'avertissement de la Cnil à l'encontre de la société Orange[8]. A l'issue d'un contrôle qui faisait lui-même suite à la notification de la violation de données clients (accès illicite à plus de 1,3 M de données), la CNIL avait relevé l'absence d'audit de sécurité des sous-traitants d'Orange, l'utilisation de moyens de communication non sécurisés, les mentions contractuelles insuffisantes et l'absence de suivi des dispositions contractuelles à destination du prestataire secondaire.
Enfin, dernièrement, suite à un contrôle réalisé en ligne sur le site de la société Ricard, la Cnil a prononcé un avertissement public[9], ayant constaté que la société avait manqué à son obligation de veiller à la sécurité et confidentialité des données (données de milliers de clients : noms, prénoms, adresses et numéros de cartes bancaires accessibles sur le site). La Cnil a rappelé que l'existence d'une sous-traitance (hébergement et gestion du site) n'exonérait pas la société Ricard de ses obligations légales telles qu'énoncées à l'article 34 de la loi. La Cnil ajoute que le seul fait de constater l'absence de mise en œuvre de mesures visant à garantir la sécurité des données suffit à caractériser le manquement à l'obligation de sécurité sans qu'il ne soit nécessaire de prouver un quelconque préjudice pour la personne concernée.
Pour la Cnil, *« les notions de sécurité et de protection de la vie privée sont aujourd'hui indissociables »*[10], notamment afin d'appréhender les changements inhérents à l'innovation numérique. Et, au-delà de la prise en compte de l'écosystème du numérique, la CNIL anticipe également les changements induits par le Règlement européen de protection des données[11] (« RGPD »), directement applicable à partir du 24 mai 2018.

La sécurité demain

La sécurité des traitements est prévue par l'article 32 du RGPD qui expose en premier lieu différents critères à prendre en compte par le responsable de traitement et le sous-traitant pour déterminer le niveau de sécurité à adopter, tels : l'état de l'art, les coûts de mise en œuvre de la sécurité, le traitement concerné en ce compris sa finalité et son contexte, la probabilité et la gravité des risques pour les droits et libertés des personnes. A l'instar de la règlementation actuelle, la logique est toujours d'adapter les mesures de sécurité aux risques identifiés, étant noté que le RGPD intègre les principes applicables à la gestion des risques pour les traitements de données personnelles.
Le règlement prévoit donc d'évaluer le (ou les) risque présenté par le traitement, en amont. Il incombe donc au responsable de traitement de réaliser une PIA (Privacy Impact Assessment ou étude d'analyse d'impact) pour tous les traitements susceptibles d'engendrer un risque élevé sur la vie privée des personnes concernées. Cela étant, certains traitements sont identifiés comme étant risqués par le RGPD et sont obligatoirement soumis à une PIA du fait de la nature des données traitées (traitement à grande échelle de données sensible ou pénales) ou de leur finalité (profilage, surveillance à grande échelle de zones accessibles au public, ...). Au-delà du risque inhérent au traitement lui-même et tel que ciblé par le PIA, le RGPD reprend les risques *« résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite »*.

Garantir la confidentialité

En ce qui concerne les garanties à mettre en place, l'article 32 énonce un certain nombre de mesures susceptibles d'être utilisées par le responsable de traitement en fonction du niveau de risque identifié par le responsable de traitement et/ou le sous-traitant. Sont ainsi évoqués : le recours à la pseudonymisation[12] et au chiffrement des données, l'adoption de moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes, l'adoption de moyens permettant de rétablir la disponibilité et l'accès aux données personnelles en cas d'incident technique ou physique, la vérification régulière des mesures. Les codes de bonne conduite (conforme article 40 du RGPD) et les certifications (conforme article 42 du RGPD) sont des solutions susceptibles d'être valablement envisagées en matière de sécurité.
En application de l'article 36 du RGPD, la consultation de l'autorité de contrôle étant un préalable à la mise en œuvre d'un traitement pour lequel le PIA aura révélé un niveau de risque élevé, les mesures choisies afin de garantir la sécurité du traitement devront être communiquées à l'autorité de contrôle compétente. Cette dernière est habilitée à apprécier si ces mesures suffisent à atténuer le risque identifié et partant pourra valider ou non le traitement concerné. Un traitement qui ne disposerait pas de garanties suffisantes au regard du risque présenté sera donc non conforme au règlement et pourra exposer le responsable de traitement ou le sous-traitant en cause aux sanctions prévues par l'article 83-4 (amende portée jusqu'à 2% du CA annuel mondial pour les entreprises ; sanctions qui, dans d'autres cas, peuvent aller au maximum jusqu'à 4% du CA).
Mais la sécurité des données ne s'arrête pas là. Par exemple, le RGPD consacre la généralisation de la notification des violations de données à l'autorité de contrôle dans la limite de 72 heures après en avoir eu connaissance (art. 33) et à la personne concernée (art. 34) ou encore, l'extension de la responsabilité du sous-traitant.
Et le RGPD nous fait dire : Quand la sécurité va, tout va !!! ■

[7] Arrêt du Conseil d'État du 30 décembre 2015, 10ème / 9ème SSR, 30/12/2015, 385019.

[8] Délibération de la formation restreinte n° 2014- 298 du 7 août 2014 prononçant un avertissement à l'encontre de la société ORANGE.

[9] Délibération de la formation restreinte n°2016-108 du 21 avril 2016 prononçant un avertissement (public) à l'encontre de la société Ricard.

[10] Rapport d'activité de la CNIL 2015, p.28 : « La protection des données personnelles au cœur de la cybersécurité »

[11] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE 4 mai 2016.

[12] Article 4-5) : «pseudonymisation», le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.