La notification des violations de données personnelles occupe une place de plus en plus importante dans l'actualité juridique. De fait à suivre Me Olivier Proust, il revient aux différents organismes concernés d'évaluer leur niveau de conformité en matière de sécurité des données et de mettre en œuvre des mesures adéquates en vue de gérer leur violation.

La notification des violations de données à caractère personnel : décryptage et analyse

Par Olivier PROUST
Of Counsel
Field Fisher Waterhouse

INTRODUCTION

À l'heure où l'Europe se dote d'une législation renforcée en matière de sécurité des réseaux et des systèmes d'information (1), la notification des violations de données personnelles occupe une place de plus en plus importante dans l'actualité juridique. La Commission nationale de l'informatique et des libertés (ci-après « Cnil ») vient de publier son rapport annuel d'activités 2012 (2) dans lequel elle annonce avoir reçu les premières notifications pour des violations de données à caractère personnel.

D'après un sondage (3) réalisé au Royaume-Uni, 93 % des grandes entreprises et 87 % des petites entreprises ont eu une faille de sécurité en 2012. En moyenne, les grandes entreprises estiment que le nombre total de failles survenues au cours de l'année passée s'élève à 113. Dans la plupart des cas, la violation des données est d'origine extérieure à l'entreprise (78 % pour les grandes entreprises et 63 % pour les petites entreprises). Par ailleurs, la violation des données personnelles a un coût indéniable pour les organismes.

Selon une étude de Ponemon Institute (4), le coût organisationnel moyen d'une effraction de données en 2011 s'élève à 2,55 millions d'euros et le coût moyen par dossier compromis est de 122 €. Les principales causes des violations de données seraient les attaques malveillantes ou criminelles qui entraînent la perte ou le vol de données (43 % des cas).

Alertée par la progression rapide de ce phénomène, la Commission européenne a entrepris une série de réformes en vue de renforcer la sécurité des données personnelles et d'introduire une obligation de notification des violations de données personnelles en Europe. Tout d'abord, en 2009, la directive n° 2002/58/CE sur la vie privée et les communications électroniques (5) a été modifiée par la directive n° 2009/136/CE (6), laquelle a introduit une obligation pour les fournisseurs de services de communications électroniques de notifier toutes les violations de données personnelles. En France, ces dispositions ont été transposées par l'ordonnance du 24 août 2011 « *relative aux communications électroniques* » (7) qui a introduit un nouvel article 34 *bis* sous la loi n° 78-17 du 6 janvier 1978 « *relative à l'informatique, aux fichiers et aux libertés* » (ci-après loi « Informatique et libertés ») (8). Ce nouveau régime a été complété par des mesures d'application énoncées dans un décret n° 2012-436 du 30 mars 2012 (9) et par la publication, le 28 mai 2012, d'une fiche pratique de la Cnil précisant les conditions de mise en œuvre de ces nouvelles dispositions (10).

Par ailleurs, la Commission européenne a publié le 25 janvier 2012 une proposition de règlement (11) qui vise à remplacer la directive n° 95/46/CE (12) relative à la protection des données personnelles.

---

(1) Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, 7 févr. 2013, COM(2013) 48 final, 2013/0027 (COD). **(2)** Cnil, 33e Rapport annuel 2012, <www.cnil.fr>. **(3)** *Information Security Breaches Survey*, réalisé par PwC, 2013, <www.pwc.co.uk/audit-assurance/publications/2013-information-security-breaches-survey.jhtml>. **(4)** Étude annuelle 2011 : coûts des effractions de données en France, réalisée par Ponemon Institute, sponsorisée par Symantec, publiée en mars 2012. **(5)** Directive n° 2002/58/CE du Parlement européen et du Conseil 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* » (directive vie privée et communications électroniques) JOCE 31 juill., art. L 201/37, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:FR:HTML>. **(6)** Directive n° 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive n° 2002/22/CE « *concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques* », la directive n° 2002/58/CE « *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques* » et le règlement (CE) n° 2006/2004 « *relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs* » (texte présentant de l'intérêt pour l'EEE), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0136:FR:NOT>. **(7)** Ordonnance n° 2011-1012 du 24 août 2011 « *relative aux communications électroniques* », <www.legifrance.gouv.fr>. **(8)** Loi n° 78-17 du 6 janvier 1978 « *relative à l'informatique, aux fichiers et aux libertés* » (modifiée par l'ordonnance n° 2011-1012 du 24 août 2012), <www.cnil.fr>. **(9)** Décret n° 2012-436 du 30 mars 2012 portant transposition du nouveau cadre réglementaire européen des communications électroniques. Ces nouvelles dispositions modifient le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 « *relative à l'informatique, aux fichiers et aux libertés* » (voir les articles 91-1 à 91-5). **(10)** Voir Cnil, La notification des violations de données à caractère personnel, publié le 28 mai 2012, <www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/la-notification-des-violations-de-donnees-a-caractere-personnel/>. **(11)** Proposition de 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), COM(2012) 11 final, 25 janv. 2012, <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm>. **(12)** Directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* », <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML>.

Une fois adopté, ce règlement imposera une obligation de notifier les violations de données à tous les responsables de traitements, quel que soit leur secteur d'activité.

En l'état actuel du droit, tous les organismes qui traitent des données personnelles sont soumis à une obligation générale de sécurité des données (I) mais seuls les fournisseurs de services de communication électronique ont l'obligation de notifier les violations des données (II). Toutefois, au vu des dispositions légales à venir, le moment semble propice pour tous les organismes d'évaluer leur niveau de conformité en matière de sécurité des données et de mettre en œuvre des mesures adéquates en vue de gérer la violation des données personnelles (III).

I. – UNE OBLIGATION GÉNÉRALE DE SÉCURITÉ DES DONNÉES PERSONNELLES APPLICABLE À TOUS LES RESPONSABLES DE TRAITEMENT

A. – Champ d'application

L'obligation de garantir la sécurité et la confidentialité des données personnelles s'applique à tous les responsables de traitements (13) dans le secteur privé et public. L'article 34 de la loi « Informatique et libertés » dispose que « *le responsable de traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ». Autrement dit, le responsable de traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données personnelles contre l'atteinte ou la violation des données, telles que la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, ainsi que toute autre forme de traitement illicite (14). Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

Cette obligation de sécurité et de confidentialité s'applique également aux sous-traitants agissant comme prestataires de services pour le compte du responsable de traitement. En vertu de l'article 35 de la loi « Informatique et libertés », « *le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34* ». Un sous-traitant ne peut traiter des données personnelles que sur instruction du responsable du traitement et pour son compte. Le contrat qui lie le sous-traitant au responsable du traitement doit préciser les obligations de sécurité qui s'imposent au sous-traitant. En cas de manquement du sous-traitant à son obligation de sécurité, c'est le responsable du traitement qui engage sa responsabilité.

B. – Des préconisations importantes de la Cnil en matière de sécurité des données personnelles

La Cnil a émis plusieurs recommandations en matière de sécurité des données personnelles. En 2010, elle a publié un premier guide qui contient des préconisations générales et des bonnes pratiques applicables à tous types de traitements en vue de garantir une sécurité de base aux données (15).

En 2012, la Commission a publié deux nouveaux guides sur les mesures de sécurité avancées applicables à des traitements complexes (16). Ces guides proposent une méthode permettant d'identifier et de traiter les risques liés aux traitements de données personnelles et un ensemble de mesures et de bonnes pratiques, sous forme de catalogue, pour aider les organismes à mieux gérer ces risques.

La Cnil place également la sécurité des données personnelles au cœur de son analyse sur le *cloud computing* dans la mesure où une faille de sécurité peut avoir des conséquences importantes sur le fonctionnement d'une entreprise qui externalise le traitement de données personnelles et peut nuire à sa relation avec ses clients. Parmi les mesures préconisées, la Cnil recommande de conduire une analyse des risques afin de déterminer les mesures de sécurité appropriées à exiger du prestataire ou à mettre en œuvre au sein de l'entreprise (17).

C. – Sanctions

Le manquement à l'obligation de sécurité des données personnelles est sanctionné par une peine de cinq ans d'emprisonnement et une amende pouvant aller jusqu'à 150 000 € (300 000 € en cas de récidive) (18). Ainsi, un responsable de traitement qui ne met pas en œuvre des mesures de sécurité, ou met en œuvre des mesures insuffisantes, peut être sanctionné par la Cnil en cas de violation des données, même s'il n'est pas soumis à une obligation de notifier celle-ci. À titre d'exemple, la Cnil a prononcé un avertissement à l'encontre d'une banque pour défaut de sécurité et de confidentialité des informations couvertes par le secret bancaire relatives aux clients de la banque alors même que le secteur bancaire n'est pas soumis à une obligation de notification (19).

D. – Vers un renforcement de l'obligation de sécurité

La proposition de règlement du 25 janvier 2012 comporte plusieurs mesures phares destinées à renforcer l'obligation de sécurité des données personnelles. Le responsable du traitement sera tenu à une obligation de sécurité conjointement avec le sous-traitant (20). En cas de manquement à l'obligation de sécurité, la responsabilité n'incombera plus seulement au responsable du traitement mais >

(13) L'article 3 de la loi « Informatique et libertés » définit un responsable de traitement comme « *la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens* » d'un traitement. (14) Voir l'article 17 de la directive n° 95/46/CE. (15) Voir le guide : La sécurité des données personnelles, éd. 2010, <www.cnil.fr/la-cnil/actualite/article/article/securite-des-donnees-personnelles-un-guide-pour-agir-et-un-test-pour-sevaluer/>. (16) Voir le guide : Sécurité avancée : méthode et le guide : Mesures pour traiter les risques sur les libertés et la vie privée, <www.cnil.fr/dossiers/banque-finance/actualites/article/deux-nouveaux-guides-securite-pour-gerer-les-risques-sur-la-vie-privee/>. (17) Voir Cnil, Recommandations pour les entreprises qui envisagent de souscrire à des services de *cloud computing*, publié le 25 juin 2012, <www.cnil.fr/la-cnil/actualite/article/article/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services>. (18) Article 226-17 du Code pénal. (19) Voir Défaut de sécurité de données confidentielles : avertissement pour la filiale Euro-Information et Crédit Mutuel-CIC, publié le 2 juillet 2012, <www.cnil.fr/la-cnil/actualite/article/article/defaut-de-securite-de-donnees-confidentielles-avertissement-pour-la-filiale-euro-information/>.(20) Article 30, proposition de règlement du 25 janvier 2012.

pourrait être imputée, le cas échéant, au sous-traitant.

Lorsqu'un traitement présente un risque particulier pour les droits et libertés des personnes du fait de la nature, de la portée ou de la finalité du traitement (par exemple, un traitement de données sensibles, la vidéosurveillance, un dispositif biométrique), le responsable du traitement (ou le sous-traitant agissant pour son compte) devra effectuer une analyse d'impact du traitement envisagé sur la protection des données personnelles (21).

Enfin, le responsable du traitement devra mettre en œuvre des mécanismes destinés à garantir que, par défaut, seules seront traitées les données personnelles nécessaires à chaque finalité spécifique du traitement et s'assurer que ces données ne sont pas collectées ou conservées au-delà de la durée nécessaire à la finalité (22). Ces mécanismes devront également garantir que les données ne sont rendues accessibles qu'à un nombre limité de personnes.

II. – UNE OBLIGATION DE NOTIFIER LES VIOLATIONS DE DONNÉES PERSONNELLES LIMITÉE AUX FOURNISSEURS DE SERVICES DE COMMUNICATION ÉLECTRONIQUE

A. – Un champ d'application limité

Le champ d'application de l'article 34 *bis* de la loi « Informatique et libertés » est doublement limité quant aux types de données concernées et quant aux personnes soumises à l'obligation de notification. En premier lieu, l'obligation de notification ne s'applique qu'aux données personnelles, c'est-à-dire à toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (23). Sont donc exclues du régime de la notification les données relatives aux personnes morales ou celles qui ne permettent pas d'identifier une personne physique (par exemple, des données chiffrées ou des statistiques).

Par ailleurs, l'article 34 *bis* ne s'applique qu'aux « *fournisseurs de services de communications électroniques accessibles au public* » (ci-après « *opérateurs de communications électroniques* »), autrement dit, les opérateurs déclarés auprès de l'Arcep (par exemple, les fournisseurs d'accès à internet et les opérateurs de téléphonie fixe et mobile) (24). Ne sont donc pas concernés les fournisseurs de services de la société d'information, tels que les banques en ligne, les commerçants en ligne ou les téléservices des administrations. Ainsi, l'article 34 *bis* ne s'applique que lorsque les conditions suivantes sont réunies :

– la mise en œuvre d'un traitement de données personnelles ;

– par un opérateur de communications électroniques ;

– dans le cadre de son activité de fourniture de services de communications électroniques (par exemple, les services de téléphonie ou d'accès à internet).

> En cas de violation des données personnelles, l'opérateur de communications électroniques doit en avertir la Cnil « *sans délai* ».

B. – Une définition large de la « violation de données »

L'article 34 *bis* définit la violation de données personnelles comme « *toute violation de la 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 de services de communications électroniques* ».

Selon la Cnil, toute violation qui ne concerne pas un traitement mis en œuvre par un opérateur de communications électroniques (par exemple, un virus informatique qui s'attaque aux PC des abonnés) ou ne concerne pas la fourniture au public de services de communications électroniques (par exemple, le piratage de la base de données des ressources humaines de l'opérateur) est exclue du champ de la loi. En revanche, une intrusion illicite dans la base de données des clients de l'opérateur, une faille technique affectant le site web du fournisseur et exposant les données bancaires de ses clients, ou encore une erreur dans la diffusion d'un e-mail confidentiel à un client sont considérées comme des violations de données personnelles.

C. – Un double régime de notification

1°/ Une notification obligatoire à la Cnil

En cas de violation des données personnelles, l'opérateur de communications électroniques doit en avertir la Cnil « *sans délai* ». La loi ne précise pas ce qu'il faut entendre par « *sans délai* » mais la Cnil interprète généralement cette notion comme signifiant « *dans les 24 heures qui suivent la constatation de la violation* ». La loi ne prévoit pas non plus de critères de gravité pour déterminer quelles violations doivent être notifiées, selon la quantité des données affectées ou le nombre de personnes concernées par la violation. Par conséquent, toutes les violations de données doivent être notifiées à la Cnil, quelle que soit leur gravité, dès l'instant où elles concernent des données personnelles qui sont traitées par un opérateur de communications électroniques dans le cadre des services qui sont offerts au public.

La notification à la Cnil s'effectue par lettre remise contre signature qui précise :

– la nature et les conséquences de la violation des données ;

– les mesures déjà prises ou proposées par l'opérateur pour y remédier ;

– les personnes auprès desquelles des informations supplémentaires peuvent être obtenues ;

– une estimation du nombre de personnes susceptibles d'être impactées par la violation en cause (lorsque cela est possible) (25).

2°/ Une notification sous condition aux personnes concernées

a) Les conditions de la notification aux personnes concernées

Lorsque la violation des données porte atteinte aux données personnelles ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur

(21) Article 33, proposition de règlement du 25 janvier 2012. (22) Article 23, proposition de règlement du 25 janvier 2012. (23) Article 2 de la loi n° 78-17 du 6 janvier 1978. (24) Article L. 33-1, alinéa 1, du Code des postes et communications électroniques. (25) Article 91-1 du décret n° 2005-1309 du 20 octobre 2005.

doit également avertir, sans délai, l'intéressé (26). Une violation est considérée comme affectant les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier lorsqu'elle est susceptible d'entraîner, par exemple, le vol ou l'usurpation d'identité, une atteinte à l'intégrité physique, une humiliation grave ou une réputation entachée en rapport avec la fourniture de services de communications accessibles au public (27).
D'après la Cnil, un opérateur de communications électroniques serait tenu d'informer ses abonnés, par exemple, en cas de piratage de sa base de données révélant les adresses e-mail ou les données de facturation de ses abonnés (28).

b) Le contenu de la notification des personnes concernées

La notification d'une violation de données aux personnes concernées peut être réalisée « *par tout moyen* » permettant à l'opérateur de communications électroniques d'apporter la preuve de l'accomplissement de cette formalité (29). Cette notification doit préciser :
– la nature de la violation de données ;
– les personnes auprès desquelles des informations supplémentaires peuvent être obtenues ;
– les mesures que l'opérateur recommande à la personne intéressée de prendre pour atténuer les conséquences négatives de cette violation.
Le décret d'application n'impose pas de forme obligatoire pour notifier les personnes concernées. Il semble donc possible d'informer les personnes concernées par lettre, par e-mail, voire même par SMS.

D. – La mise en œuvre de mesures de protection appropriées

La notification des personnes concernées n'est pas requise lorsque la Cnil constate que l'opérateur de communications électroniques a mis en œuvre des « *mesures de protection appropriées* » (30).
Pour que ces mesures de protection soient considérées comme « *appropriées* », elles doivent remplir deux critères, à savoir :
– rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès (31) ;
– et être appliquées aux données concernées par ladite violation (32).
La Cnil considère, par exemple, que le fait de chiffrer ou de crypter les données permettrait de rendre les données incompréhensibles aux tiers (33). Cependant, elle note que, si la clé de chiffrement ou de cryptage est compromise et qu'un tiers y a accès, cette mesure de protection deviendrait inefficace puisque le tiers en question pourrait déchiffrer les données.
S'il n'a pas informé les personnes concernées de ladite violation, l'opérateur de communications électroniques doit donc démontrer à la Cnil qu'il a mis en œuvre des mesures de protection appropriées en vue de remédier à cette violation et que ces mesures ont été efficacement appliquées aux données concernées par cette violation (34). En pratique, l'opérateur veillera à informer la Cnil sur les mesures de protection mises en œuvre en même temps qu'il lui notifie la violation de données (35).
L'information sur les mesures de protection appropriées peut se faire par tout moyen permettant d'apporter la preuve de la notification (36) et doit porter sur :
– le nom, le prénom, l'adresse et les coordonnées téléphoniques du responsable du traitement ;
– la description des mesures de protection ;
– les dispositions prévues et appliquées pour conférer une pleine efficacité à ces mesures ;
– le cas échéant, les références du dossier de formalités accomplies auprès de la Cnil préalablement à la mise en œuvre du traitement considéré ;
– l'accomplissement ou non de la formalité de notification aux personnes et, dans la négative, les raisons justifiant l'absence de notification (37).
Une fois informée, la Cnil dispose alors d'un délai de deux mois à compter de la réception complète des informations pour vérifier si les mesures de protection ont été mises en œuvre et appliquées, et pour apprécier la gravité de la violation (38). La loi ne précise pas les conditions de cette vérification, notamment, si la Commission peut se rendre sur place auprès du responsable du traitement pour vérifier la mise en œuvre effective des mesures de protection.
À l'issue du délai de deux mois, deux hypothèses sont possibles. Soit la Cnil n'apporte aucune réponse, ce qui équivaut à un constat de non-application au cas particulier des mesures de protection. Autrement dit, elle considère que les mesures de protection ne répondent pas aux exigences de l'article 34 de la loi « Informatique et libertés » sur la sécurité et la confidentialité des données et, par conséquent, l'opérateur de communications électroniques doit immédiatement informer les personnes concernées sur la violation des données (sauf s'il a déjà accompli cette formalité) (39). Soit la Commission considère que les mesures mises en œuvre par l'opérateur sont efficaces et elle l'en informe avant la fin du délai de deux mois. Dans ce cas, aucune notification aux personnes n'est exigée.
Si toutefois elle estime que la violation des données est grave, la Cnil peut mettre en demeure l'opérateur de communications électroniques d'informer les personnes concernées dans un délai maximal de un mois, indépendamment des mesures de protection qu'il a pu mettre en œuvre (40).
Enfin, il convient de noter que, même si elle constate l'efficacité des mesures de protection, il n'est pas interdit à l'opérateur de communications électroniques de notifier volontairement les personnes concernées dans un souci de bonne foi et de transparence à leur égard. De même, l'obligation qui est faite à un opérateur de communications électroniques d'informer ses abonnés de certains risques en matière de sécurité ne le dispense pas de prendre immédiatement les mesures appropriées pour remédier à tout nouveau risque imprévisible en matière de sécurité (41).

(26) Article 34 *bis*-II de la loi n° 78-17 du 6 janvier 1978. **(27)** Considérant 61 de la directive n° 2009/136/CE. **(28)** Voir *supra*, note 8. **(29)** Article 91-2 du décret n° 2005-1309 du 20 octobre 2005. **(30)** Article 34 *bis*-II, paragraphe 3, de la loi n° 78-17 du 6 janvier 1978. **(31)** Article 91-3 du décret n° 2005-1309 du 20 octobre 2005. **(32)** Article 34 *bis*-II, paragraphe 3, de la loi n° 78-17 du 6 janvier 1978. **(33)** Voir Cnil, *supra*, note n° 8. **(34)** Article 91-2 du décret n° 2005-1309 du 20 octobre 2005. **(35)** Voir Cnil, *supra*, note n° 8. **(36)** Article 91-2 du décret n° 2005-1309 du 20 octobre 2005. **(37)** Article 91-4 du décret n° 2005-1309 du 20 octobre 2005. **(38)** Article 91-5 du décret n° 2005-1309 du 20 octobre 2005. **(39)** Voir Cnil, *supra*, note 8. **(40)** Article 91-5 du décret n° 2005-1309 du 20 octobre 2005. **(41)** Considérant 20 de la directive n° 2002/58/CE.

E. – Sanctions

Le manquement à l'obligation de notifier en cas de violation des données est puni d'une amende de 300 000 € et jusque cinq ans d'emprisonnement (42). En cas de contrôle sur place, la Cnil qui constate l'absence de mesures de sécurité adéquates peut engager une procédure de sanction à l'encontre du responsable de traitement défaillant et peut ainsi prononcer une amende pouvant aller jusqu'à 150 000 € (300 000 € en cas de récidive). Ainsi, le responsable du traitement encourt deux sanctions différentes, d'une part, pour absence ou insuffisance de mesures de sécurité appliquées aux données et, d'autre part, pour absence de notification en cas de violation des données.

F. – Vers une généralisation de la notification des violations de données

À ce jour, l'obligation de notification d'une violation des données personnelles ne s'impose qu'aux opérateurs de communications électroniques. Toutefois, la proposition de règlement du 25 janvier 2012 « *relatif à la protection des données personnelles* » prévoit d'étendre le régime de notification à tous les responsables de traitements, quel que soit leur secteur d'activité. Ainsi, tous les responsables de traitements devront notifier à la Cnil en cas de violation des données, sans retard injustifié et, si possible, dans les 24 heures au plus tard après en avoir pris connaissance (43). Un délai de notification plus long sera possible mais sous condition de justifier ce délai.

Lorsque la violation est susceptible de porter atteinte à la protection des données personnelles ou à la vie privée, le responsable du traitement devra communiquer la violation sans retard indu aux personnes concernées (44). Cette notification ne sera pas exigée si le responsable du traitement prouve, à la satisfaction de l'autorité de contrôle, qu'il a mis en œuvre des mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. Lorsque le responsable du traitement omet de signaler ou de notifier une violation des données, ou omet de notifier la violation en temps utile ou de façon complète à la Cnil ou à la personne concernée, il encourt une sanction pouvant aller jusqu'à 2 % de son chiffre d'affaires annuel mondial (45).

III. – LA MISE EN ŒUVRE DE MESURES CONCRÈTES POUR GÉRER LA VIOLATION DE DONNÉES PERSONNELLES

Au vu des évolutions législatives en cours, le moment semble opportun de mettre en œuvre des mesures concrètes afin de gérer les violations de données. Sans vouloir être exhaustif, les mesures suivantes sont recommandées (46).

A. – Des mesures préventives

La mise en œuvre de mesures préventives permet d'anticiper d'éventuelles violations des données.

> À ce jour, l'obligation de notification d'une violation des données personnelles ne s'impose qu'aux opérateurs de communications électroniques.

1°/ Rédiger une politique de sécurité des systèmes d'information

La rédaction d'une politique de sécurité des systèmes d'information permet d'informer le personnel sur les risques identifiés en matière de traitement des données personnelles et les mesures de sécurité qu'il convient de respecter afin de limiter les risques de violation des données.

2°/ Identifier les incidents de sécurité

La classification des incidents de sécurité permet de mieux traiter les violations de données. Cette classification permet notamment de qualifier les violations de données selon des critères prédéfinis : la gravité et l'impact de la violation sur la vie privée des individus, le type de données affectées (par exemple, données d'identification, données financières, données de santé, etc.), les personnes concernées par l'incident (par exemple, salariés, consommateurs, clients, etc.), et les conséquences de la violation.

3°/ Créer une cellule de crise pour gérer les violations de données

La mise en place d'une cellule de crise permet d'organiser la gestion de la violation des données. La taille et la composition de la cellule de crise peuvent varier en fonction de l'organisme qui traite les données. La cellule de crise peut être composée de différentes personnes qui sont toutes impliquées dans la gestion et/ou la protection des données personnelles, telles que le correspondant informatique et libertés, le DSI ou RSSI, le responsable des ressources humaines, le responsable juridique, le responsable du département éthique et conformité et les dirigeants de l'entreprise. Le rôle et les attributions de chaque membre pourront être définis dans des règles de procédure.

4°/ Former et informer

La rapidité de réaction est primordiale en matière de sécurité des données. Une information claire, précise et préalable sur les mesures à prendre en cas de violation de données est nécessaire pour éviter de perdre du temps. En interne, les salariés doivent être informés sur la procédure à suivre en cas d'atteinte à la sécurité des données, notamment qui informer, quand déclencher l'alerte et quand effectuer une enquête interne.

B. – Un plan de réaction à la violation des données

Afin de faire face à l'éventualité d'une violation de données, il est recommandé de mettre en place un plan de réaction qui permet à l'organisme victime d'une violation de données de gérer la situation de crise et de remédier rapidement à ses effets. Ce document a pour but de décrire, étape par étape, les mesures à mettre en œuvre en cas de violation de données. Ci-dessous sont décrites les principales étapes de la gestion d'une violation de données.

1°/ Identifier l'incident de sécurité

En premier lieu, il convient d'identifier l'incident qui est éventuellement à l'origine d'une violation des données person-

(42) Article 226-17-1 du Code pénal. **(43)** Article 31 de la proposition de règlement du 25 janvier 2012. **(44)** Article 32 de la proposition de règlement du 25 janvier 2012. **(45)** Article 79(6) de la proposition de règlement du 25 janvier 2012. **(46)** Les mesures énoncées ci-dessous n'ont pas vocation à être exhaustives et sont énoncées purement à titre informatif. Il va de soi que chaque organisme doit mettre en œuvre des mesures de sécurité adaptées à sa structure, à sa taille et aux traitements de données qu'il effectue.

nelles. Il convient ensuite d'analyser et de décrire cet incident dans un rapport d'analyse, puis d'en informer sans tarder la cellule de crise afin qu'elle puisse déterminer s'il s'agit d'une violation des données et, le cas échéant, déclencher la procédure à suivre en cas de violation des données personnelles.

2°/ Recueillir toutes les informations nécessaires sur l'incident en question

Afin de déterminer s'il y a eu violation des données, il convient de réunir toutes les informations nécessaires sur l'incident en question, telles que :
– les catégories de données affectées ;
– une estimation de la quantité de données perdues, volées ou révélées de manière illicite ;
– le ou les systèmes d'information concernés ;
– la catégorie, le nombre et la situation géographique des individus affectés par la violation de données ;
– les conséquences de la violation des données.

3°/ Prendre des mesures immédiates

Selon la gravité de la violation des données, il peut être nécessaire de prendre certaines mesures techniques et organisationnelles immédiates, telles que le blocage des données, l'interdiction ou la restriction d'accès aux données, ou l'arrêt temporaire du traitement.
L'organisme peut vouloir publier un communiqué de presse afin de répondre aux questions des médias ou afficher une « foire aux questions » sur son site internet afin de gérer d'éventuelles requêtes des personnes concernées.

4°/ Notifier l'autorité compétente de la violation des données

Enfin, l'une des étapes les plus importantes dans la gestion d'une violation de données est de notifier à l'autorité nationale compétente, voire aux personnes concernées, lorsque cela est exigé par la loi. Il convient donc d'identifier le ou les pays où s'est produite la violation des données et de mettre en œuvre une procédure de notification (délai, forme, contenu) conformément au droit national applicable.

C. – Le bilan d'une violation des données

À l'issue d'une violation des données personnelles, il est conseillé de faire le bilan de celle-ci et d'identifier les éventuelles faiblesses dans le dispositif de sécurité de l'entreprise afin de renforcer celui-ci et de limiter autant que possible d'autres violations à l'avenir. Le bilan doit aussi permettre à l'organisme d'améliorer son plan de réaction et de corriger d'éventuelles lacunes dans son dispositif de gestion des violations de données. Enfin, dans certains pays, comme en France, il est obligatoire de maintenir un inventaire des violations de données.

CONCLUSION

En l'état actuel du droit, le régime de la notification des violations de données se limite au secteur des communications électroniques. Cependant, ce régime pourrait bientôt être étendu à tous les secteurs d'activité une fois que le nouveau règlement européen sur la protection des données personnelles entrera en vigueur. La question qui se pose alors est de savoir comment ce nouveau régime va se marier avec le régime actuel de la directive n° 2002/58/CE (applicable aux opérateurs de communications électroniques). En effet, les opérateurs de communications électroniques risquent de se voir appliquer deux régimes juridiques distincts, ce qui pourrait soulever des difficultés pratiques en cas de divergences entre ces deux textes. ◆