LA NOTIFICATION DES FAILLES DE SECURITE : VERS UNE OBLIGATION DE DENONCIATION ?

11 décembre 2012

Introduction

A la fin de cet été, les utilisateurs de Facebook dénonçaient la révélation de leurs messages privés aux yeux de tous, sur le réseau social. Véritable bug de Facebook ou hallucination collective ? Telle était alors la question sur laquelle la CNIL est intervenue, en sommant le géant des réseaux sociaux d'éclaircir cette situation.

Cet évènement, qui est à prendre très au sérieux, aura eu pour effet de mettre au cœur de l'actualité l'inéluctable risque de révélation ou d'altération de données à caractère personnel.

C'est dans un objectif de prévention de ces risques qu'a été instaurée en 2011, avec l'article 34 bis de la Loi Informatique et Libertés, une obligation de notification (à la CNIL et aux personnes concernées) des violations de données à caractère personnel. Cette obligation pèse uniquement, pour le moment, sur les fournisseurs de services de communications électroniques. L'obligation sera, à terme, élargie à tout responsable de traitement.

Cela s'apparente à une obligation légale de dénonciation – en fait d'auto-dénonciation – auprès de la CNIL (qui peut transmettre au Parquet). Surprenant, mais précisons qu'il existe d'autres obligations de ce type en droit pénal français.

La nouveauté ici, c'est que l'obligation trouve à s'appliquer quelle que soit la personne qui est à l'origine de la violation :

- soi-même (en raison d'une simple imprudence, une perte de matériel, ou d'une négligence) ;

- d'un tiers connu ou non (piratage, introduction d'un virus, etc.).

Avant d'aborder la portée juridique de ce nouveau dispositif de saisine de la CNIL (§2), il convient de se demander si notre droit connaît déjà l'obligation de dénonciation (§1).

1. L'obligation de dénonciation existe-t-elle déjà dans notre système juridique ?

La réponse est positive. La dénonciation désigne, en droit pénal, l'acte par lequel un citoyen informe les autorités judiciaires ou administratives d'une infraction commise par autrui. Lorsque cet acte émane de la victime, il ne s'agit pas d'une dénonciation mais d'une plainte.

La dénonciation pose d'importantes questions éthiques, morales, et donc juridiques. En droit français, il existe un délit de non-dénonciation, qui sanctionne le manquement à une obligation préexistante de dénonciation.

Chaque citoyen peut (doit) se poser la question de savoir dans quelle(s) hypothèse(s) la non-dénonciation d'une infraction dont une personne a été témoin est sanctionnée par notre droit pénal.

Toutes les infractions ne sont pas concernées par cette obligation. L'article 434-1 du Code pénal prévoit que la non-dénonciation d'un crime, « *dont il est encore possible de prévenir ou de limiter les effets ou dont les auteurs sont susceptibles de commettre de nouveaux crimes qui pourraient être empêchés* », constitue un délit.

De surcroit, le Code pénal (art. 434-3) prévoit que le fait, pour quiconque ayant eu connaissance de privations, de mauvais traitements ou d'atteintes sexuelles infligés à un mineur de moins de quinze ans ou infligés à des personnes fragiles, de ne pas en informer les autorités judiciaires ou administratives constitue un délit de non-dénonciation.

Ce délit de non-dénonciation ne concerne que les cas susvisés ; les délits autres que ceux prévus à l'article 434-3 du Code pénal et les contraventions n'ont pas à être dénoncés.

A l'inverse, les officiers publics et fonctionnaires ayant connaissance d'un crime ou d'un délit dans l'exercice de leurs fonctions sont tenus d'informer sans délai le procureur de la République[1]. Ceux-ci doivent donc dénoncer tous les délits dont ils ont connaissance dans le cadre de leur fonction (et non pas seulement ceux prévus à l'article 434-3 du Code pénal évoqués ci-dessus). Ce n'est pas, en principe, aux officiers publics ou aux fonctionnaires de décider de l'opportunité des poursuites, mais au Procureur de la République.

Toutes les personnes ne sont pas également concernées par l'obligation légale de dénonciation :

- Les parents et les proches de l'auteur ou du complice sont exemptés de cette obligation. Cette exemption n'est cependant pas applicable lorsque le crime est commis sur un mineur de moins de quinze ans.

- Les personnes astreintes au secret professionnel sont elles aussi exemptées[2]. Toutefois, bien que tenues au secret professionnel, elles ont néanmoins la possibilité de choisir en conscience entre la dénonciation et le secret. Pour cela, il faut toutefois que la connaissance du crime ait bien eu lieu dans le cadre étroit du secret professionnel (Cass. Crim., 27 février 2001, Juris-Data n° 2001-84532).

Puisqu'il y a dans notre droit positif une obligation de dénonciation, pour une infraction donnée et une personne non exemptée qui en a connaissance, que doit contenir cette dénonciation ?

L'obligation de dénonciation d'un crime ou d'un délit impose seulement la révélation de l'existence du crime ou du délit. L'obligation de dénonciation (signaler la commission d'un acte pénalement répréhensible) n'est pas une obligation de délation (imputer un fait répréhensible à une personne nommément désignée), comme le rappelle la jurisprudence (Cour de cassation, Chambre Criminelle, arrêt du 2 mars 1961, Dalloz 1962). Pour autant, la personne ayant déclaré connaître les auteurs de l'infraction est tenue de répondre aux questions qui lui sont posées à cet égard.

Les personnes commettant le délit de non-dénonciation de crime[3] ou de non-dénonciation d'un délit[4] s'exposent à trois ans d'emprisonnement et 45 000 euros d'amende. Lorsque le crime visé constitue une atteinte aux intérêts fondamentaux de la nation ou un acte de terrorisme, la peine est portée à cinq ans d'emprisonnement et 90 000 euros d'amende[5].

A contrario, il importe de souligner que les dénonciations intempestives ou fausses sont dites « *calomnieuses* » et font encourir de lourdes peines à leur auteur[6] (cinq ans d'emprisonnement et 45 000 euros d'amende).

C'est à la lumière du contexte juridique ci-dessus rappelé qu'il convient de se demander quelle portée peut être donnée à cette nouvelle obligation de notifier à la CNIL (et le cas échéant aux personnes concernées) les violations de données à caractère personnel.

En d'autres termes, s'agit-il d'une obligation de s'auto-dénoncer ou de dénoncer son employeur ?

2. Quelle est la portée juridique de la notification à la CNIL des violations des données personnelles ?

Une directive européenne de 2002[7] dite « Paquet Télécom » institue une obligation de notification des violations de données à caractère personnel à la CNIL et, le cas échéant, aux personnes concernées. Cette obligation a été transposée dans la loi dite « Informatique et Libertés »[8] de 1978 bien qu'elle ne concerne pas toutes les entreprises mais seulement les fournisseurs de services de communications électroniques[9].

Désormais, toutes les violations de données[10] à caractère personnel subies par le responsable de traitement concernant les fournisseurs de services de télécom doivent être systématiquement notifiées à la CNIL, et ce, quelle que soit leur gravité.

A ce jour, il existe un projet de règlement européen, qui sera donc d'application immédiate à la différence d'une directive, ayant pour objet d'élargir ce dispositif de « ***signalement*** » à tous les secteurs d'activités et à toutes les entreprises.

Plus précisément, tous les responsables de traitement de données qui subiront une destruction, une perte, une altération, une divulgation, ou un accès non autorisé à des données à caractère personnel, qu'il s'agisse d'un acte de malveillance, d'une erreur ou encore d'une fausse manipulation[11], devront en informer la CNIL.

Cette dernière devra faire face à un nouveau flux d'informations, vraisemblablement quotidien, puisque toutes les violations doivent lui être notifiées, quelle que soit leur gravité. La notion de violation de sécurité recouvre un ensemble de situations pratiques extrêmement différentes : la perte d'un ordinateur portable ou d'une clé USB comportant des données à caractère personnel, celle d'un PDA ou d'un téléphone portable, ou encore le piratage d'un réseau ou même une imprudence permettant à un tiers non habilité d'accéder à un système d'informations. Cela rend cette nouvelle obligation européenne assez difficile à circonscrire dans un cadre raisonnable et donc difficilement praticable au quotidien.

La CNIL devra également vérifier que les personnes concernées ont également été informées par le responsable de traitement lorsque la loi l'exige. En effet, il est prévu que les personnes concernées soient également informées des violations qui portent atteinte aux données à caractère personnel les concernant, lorsqu'elles sont susceptibles d'entraîner

par exemple le vol ou l'usurpation d'identité, une atteinte à l'intégrité physique, une humiliation grave ou une réputation entachée.

Lorsqu'elle est requise, la notification aux personnes doit être effectuée sans délai, à l'instar de la notification qui doit être faite à la CNIL.

Le fait, à ce jour, pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la CNIL est puni de cinq ans d'emprisonnement et de 300 000 € d'amende[12].

Dès lors, la question de déterminer si nous sommes en présence d'une nouvelle obligation légale de dénonciation revêt une acuité toute particulière. Le risque est, en effet, particulièrement élevé.

Afin d'éclairer l'analyse, voyons les hypothèses qui peuvent être distinguées.

(i) On peut concevoir que le responsable de traitement ne soit pas à l'origine de la violation de données personnelles ; elle ne lui serait pas imputable. En ce sens, le responsable de traitement en est la victime. Dans ce cas, on peut considérer que la violation de données trouvera son origine dans :

- l'action délibérée d'un tiers (identifié ou non) qui commettrait un acte frauduleux, dans le but de porter atteinte à un système de traitement automatisé de données, ce qui est incriminé par les articles 323-1 et suivants du Code pénal ;

- l'action fautive d'un préposé (un salarié) ou un sous-traitant qui serait susceptible d'engager sa propre responsabilité pénale.

(ii) On peut aussi concevoir que la victime de l'atteinte aux données, ait commis une faute qui soit à l'origine de son propre dommage. Cela suppose, par définition, que la violation de données trouve son origine dans un acte involontaire tel qu'une erreur de manipulation, une négligence ou encore une imprudence du responsable de traitement.

Dans tous les cas, le responsable de traitement se trouve débiteur d'une d'obligation légale de se signaler comme « victime » des actes mentionnés ci-dessus.

(iii) On peut enfin concevoir que l'existence de cette obligation légale de notification pourrait contrebalancer le phénomène trop souvent constaté du silence des victimes d'agression, silence qui empêche ou rend plus difficile les poursuites.

Outre le fait que ce silence entrave la poursuite des auteurs présumés, il conduit à une sous-estimation du phénomène délictuel (l'ampleur de la fraude en quelque sorte) dans le domaine des nouvelles technologies. Il s'agit malheureusement d'un phénomène répandu, qui ne se cantonne pas à ce seul secteur d'activité.

La règle est simple : désormais, les victimes de violations de données personnelles devront parler. Elles devront signaler l'infraction dont elles sont victimes. Le silence n'est plus de mise. A défaut, c'est la victime elle-même qui pourrait être condamnée. Cela pose effectivement de nombreuses difficultés, notamment quant à l'exercice des droits de la défense : comment considérer qu'une personne peut se défendre librement et efficacement si elle est obligée de se dénoncer, de s'accuser. En principe, les droits de la défense autorisent, a minima, à garder le silence. A titre d'illustration de l'exercice et de l'importance des droits de la défense (droits fondamentaux ayant une valeur constitutionnelle), rappelons qu'il existe une jurisprudence constante de la Cour de cassation issue de deux arrêts de principe rendus en mai 2004 ; cette jurisprudence autorise un salarié à soustraire des documents appartenant à son employeur afin de les produire en justice à titre de preuve, dans un procès qui les oppose, sans encourir une condamnation pour vol sur le fondement de l'article 311-1 du Code pénal.

Or, nous sommes en présence d'une obligation légale de se signaler comme victime… et aussi, potentiellement, comme auteur d'infraction. Certains y voient une obligation (inique) de s'auto-incriminer.

En toute hypothèse, et c'est le côté positif du sujet, cela devrait faciliter la mise en œuvre de la répression, via des enquêtes mieux ciblées susceptibles d'aboutir à des poursuites plus efficaces. D'autant plus que dans le domaine des investigations numériques, ce sont les premières heures qui comptent.

Nous pensons également que cela devrait permettre de mieux évaluer l'importance du phénomène délictuel (la CNIL disposera de bien meilleures statistiques). Il sera plus facile, également, de mesurer l'efficacité des mesures prises[13] pour y remédier.

Rappelons à ce titre que le responsable de traitement est censé 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* ». Il existe ainsi une notion d'efficacité des mesures prises, dans le sens où ces mesures doivent être adaptées donc efficaces eu égard au risque encouru effectivement.

C'est bien cette obligation de principe qui vient à être renforcée par l'article 34 bis de la loi Informatique et libertés créant l'obligation de notification des violations de données. Aujourd'hui, telle qu'elle semble être conçue, l'obligation de sécurité des données personnelles s'apparente pratiquement à une véritable obligation légale de résultat.

Ne s'agirait-il pas, en ce sens, d'une responsabilité dite objective, c'est-à-dire sans faute ?

Tel est souvent le cas dans le domaine de la sécurité, surtout à notre époque où l'on tolère de moins en moins l'aléa, où le besoin fondamental de sécurité devient irrépressible. Notre époque semble rendre nécessaire la désignation d'un responsable à chaque sinistre. Plus spécifiquement, il s'agit d'un responsable et de son assureur. En effet, la préoccupation d'indemniser les victimes que sont les personnes dites « concernées » par les données personnelles, et de faire face aux conséquences financières de la violation, devient majeure (dans certains cas, les coûts de notification peuvent représenter des dizaines de milliers d'euros).

Si l'on raisonne a contrario, prendre toutes les mesures « *utiles pour préserver la sécurité des données* » pourrait signifier que lorsqu'une donnée aura été déformée, endommagée ou qu'un tiers non autorisé y aura eu accès, c'est nécessairement que l'une des mesures utiles à la sécurité de cette donnée n'a pas été prise en amont par le responsable de traitement. Selon nous, la mesure qui aurait été *utile* est celle qui aurait empêché que le sinistre n'arrive. Utile : qui a un rôle efficace, qui est nécessaire et adapté.

En ce sens, se conformer aux (meilleures) règles de l'art dans le domaine de la sécurité des systèmes d'information aurait pour effet de réduire très significativement la probabilité de survenance d'un sinistre (on parle alors de sinistralité dite « résiduelle » donc plus facilement assurable) ; toutefois, cela n'exclut pas que le responsable de traitement soit tenu responsable de ce sinistre pour le cas où par extraordinaire il surviendrait.

Ainsi, dès que la violation de données trouve son origine dans le fait d'un tiers, non seulement la victime doit informer la CNIL mais elle s'expose à des poursuites au titre de l'article 34 de la loi Informatique & Libertés pour ne pas avoir pris toutes les mesures utiles à la sécurité des données. Cela revient à obliger le responsable de traitement à s'auto-dénoncer. En cas de violation de données, ce dernier s'expose donc à être condamné pour absence de notification s'il demeure silencieux, ou pour absence de sécurité, s'il parle... Est-ce viable pour lui ?

Dans ce contexte de renchérissement des obligations pesant sur le responsable du traitement, rappelons que ce dernier doit tenir à jour un inventaire des violations de données à caractère personnel, notamment de leur modalités, de leur effet et des mesures prises pour y remédier. Il lui appartient de surcroît de conserver cet inventaire à disposition de la CNIL.

Aujourd'hui, il ne s'agit que des opérateurs de communications électroniques. Demain, il s'agira de tous les responsables de traitement de données personnelles.

En substance, celui qui collectera et tirera profit de la valeur économique des données personnelles en sera gardien et sera donc débiteur d'une obligation de résultat s'agissant de leur sécurité. Pour être pragmatique, il convient d'anticiper cette transition, en prévoyant dès à présent des dispositifs technico-juridiques de maîtrise des risques. Il s'agira de pouvoir rapporter la preuve de la bonne application de la loi à chaque instant. S'organiser en fait.

Nous nous dirigeons ainsi vers une approche qualitative de la gestion et du traitement de l'information (le nerf de la guerre économique), approche qui d'ailleurs accroît encore la valeur économique des données, et donc mécaniquement, le résultat de ceux qui en vivent. Il pourrait bien s'agir d'un cercle vertueux où on pourrait aller jusqu'à dire que cela permettrait la mutualisation des cas de violation de données, et donc, par voie de conséquence, un partage des savoirs permettant de mieux y faire face.

Pour y parvenir, les responsables de traitement auront tout intérêt à s'appuyer sur leur CIL, interne ou externe.

Arnaud TESSALONIKOS
Avocat Associé

Informatique & Réseaux
Correspondant Informatique et Libertés

COURTOIS LEBEL
15, rue Beaujon
75008 Paris
T : +33 1 58 44 92 92 M : + 33 6 29 68 95 04 F : +33 1 58 44 92 58

[1] Article 40 du Code de procédure pénale.
[2] Article 226-14 du Code pénal.
[3] Prévu à l'article 434-1 du Code pénal.
[4] Prévu à l'article 434-3 du Code pénal.
[5] Article 434-2 du Code pénal.
[6] Article 226-10 du Code pénal : « *La dénonciation, effectuée par tout moyen et dirigée contre une personne déterminée, d'un fait qui est de nature à entraîner des sanctions judiciaires, administratives ou disciplinaires et que l'on sait totalement ou partiellement inexact, lorsqu'elle est adressée soit à un officier de justice ou de police administrative ou judiciaire, soit à une autorité ayant le pouvoir d'y donner suite ou de saisir l'autorité compétente, soit aux supérieurs hiérarchiques ou à l'employeur de la personne dénoncée, est punie de cinq ans d'emprisonnement et de 45000 euros d'amende*. »
[7] Directive 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).
[8] Loi n° 78-17 du 6 janvier 1978 modifiée, comprend donc un nouvel article 34bis, ainsi rédigé :
« **I. -** *Le présent article s'applique au traitement des données à caractère personnel mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de données et d'identification.*
Pour l'application du présent article, on entend par violation de données à caractère personnel 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 au public de services de communications électroniques.
***II.** - En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit, sans délai, la Commission nationale de l'informatique et des libertés.*

Lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur avertit également, sans délai, l'intéressé.
La notification d'une violation des données à caractère personnel à l'intéressé n'est toutefois pas nécessaire si la Commission nationale de l'informatique et des libertés a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation.
A défaut, la Commission nationale de l'informatique et des libertés peut, après avoir examiné la gravité de la violation, mettre en demeure le fournisseur d'informer également les intéressés.
***III. -** Chaque fournisseur de services de communications électroniques tient à jour un inventaire des violations de données à caractère personnel, notamment de leurs modalités, de leur effet et des mesures prises pour y remédier et le conserve à la disposition de la commission.* »

[9] Des mesures d'application de la loi ont été précisées par un décret n° 2012-436 du 30 mars 2012.
[10] CNIL, rapport d'activité 2011, publié le 10 juillet 2012, page 17.
[11] Imputable à un salarié ou à un tiers autorisé, par exemple.
[12] Article 226-17-1 du Code pénal.
[13] Mesures d'ordre législatives, répressives, organisationnelles ou encore techniques prises par l'Etat, la CNIL et les responsables de traitements.