Données bancaires et durée de conservation : la CNIL avertit publiquement un e-commerçant à l'issue d'un contrôle

[DONNEES PERSONNELLES]
Délibération de la formation restreinte n° 2012-214 du 19 juillet 2012

Par une délibération du 19 juillet 2012, la formation restreinte de la CNIL a prononcé à titre de sanction un avertissement public à l'encontre d'un important acteur de l'e-commerce, essentiellement fondé sur les conditions de traitement et de conservation des données bancaires des clients.

Cette sanction a été prononcée à l'issue d'une phase de contrôle engagée dans le cadre du programme annuel des contrôles de la CNIL (et donc en dehors de toute plainte) ; le e-commerce fait partie des secteurs inclus dans le programme de contrôle 2012.

La décision de la CNIL comporte plusieurs indications importantes sur les conditions de traitement des données bancaires des clients par les sites de e-commerce (i) et sur la durée de conservation de l'ensemble des données clients, dont les données bancaires (ii).

(i) Concernant les conditions de conservation des données bancaires, la CNIL prend position officiellement (pour la première fois, à notre connaissance) sur la pratique consistant à enregistrer les données bancaires du client pour la réalisation de la première transaction sur le site de e-commerce mais également en vue de la réalisation d'éventuelles transactions ultérieures. Ce service en fort développement permet aux clients de ne pas avoir ressaisir les données à chaque nouvelle commande.

En l'espèce, l'organisme contrôlé mettait cette pratique en œuvre moyennant une information préalable des clients, tout en leur réservant la possibilité de supprimer les données bancaires qu'ils avaient initialement enregistrées. La CNIL, fidèle à sa position traditionnelle selon laquelle les données bancaires ne peuvent par principe être conservées au-delà de l'exécution de chaque transaction, considère que ce service, dont elle reconnaît l'utilité et l'intérêt pour les clients, ne peut être fourni sans consentement exprès de ces derniers. L'on retrouve ici le principe inscrit dans la nouvelle norme simplifiée 48 (sur le traitement des fichiers clients) publiée en juillet 2012. La CNIL précise dans sa décision de sanction que le caractère « sensible » des données bancaires impose des « garanties renforcées » et que « *la simple information sur la conservation de ces données associée à une faculté d'effacement ex post ne sauraient constituer de telles garanties* ».

Le principe affirmé par la CNIL dans cette décision (et la norme simplifiée 48) sur l'exigence du consentement exprès concernant la conservation des données bancaires a, en termes d'efficacité, une portée assez théorique à l'égard des clients des sites de e-commerce. L'on sait en effet que le problème central en matière de conservation des données bancaires porte avant tout sur *le niveau de sécurité* mis en œuvre lors de la conservation (cf. plus bas). Or, l'obtention du consentement exprès des clients à la conservation de ces données, au-delà de l'exécution de la première transaction, ne leur apporte aucune garantie supplémentaire en termes de sécurité. La position de la CNIL n'en est pas moins clairement affirmée et les sites qui ne se mettraient pas en conformité (par exemple, par l'insertion d'une case à cocher dans les formulaires de collecte) s'exposent donc à des sanctions.

En l'espèce, la CNIL relève par ailleurs une insuffisance des mesures de sécurité mises en œuvre pour la conservation des données bancaires des clients du site contrôlé. En effet, les agents de la CNIL ont constaté que les cryptogrammes visuels transmis par les clients pour la réalisation des paiements ne faisaient pas l'objet d'une purge régulière suivant la réalisation de l'opération de paiement, les données bancaires (noms des titulaires de cartes, numéros, durée de validité et cryptogramme) étant conservées en clair (ou en tout cas, sans mesure de cryptage complexe) dans une base unique. Sur ces points, la CNIL rejette l'argument de la société contrôlée faisant valoir l'absence d'intrusion dans ses systèmes à ce jour et décide que, compte tenu de la sensibilité des données stockées, celle-ci a méconnu les termes de l'article 34 de la loi Informatique et Libertés imposant au responsable de traitement de prendre toute mesure utile « *au regard de la nature des données et des risques présentés par le traitement* ».

(ii) La durée de conservation des données clients (incluant les données des cartes bancaires) constitue le second axe de la décision de sanction. Etant rappelé que la durée précise de conservation des données clients n'est fixée ni par la loi, ni par la norme simplifiée 48 (dans son ancienne version alors applicable), il appartient aux responsables de traitement de définir, conformément à l'article 5 de la loi Informatique et Libertés, la durée « *nécessaire* » de conservation au regard de la finalité du traitement, ce qui constitue généralement une question complexe (notamment au regard des durées de prescription). En l'espèce, le site contrôlé détenait des données clients remontant à 1999 et correspondant à des comptes inactifs depuis cette date.

La CNIL admet que, même en présence d'un compte client inactif depuis plusieurs années, le responsable de traitement peut disposer d'un intérêt légitime à conserver les données pendant une durée longue, y compris pour des raisons liées au marketing (entretenir ou relancer la communication commerciale avec les clients inactifs répertoriés).

En revanche, la CNIL fait grief au site contrôlé de ne pas avoir établi *une politique de conservation définissant les durées précises de conservation* selon que les comptes sont actifs ou non et de ne pas avoir établi *une procédure de purge régulière (manuelle ou automatique)*. Elle retient par conséquent que le site n'a pas respecté l'article 5 de la loi Informatique et Libertés disposant que la durée de conservation de données permettant l'identification des personnes ne peut excéder la durée nécessaire aux finalités pour lesquelles elle est collectée.

Le grief vaut également pour les données des cartes bancaires mais la CNIL précise sa position en admettant que, dans le cadre de la relation entre un commerçant et ses clients, la durée de conservation doit nécessairement être supérieure à 13 mois (compte tenu du délai de prescription fixé par le code monétaire et financier en matière de fraude) tout en demeurant limitée. L'on retrouve ici le délai de 13 mois également visé dans la nouvelle norme simplifiée 48, publiée par la CNIL quelques semaines avant la décision ici commentée et auxquels les sites e-commerce peuvent désormais se référer [Voir article Netcom Septembre 2012].

Au terme de la décision, l'organisme contrôlé ne s'est pas vu infliger de sanction financière par la formation restreinte de la CNIL qui semble considérer que la publicité donnée à l'avertissement constitue une mesure plus efficace.

Hélèna DELABARRE