nomosnetcom.fr **Septembre 2016**

Mise en demeure par la CNIL de se conformer à la loi Informatique et Libertés

[DONNEES PERSONNELLES]
Décision du 30 juin 2016

Le 10 juillet 2015, la société Microsoft Corporation lançait la commercialisation de son nouveau système d'exploitation dénommé « Windows 10 ». A la suite de ce lancement, des journalistes et hommes politiques ont alerté la CNIL sur l'existence d'une potentielle collecte massive de données personnelles des utilisateurs du logiciel.

La CNIL a mené 7 constats en ligne entre le 11 avril et le 29 juin 2016.

Suite à ces vérifications, la CNIL a fait état de plusieurs manquements à la loi Informatique et Libertés :

- l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données n'aurait pas été respectée : Microsoft Corporation propose un système de télémétrie, qui ne peut être désactivé, et qui vise à améliorer les services en résolvant notamment les problèmes liés à l'utilisation du logiciel. La CNIL constate cependant que la majorité des données collectées par Microsoft Corporation dans le cadre de ce service n'est pas « *directement nécessaire au fonctionnement du système d'exploitation* », ce qui constitue un manquement à l'article 6-3 de la loi du 6 janvier 1978, qui dispose que les données collectées doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* » ;

- sur l'obligation d'informer les personnes : chaque personne dont les données sont transférées dans un pays non membre de la Communauté européenne doit notamment être informée, en vertu de l'article 32-I de la loi Informatique et Libertés et du décret d'application du 20 octobre 2005, de la nature des données transférées et de la finalité du transfert envisagé. Or, la CNIL constate que ces informations ne sont pas fournies aux utilisateurs du logiciel Windows 10, ce qui constitue un manquement à l'article précité ;

- sur les dispositions de l'article 32-II de la loi Informatique et Libertés telles qu'interprétées par la CNIL dans sa délibération n°2013-378 du 5 décembre 2013. En effet, la CNIL a relevé que Microsoft Corporation installe des cookies sur le terminal des utilisateurs de son logiciel Windows 10, sans obtenir préalablement leur consentement. La Commission constate en outre que les informations dispensées aux utilisateurs ne sont pas satisfaisantes, ces cookies étant installés sans que les utilisateurs ne soient informés de leur finalité et sans qu'un mécanisme valable d'opposition ne soit mis en œuvre par Microsoft Corporation ;

- sur l'obligation d'assurer la sécurité des données : tout utilisateur de Windows 10 dispose de la faculté de créer un code PIN constitué de 4 chiffres permettant l'ouverture de la session et l'accès « *à tous les services en ligne de Microsoft, et notamment à sa boite de messagerie ainsi qu'à son compte Microsoft qui recense les achats* ». La CNIL constate que ce mot de passe peut être constitué de 4 chiffres identiques, et que l'authentification n'est pas suspendue dans la durée après 20 tentatives infructueuses de connexion. La CNIL considère que la sécurité et la confidentialité des données des utilisateurs ne sont pas assurées, et que ces faits constituent un manquement à l'article 34 de la loi Informatique et Libertés ;

- sur l'obligation d'accomplir les formalités préalables à la mise en œuvre des traitements de lutte contre la fraude et d'exclusion : la Déclaration de confidentialité de Microsoft Corporation précise que, dans un but de sécurité et de lutte contre la fraude, elle peut supprimer des contenus et des communications. Par lettre du 30 mai 2016 adressée à la CNIL, Microsoft précise en outre qu'elle se réserve « *le droit d'interdire à des utilisateurs qui se livrent à des actes de fraude* » d'utiliser ses services. Or, la CNIL constate que Microsoft Corporation n'a effectué aucune demande d'autorisation, alors que l'article 25 de la loi Informatique et Libertés soumet à autorisation tout traitement susceptible d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat ;

- sur l'obligation de disposer d'une base légale pour transférer des données à caractère personnel hors de l'Union Européenne :la CNIL relève que la Déclaration de confidentialité de Microsoft Corporation énonce notamment que les données recueillies peuvent être stockées et traitées aux Etats-Unis, conformément aux principes du « Safe Harbor ». Or, la CNIL rappelle qu'il n'était plus possible à l'époque des faits de procéder à un transfert de données personnelles vers les Etats-Unis sur la base du Safe Harbor, suite à la décision de la CJUE du 6 octobre 2015 (sauf adoption de Clauses contractuelles types, ou, au sein d'une entreprise ou d'entreprises d'un même groupe, de règles internes d'entreprise (BCR)).

Ainsi, Microsoft Corporation dispose d'un délai de 3 mois à compter de la notification de la décision pour conformer son logiciel Windows 10 à la loi Informatique et Libertés.

La CNIL estime que la gravité de ces atteintes à la loi Informatique et Libertés, la taille de l'entreprise concernée et l'importance du nombre de personnes concernées (plus de 10 millions en France) justifient la publication de la mise en demeure adressée à Microsoft Corporation.

Antoine JACQUEMART