# Opérateurs de Services Essentiels : les collectivités territoriales ne sont pas exemptées de la Directive NIS

Le 26 février 2018 a été votée la Loi n°2018-133 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, dont le Titre Ier comporte les dispositions tendant à transposer la directive NIS. La directive 2016/1148 du Parlement européen du 6 juillet 2016 concerne des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Aussi appelée directive SRI ou directive NIS (pour Network Information Security), elle définit des mesures dans le but d'obliger les Etats membres à adopter une stratégie nationale en la matière. Pour atteindre ce but, la directive crée notamment une nouvelle catégorie d'acteurs qui devront être soumis à des standards plus élevés en matière de sécurité informatique. Il s'agit des Opérateurs de Services Essentiels (OSE). La directive NIS fait mention d'une série de secteurs au sein desquels les Etats membres devront identifier des OSE, parmi lesquels figurent l'énergie, la santé, la fourniture et la distribution d'eau potable...

**Qui est concerné par la Directive NIS ?**

Les acteurs de tous ces secteurs sont, en France, déjà potentiellement concernés par la qualification d'Opérateurs d'Importance Vitale (OIV) créée par la Loi de Programmation Militaire (LPM) du 18 décembre 2013 qui identifiait comme étant d'importance vitale pour la survie de la nation des fonctions dont avaient la charge certaines collectivités territoriales. La liste des OIV relève du secret de la défense et est classée Confidentiel Défense, ce qui ne sera pas le cas pour la liste des OSE. En effet, l'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information, a maintenant jusqu'à novembre 2018 pour arrêter la liste des acteurs concernés au niveau Français. Toute entité, publique ou privée, est susceptible d'être désignée comme OSE si elle fait partie de l'un des secteurs adressés par la Directive NIS et si elle correspond aux critères d'identification suivants :

"Elle fournit un service essentiel au maintien d'activités sociétales et/ou économiques critiques" ;

"La fourniture de ce service est tributaire des réseaux et des systèmes d'information" ;

"Un incident aurait un effet disruptif important sur la fourniture dudit service".

Bien que la Directive NIS ait été fortement influencée par la France et la LPM, la définition d'OSE est bien plus large que celle d'OIV, et de nombreux acteurs épargnés par la LPM se retrouveront contraints par cette nouvelle réglementation. Ce sera notamment le cas de nombreuses collectivités territoriales qui, du fait de certains services qu'elles offrent à leurs administrés, seront soumises à de nouvelles exigences réglementaires.

**Collectivité territoriale désignée OSE : que faire ?**

La transcription en droit interne de la directive NIS le 26 février 2018 a soulevé les enjeux organisationnels qui s'imposeront aux structures désignées OSE par l'ANSSI d'ici la fin de l'année 2018. Les exigences qui seront imposées aux OSE, notamment aux collectivités territoriales, nécessiteront, pour certaines d'entre elles, de s'appuyer sur de nouvelles formes de collaboration, comme la mutualisation des ressources. Sur ce point, les structures de mutualisation qui se créent pour l'accompagnement des petites collectivités territoriales et des TPE-PME dans leur mise en conformité au RGPD peuvent servir de modèles. La directive NIS nécessitera aussi de la part des opérateurs l'élaboration d'une politique de sécurité globale prenant en compte les enjeux organisationnels et managériaux de la sécurité numérique, et nécessitera de mettre en place des mécanismes de contrôle en interne de la conformité réglementaire. Ces nouvelles contraintes réglementaires ont vocation à obliger les structures publiques et privées désignées OSE à lever leur niveau de sécurité globale. Mais ces contraintes sont surtout des opportunités à saisir pour les collectivités qui jouent un rôle majeur dans l'attractivité économique des territoires. La sécurité numérique deviendra un élément différenciant qui permettra aux territoires d'être plus attractifs, en assurant un haut niveau de cybersécurité de la part des collectivités territoriales.

C'est pour répondre à ces enjeux que le CyberCercle, qui travaille depuis ses origines avec les collectivités et les territoires lors des Rencontres Cybersécurité & Territoires et dans le cadre du Tour de France de la Cybersécurité, organise le 20 septembre 2018 à Toulouse Les Assises de la Cybersécurité des Territoires, qui sont le rendez-vous incontournable pour les collectivités qui veulent s'engager dans une transition numérique responsable et sécurisée. N'oubliez pas de nous rejoindre à cette occasion !

*Bénédicte Pilliet, Directeur fondateur de CyberCercle, b.pilliet@cybercercle.com*