# Cybersécurité : Les réseaux sociaux boutés de la directive NIS

L'activité des moteurs de recherche, des sites e-commerce et des fournisseurs Cloud tombera bien sous le coup de la directive NIS (Network and Information Security)… au contraire de celle des réseaux sociaux. Les députés européens et le Conseil des ministres ont fini par trouver un consensus sur le statut à donner à ces plates-formes de contenus et services dans le cadre de l'extension des obligations de sécurité aux entreprises de la société de l'information.

Proposée en février 2013 à l'issue d'une consultation publique, la directive NIS a pour objectif de renforcer la réactivité des 28 États membres et de stimuler la coopération entre les autorités de lutte contre la cybercriminalité, tout en leur donnant des moyens techniques et légaux appropriés. Troisième volet de la stratégie « Europe 2020 » aux côtés de l'accès Internet (très) haut débit, de l'éducation des citoyens aux nouvelles technologies ou encore de l'interopérabilité par les standards, le texte doit participer à la construction d'un marché unique du numérique dans l'UE.

Les problématiques de coopération avaient été abordées en 2013 avec le lancement de l'EC3 (European Crime Centre), dans les locaux d'Europol. Parmi les autres mesures aujourd'hui entérinées, la mise en place d'un réseau paneuropéen de CERTs (Computer Emergency Response Teams), c'est-à-dire des centres d'alerte et de réaction aux attaques informatiques.

## Le numérique rejoint les secteurs « critiques »

Les négociations auront été plus compliquées sur des enjeux comme l'inclusion des plates-formes de services sus-évoquées. Le Parlement européen avait initialement suggéré de limiter la portée de la NIS aux secteurs considérés « critiques » : énergie, transport, banque, santé, marchés financiers… Selon un document consulté par Reuters, le vent aurait tourné au cours de l'été : il aurait été décidé d'englober Google, Amazon, eBay et consorts – mais pas Facebook ou Twitter – avec toutefois des obligations moins lourdes que pour les sociétés exploitant des infrastructures qualifiées de « critiques ».

Ces dernières devront obligatoirement signaler leurs incidents de sécurité majeurs aux autorités nationales compétentes, explique *ITespresso.fr*. Les plates-formes qui leur fournissent des services seront assujetties aux mêmes règles et pourront être sanctionnées si elles ne s'exécutent pas.

Principal objectif pour Andrus Ansip, commissaire européen au Numérique : restaurer la confiance des consommateurs envers les sociétés dont l'activité est basée sur le numérique, « *qui n'a pas de frontières* […] *; un problème dans un État membre peut avoir un effet dans les 27 autres* ». Ce texte, qui pose les bases d'une première loi cybersécurité harmonisée, doit encore être approuvé par la Commission au marché intérieur et par le Comité des représentants permanents.

La France est déjà en avance sur ce problème avec la loi de programmation militaire qui dans son article 22 donne obligation aux OIV (opérateur d'importance vitale) de remonter les incidents de sécurité à l'Anssi (Agence Nationale de Sécurité des Systèmes d'Information). Des arrêtés sont en

cours de finalisation pour définir exactement les efforts de sécurité à mener selon les secteurs concernés. Guillaume Poupard, directeur général de l'Anssi, avait évoqué la directive NIS lors dernières Assises de la Sécurité en soulignant que « *il ne s'agit pas d'abaisser les niveaux de sécurité, il faut des produits robustes, pas des bouts de logiciel et de la poudre de perlimpinpin* ». Il faudra encore attendre pour voir cette directive européenne être finalisée.

**A lire aussi :**

Directive NIS : ce que l'Europe prépare pour les acteurs du Web

Assises de la sécurité 2015 : L'Anssi couve les OIV