# Le Conseil de l’UE rend sa copie sur la directive cybersécurité

| | |
|---|---|
| | Le Conseil de l’UE rend sa copie sur la directive cybersécurité |

**Les députés et le Conseil des ministres de l'UE sont parvenus à un accord autour de la directive NIS (Network and Information Security.) Celle-ci entend harmoniser les exigences en matière de cybersécurité entre les 28 pays membres de l'UE.**

L'Europe ouvre la voie à une gestion communautaire de la cybersécurité et annonce un accord entre le parlement et le Conseil de l'UE autour de la directive NIS.

Cette directive en négociation depuis plusieurs mois est chargée d'harmoniser le cadre légal des pays membres autour des dispositions relatives à la sécurité des systèmes jugés critiques. La directive était en discussion au conseil depuis le mois d'octobre 2014, après une validation du parlement et à l'époque, les négociations s'annonçaient serrées.

Le texte initial s'accordait sur la nécessité pour les opérateurs « critiques » de faire remonter auprès des responsables et autorités les incidents de sécurité qui pouvaient affecter leurs systèmes. Derrière ce terme, on retrouvait ceux qu'en France on place sous la catégorisation d'OIV (opérateurs d'importance vitale) depuis la loi de programmation militaire de 2013 : les acteurs majeurs du secteur de l'énergie, des transports, de la santé ou des marchés financiers par exemple.

Mais le texte revu et corrigé par le Conseil de l'UE va plus loin et propose d'étendre la régulation des plateformes en ligne à l'instar de Google, Amazon ou Ebay. Ces plateformes en ligne devront donc également se plier à des exigences de reporting en matière de cybersécurité, mais celles-ci seront moins lourdes que les exigences envisagées pour les opérateurs critiques. Seuls les incidents graves devront être signalés.

Les États membres auront pour rôle d'identifier les acteurs et plateformes jugés « indispensables pour la société et l'économie » en amont, mais le texte prend soin d'exclure les micro et petites entreprises du numérique, qui jouiront d'une exemption.

## Mieux vaut prévenir que subir

Le texte prévoit également la création d'un « réseau d'équipes d'intervention en cas d'incident lié à la sécurité informatique » établi dans chaque état membre afin de traiter et de répondre aux incidents transfrontaliers et « identifier des réponses coordonnées.

Reuters avait déjà publié en août un article relatant l'évolution des négociations en ce sens, une information qui avait suscité les inquiétudes de l'Afdel et de l'Asic. Les associations d'éditeurs en ligne craignaient en effet une loi trop pesante venant désavantager les entreprises et plateformes web européennes face à leurs concurrents étrangers.

Le texte doit encore être approuvé par la commission du marché intérieur du Parlement et par le comité des représentants permanents du Conseil avant d'être appliqué. En l'état actuel du texte, force est de reconnaître que cela ne devrait pas changer fondamentalement la donne en France : le reporting des incidents affectant les OIV était déjà l'une des mesures phares de la loi de Programmation Militaire de 2013 tandis que l'Anssi assume de fait le rôle d'équipe d'intervention en cas d'incident.

Mais la mention des plateformes web parmi les acteurs concernés pourrait en revanche amener le gouvernement à élargir la liste des OIV à placer sous la coupe de la LPM afin de se mettre en harmonie avec la directive européenne.

---

Réagissez à cet article

Source : http://www.zdnet.fr/actualites/le-conseil-de-l-ue-rend-sa-copie-sur-la-directive-cybersecurite-39829484.htm