**Synthèse du projet de loi n° 7314 (PL 7314)**

**PROJET DE LOI**

**portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d’information dans l’Union européenne et modifiant :**

**1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l’information de l’Etat et**

**2° la loi du 23 juillet 2016 portant création d’un Haut- Commissariat à la Protection nationale**

L’objet du **PL 7314** consiste en la transposition en droit national de la **directive (UE) 2016/1148** du Parlement européen et du Conseil **du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d’information dans l’Union**. (ci-après « **la directive** »).

La digitalisation progressive de la quasi-totalité de notre société va de pair avec une croissance continue

- du nombre,

- de l’ampleur, et

- des répercussions

des attaques informatiques sur les systèmes et réseaux numériques.

Dans notre ère numérique, les systèmes d’information représentent dans beaucoup de cas des éléments essentiels pour le fonctionnement tant des entreprises que des administrations publiques, mais également en ce qui concerne la vie sociale des citoyens. Par conséquent il est inéluctable de renforcer constamment les efforts de sécurisation des systèmes et réseaux informatiques, d’autant plus que la connexion de toujours plus d’appareils électroniques augmente en parallèle la vulnérabilité et les sources de risque pour ces attaques.

Partant, **la directive** vise à harmoniser et renforcer davantage la coopération des États membres de l’Union européenne (UE) en termes de gestion des risques cyber.

Elle établit des règles communes horizontales pour ce qui est de la gestion de la sécurité cyber, en particulier en ce qui concerne :

- les opérateurs qui fournissent des services essentiels (OSE), ainsi que

- les fournisseurs des services numériques (FSN).

Les secteurs considérés essentiels au fonctionnement de la société sont les suivants :

- l’énergie,

- les transports,

- les banques,

- les infrastructures des marchés financiers,

- la santé,

- la fourniture et distribution d’eau potable, et

- les infrastructures numériques.

Ainsi les acteurs concernés doivent se soumettre à certaines obligations, à savoir, entre autres, à

- l’obligation de prendre toutes les précautions nécessaires pour assurer au mieux la sécurité de leurs systèmes informatiques, ou encore

- l’obligation de signaler les incidents qui ont un impact considérable sur leurs activités aux autorités compétentes.

Le **PL 7314** prévoit notamment des critères détaillés pour déterminer la gravité d’un incident numérique.

Au niveau national, **la directive** prévoit le renforcement des capacités nationales.

Les États membres de l’UE doivent désigner des autorités nationales compétentes qui contrôlent le respect par les OSE et les FSN de leurs obligations respectives.

De plus, les États membres de l’UE sont tenus à

- se doter d’équipes nationales de réponse aux incidents informatiques, et

- d’élaborer une stratégie nationale de cybersécurité.

Finalement, au niveau européen, la coopération et l’échange d’informations sont renforcés.

À cette fin, un groupe de coopération et un réseau de centres de réponse aux incidents de sécurité informatiques (« réseau des CSIRT - Computer Security Incident Response Teams ») sont mis en place.

Plus particulièrement, le rôle du groupe de coopération consiste à échanger des informations, du savoir-faire et de bonnes pratiques, ainsi que à encourager la coopération stratégique entre les États membres.

Le réseau des CSIRT, quant à lui, sert à promouvoir une coopération opérationnelle rapide et effective entre les États membres.