ASSEMBLÉE NATIONALE

30 septembre 2021

PLF POUR 2022 - (N° 4482)

Non soutenu

AMENDEMENT

N º I-CF312

présenté par
Mme Bazin-Malgras

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 4, insérer l'article suivant:

I. – Après l'article 244 *quater* X du code général des impôts, il est inséré un nouvel article 244 *quater* Y ainsi rédigé :

« *Art. 244* quater *Y*. – I. – Les entreprises imposées d'après leur bénéfice réel peuvent bénéficier d'un crédit d'impôt égal à 30 % de la somme :

« – Des dépenses d'audit de cybersécurité ;

« – Des dépenses d'acquisition, de souscription ou de maintenance d'un produit ou service de cybersécurité ;

« – Des dépenses de formation en cybersécurité engagées par l'entreprise en faveur de salariés.

« II. – Les subventions publiques reçues par les entreprises à raison des dépenses ouvrant droit au crédit d'impôt sont déduites des bases de calcul de ce crédit.

« III. – Le crédit d'impôt est plafonné pour chaque entreprise y compris les sociétés de personnes, à 100 000 €.

« VI. – Le crédit d'impôt est imputé sur l'impôt sur les sociétés après imputation des réductions d'impôt, des crédits d'impôt et des prélèvements ou retenues non libératoires. S'il excède l'impôt dû, l'excédent est restitué.

« V. – Un décret fixe les conditions d'application du présent article.

II. – La perte de recettes pour l'État est compensée à due concurrence par la création d'une taxe additionnelle aux droits mentionnés aux articles 575 et 575 A du code général des impôts.

III. Le I ne s'applique qu'aux sommes venant en déduction de l'impôt dû.

EXPOSÉ SOMMAIRE

Cet amendement propose la création d'un crédit d'impôt sur les sociétés de 30 % pour l'investissement dans des diagnostics d'audit de cybersécurité ou l'acquisition de solutions de protection des données ou du système informatique des entreprises, dans la limite 100 000 euros par an.

La mise en œuvre du travail à distance et l'adoption de systèmes d'information en urgence ont été réalisées au mépris de règles basiques de cybersécurité, soit par manque de connaissance face aux risques, soit volontairement pour assurer une continuité de l'activité. Les entreprises se sont rendues plus vulnérables aux cyberattaques (rançongiciel, hameçonnage, vol de données, etc.). Elles ont désormais besoin de réaliser un premier bilan sur les risques auxquels elles sont exposées, et les mesures à prendre pour sécuriser leur système d'information.