# ASSEMBLÉE NATIONALE

10 novembre 2017

PLF POUR 2018 - (N° 235)

| | |
|---|---|
| Commission | |
| Gouvernement | |

Non soutenu

# AMENDEMENT

N º II-1326

présenté par
Mme de La Raudière, Mme Auconie, M. Becht, M. Benoit, M. Bournazel, M. Charles de Courson, M. Favennec Becot, Mme Firmin Le Bodo, M. Meyer Habib, M. Lagarde, M. Ledoux, M. Leroy, Mme Magnier, M. Morel-À-L'Huissier, Mme Sage, M. Vercamer et M. Zumkeller

---

## ARTICLE 46

Après le mot :

« attestation »,

rédiger ainsi la fin de l'alinéa 4 :

« de l'éditeur, conforme à un modèle fixé par l'administration, ou par une attestation produite par l'équipe technique de l'entreprise attestant des caractéristiques de sécurisation des données accompagné d'un dossier technique étayant ces qualités ; ».

## EXPOSÉ SOMMAIRE

Cet amendement a pour but de rendre certifiables les logiciels open-sources et les logiciels développés en interne, ainsi que de simplifier le processus de certification.

En l'état de la loi et du contenu de l'art 286 du code général des impôt et de l'article 46 du PLF 2018, la loi imposera au 1 janvier 2018 à toutes les entreprises qui effectuent de la vente aux particuliers et soumises à la TVA de s'équiper de logiciels dits anti-fraude à la TVA.

Cette injonction peut sembler, au première abord, simple et de bon sens.

Son application au monde du commerce de proximité est peut-être justifiée et sans grandes difficultés de mise en oeuvre.

Mais pour ce qui est des TPE / PME du e-commerce cette loi met en danger des milliers de petites structures ; sa mise en oeuvre est impossible dans de nombreux cas et sans aucun contribution à la lutte contre la fraude à la TVA qu'elle est sensée combattre.

En effet, les entreprises du e-commerce utilisent très souvent des logiciels « open-sources » ou des logiciels « développés en interne » pour construire leurs sites de vente en ligne.

Or, conceptuellement ces outils ne sont pas certifiables de par le fait qu'ils permettent la modification du code informatique (« code source ») par l'utilisateur du logiciel.

Ces logiciels de e-commerce n'ont rien à voir avec les « caisses enegistreuses » des petits commerçants de quartier, et une mise en conformité avec cette nouvelle obligation ne consiste pas en une simple mise à jour de logiciel.

Ainsi, pour une part importante des 134 000 TPE / PME du e-commerce qui réalisent moins de 30 000 € de Chiffre d'Affaire l'illégalité sera la norme au 1 janvier 2018.

Sachant que l'amende due dans ce cas est de 7 500 €, renouvelable tous les 60 jours, les conséquences pérvisibles sont catastrophiques.

De plus, cette obligation est bien souvent ignorée des e-commerçants, principalement en raison de l'usage par l'administration du terme « logiciel de caisse », qui laisse à penser que les solutions de e-commerce ne sont pas concernées ; or, un site de e-commerce est bel et bien un « logiciel de caisse » du point de vue de l'administration fiscale.

Aussi, dans le cas du e-commerce la loi est tout à la fois :

Inutile : car les règlements de commandes passées sur un site de e-commerce sont réalisés exclusivement via des moyens de paiement électroniques, ne permettant pas la fraude : carte bancaire, virement bancaire, Paypal... Tout ces moyens de paiement sont traçables, et ne permettent pas la fraude à la TVA, ni la dissimulation de revenus.

Force est donc de constater que pour les entreprises du e-commerce l'usage de logiciels certifiés est tout simplement inutile, sans objet.

Economiquement dangereuse : Une étude de la FEVAD stipule qu'en 2017 le commerce en ligne français est constitué de plus de 204 000 sites actifs, dont 66 % réalisent un chiffre d'affaire de moins de 30 000 €, ce qui représente 134 000 entreprises.

Pour ces 134 000 petites structures les moyens humains, techniques et financiers sont très limités, et ne peuvent être dispersés sur des projets sans valeur ajoutée ni pour les clients, ni pour l'entreprise, ni même pour l'état.

Bien que les grands acteurs du e-commerce puissent éventuellement supporter les coûts très élevés d'une certification il n'en demeure pas moins vrai qu'eux non plus ne gèrent pas de paiements susceptibles de permettre la fraude, ou seulement pour des volumes très faibles de transaction.

Cette obligation met donc inutilement en péril la survie de dizaines de milliers de petites structures.

Enfin, inapplicable aux logiciels open-sources et aux logiciels développés en interne :

Contrairement aux logiciels de caisse mis en œuvre dans les commerces de proximité, qui sont édités et maintenus par un petit nombre d'entreprises, les logiciels mis en œuvre par les sites de e-commerce sont des constructions complexes, bien souvent basés sur des logiciels « open-sources » (83 % des cas) et/ou « développés en interne ».

Ces briques techniques proviennent de nombreux éditeurs, français et étrangers, professionnels ou non.

Les modifications logicielles, très fréquentes dans le e-commerce car facteur important de différenciation, sont réalisées par des techniciens qui ajoutent ou suppriment des briques logicielles et modifient le code source. Ces experts œuvrent parfois en tant qu'indépendant, ou au sein d'entreprises de services informatiques ; ils sont parfois français, et parfois situés sur d'autres continents.

Dans ces conditions la mise en conformité et la certification des logiciels sont très compliqués, voir tout simplement impossibles car abusivement cher (plusieurs milliers d'Euros). Et chaque adaptation ou personnalisation un tant soit peu importante impliquerait potentiellement un nouveau cycle de certification.

Également inapplicable et excessive est l'obligation de certification individuelle ( i.e : une « configuration logicielle » doit être certifiée « individuellement » par un « certificateur » pour « une entreprise donnée »). Cette disposition n'empêchera jamais un e-commerçant malhonnête de missionner un technicien pour manipuler le code informatique d'un logiciel dûment certifié, à l'insu du certificateur. Cette disposition ne fait que compliquer la vie des entreprises honnêtes sans entraver les pratiques de contournement.

Le seul moyen d'interdire toutes modifications frauduleuses d'un système de gestion de site de e-commerce serait de totalement interdire l'accès au « code source » des logiciels, et d'interdire aux personnes de l'entreprise qui exploite le site toutes interventions directes sur le système informatique. Cela reviendrait à obliger tous les e-commerçants à recourir exclusivement à des logiciels « fermés », ou à des logiciels Saas ; et à faire appel exclusivement à des sociétés de services informatiques pour l'installation, l'exploitation et la maintenance de leur système.

Aller dans cette direction signifierait faire disparaître les « petits e-commerçants » au profit des « grands groupes », livrer les survivants aux diktats des entreprises de l'industrie et des services informatiques et faire disparaître toute trace des offres logicielles « open-sources » dans le e-commerce.

De telles contraintes seraient totalement inacceptables, et financièrement intenables pour les TPE et les PME du secteur de la vente en ligne.

Donc, en complément des adaptations suggérées par l'article 46 du PLF 2018 nous pensons indispensables les adaptations suivantes :

· Seuls les logiciels utilisés pour enregistrer des paiements en espèces doivent être soumis à l'obligation de certification. Cela exclut de fait les logiciels de e-commerce du périmètre de certification.

· L'obligation de certification doit s'appliquer uniquement à des entreprises pour lesquelles le volume de Chiffre d'Affaire avec règlement « en espèces » dépasse un certain seuil, basé éventuellement sur le chiffre d'affaire total de l'entreprise. Avec possible mise en place d'un plafond au-delà duquel l'obligation devient effective indépendamment du CA global.

· Lorsque l'entreprise est soumise à l'obligation de faire usage de logiciels certifiés : la certification individuelle doit être abandonnée et remplacée par une simple attestation de l'éditeur ou d'un prestataire garantissant la conformité de sa solution.

· Les entreprises soumises à l'usage de logiciels certifiés doivent pouvoir « auto- certifier » les modifications et les développements réalisés par leurs équipes informatiques ou par leurs prestataires. Un dossier technique complémentaire permettant de tracer les modifications techniques réalisées sur le système en question.

Ces adaptations permettent de sécuriser l'activité des entreprises de e-commerce sans remettre en cause l'efficacité de la loi initiale, ni l'objectif de lutte contre les fraudes liées aux transactions en espèces.