Cyber Resilience Act : Danger pour le logiciel libre en Europe
Mac et Linux
PostÃ© par : JerryG
PubliÃ©e le : 17/7/2023 14:00:00

Le Conseil National du Logiciel Libre (CNLL), qui reprÃ©sente plus de 300 entreprises de la filiÃ¨re du logiciel libre et du numÃ©rique ouvert en France, exprime sa profonde prÃ©occupation concernant le projet de rÃ©glementation de lâ□□Union europÃ©enne intitulÃ© â□□Cyber Resilience Actâ□□ (CRA).

Le CRA a pour objectif louable dâ□□amÃ©liorer la cybersÃ©curitÃ© des produits numÃ©riques en Europe. Cependant, câ□□est un texte â□□buggÃ©â□□ qui va faire lâ□□objet dâ□□un vote crucial le 19 juillet au sein du comitÃ© ITRE du Parlement europÃ©en, et qui pourrait Ãªtre adoptÃ© dans la foulÃ©e, sans vote en session plÃ©niÃ¨re, par le Parlement lui-mÃªme.

Si rien de change dâ□□ici son adoption finale, il aura des consÃ©quences particuliÃ¨rement lourdes pour les petites et moyennes entreprises (PME) Ã©voluant dans le domaine du logiciel libre, et plus gÃ©nÃ©ralement sur la filiÃ¨re du logiciel libre, une composante essentielle de lâ□□Ã©conomie numÃ©rique europÃ©enne.

Quels sont les principaux problÃ¨mes que pose le texte du comitÃ© ITRE pour la filiÃ¨re europÃ©enne du logiciel libre ?

Le CRA va imposer des exigences administratives et techniques trÃ¨s coÃ»teuses pour les organisations qui diffusent des produits ou des services logiciels ou contenant des logiciels.

Elles devront notamment dÃ©velopper, documenter et mettre en Å□uvre des politiques et des procÃ©dures pour chaque projet, prÃ©parer une documentation technique pour chaque version de produit et suivre un processus complexe de marquage CE.

Lâ□□Ã©tude dâ□□impact de la Commission estime Ã 30% lâ□□augmentation des coÃ»ts de dÃ©veloppement pour les PME, ce qui est largement supÃ©rieur aux marges habituellement constatÃ©es dans le secteur. En cas de non-respect de ces obligations, les PME sont passibles dâ□□une amende de 15 millions dâ□□euros.

Les logiciels libres sont, par dÃ©finition, des logiciels diffusÃ©s sous une licence de logiciel libre (ou open source, ce qui revient essentiellement au mÃªme). Toutes les licences de logiciel libre en usage actuellement comprennent une clause de non-responsabilitÃ©: il est en effet logique quâ□□un individu, une entreprise, petite ou grande, une fondation, un institut de recherche, etc. ne tiennent pas Ã Ãªtre tenu Ã une responsabilitÃ© (lorsquâ□□il nâ□□y a pas une volontÃ© dÃ©libÃ©rÃ©e de nuire) quand il ou elle offre, gratuitement, le fruit de son travail en tant que bien commun au reste de lâ□□humanitÃ©.

En parallÃ¨le, les Ã©diteurs de logiciels libres nâ□□ont pas attendu le CRA pour proposer Ã leurs clients des contrats oÃ¹ ils sâ□□engagent Ã assurer la maintenance de leurs logiciels libres, contre une rÃ©munÃ©ration, qui couvre les frais de maintenance mais aussi les frais de R&D nÃ©cessaire Ã la crÃ©ation et Ã lâ□□Ã©volution de ces logiciels.

Dans le texte dâ□□origine de la Commission, le CRA comprend une exemption pour les â□□activitÃ©s non-commercialesâ□□, dont les reprÃ©sentants de lâ□□Ã©cosystÃ¨me open source ont soulignÃ©, dÃ¨s la publication du projet de texte initial, lâ□□ambiguÃ¯tÃ© et les risques que

celle-ci reprÃ©sente.

Selon le projet de texte actuel du comitÃ© ITRE, tout projet de logiciel libre qui compte parmi ses contributeurs des employÃ©s dâ□□une entreprise est considÃ©rÃ© comme une activitÃ© commerciale. Cette dÃ©finition Ã©largie englobe presque tous les projets de logiciels libres significatifs, avec des consÃ©quences potentiellement dÃ©vastatrices.

Non seulement cela inciterait les projets, dont on sait que certains ont des difficultÃ©s Ã assurer leur durabilitÃ© financiÃ¨re, Ã refuser les contributions de sociÃ©tÃ©s utilisatrices de leurs logiciels, mais cela pourrait Ã©galement conduire les entreprises Ã interdire Ã leurs employÃ©s de participer Ã des projets de logiciel libre.

Cela inciterait Ã©galement les entreprises de la filiÃ¨re du logiciel libre Ã cesser de publier leurs composants en open source, Ã rendre moins transparentes leurs pratiques de dÃ©veloppement, et Ã renoncer Ã contribuer Ã des projets de logiciels libres lorsque ceux-ci ne rentrent pas dans les exceptions, trÃ¨s restrictives, prÃ©vues par le texte.

Par ailleurs, le texte du comitÃ© ITRE dispose que tout projet de logiciel libre acceptant des donations rÃ©currentes de la part dâ□□entitÃ©s commerciales est considÃ©rÃ© comme une activitÃ© commerciale.

Cela reprÃ©sente un risque majeur pour la pÃ©rennitÃ© des projets de logiciel libre qui servent de briques de base aux produits que les PME du logiciel libre mettent sur le marchÃ©. En effet, la durabilitÃ© financiÃ¨re de ces projets open source est un dÃ©fi maintes fois Ã©voquÃ© et largement reconnu.

Les donations rÃ©guliÃ¨res provenant dâ□□entitÃ©s commerciales sont souvent une source de financement essentielle qui permet aux projets de continuer leur travail.

Cependant, si le CRA est adoptÃ© en lâ□□Ã©tat, ces projets seront incitÃ©s Ã refuser les donations, et donc voir leurs ressources limitÃ©es strictement au bÃ©nÃ©volat, ce qui va Ã lâ□□encontre de la volontÃ© affichÃ©e par ailleurs dâ□□amÃ©liorer leur durabilitÃ© financiÃ¨re. Lâ□□impact nÃ©gatif se propagera en aval de tous ces projets, avec comme consÃ©quence systÃ©mique un affaiblissement de la sÃ©curitÃ© globale des produits mis sur le marchÃ© en Europe, en plus de la disruption de la chaÃ®ne dâ□□approvisionnement logicielle des Ã©diteurs de logiciels europÃ©ens.

Enfin, notons que la filiÃ¨re du logiciel libre, au-delÃ des PME qui la composent principalement, est un secteur Ã©conomique majeur pour lâ□□Europe. Elle contribue Ã lâ□□Ã©conomie de lâ□□UE Ã hauteur de 65 Ã 95 milliards dâ□□euros par an, selon lâ□□Ã©tude de la Commission de 2021, et est au cÅ□ur de la recherche et dÃ©veloppement dans de nombreux domaines technologiques avancÃ©s, y compris du programme de R&D Horizon Europe. Lâ□□impact du CRA sur cette filiÃ¨re risque donc dâ□□avoir des consÃ©quences bien au-delÃ des entreprises directement concernÃ©es.

Le CNLL appelle donc les lÃ©gislateurs europÃ©ens Ã prendre en compte ces enjeux, et Ã rÃ©viser le CRA de maniÃ¨re Ã protÃ©ger la filiÃ¨re du logiciel libre, et notamment les PME qui en sont le socle, sans pour autant compromettre lâ□□objectif de renforcement de la cybersÃ©curitÃ©.

A lâ□□avenir, ce type de rÃ©glementation devra Ãªtre Ã©laborÃ© en concertation Ã©troite avec les acteurs de lâ□□Ã©cosystÃ¨me open source, y compris les entreprises europÃ©ennes qui dÃ©veloppement des logiciels libres et celles qui intÃ¨grent des composants open source dans leurs produits, les plus Ã mÃªme de comprendre et dâ□□expliquer les spÃ©cificitÃ©s et les enjeux de leur secteur.

Lâ□□APELL (Association Professionnelle EuropÃ©enne du Logiciel Libre), qui fÃ©dÃ¨re les associations nationales dâ□□entreprises du libre en Europe, doit Ãªtre un interlocuteur privilÃ©giÃ© des institutions europÃ©ennes sur ces questions, tout comme le CNLL auprÃ¨s du gouvernement franÃ§ais.

Nous appelons Ã©galement Ã la crÃ©ation au sein de la Commission dâ□□un OSPO (Open Source Programme Office) externe, focalisÃ© sur le dÃ©veloppement de la filiÃ¨re du logiciel libre en Europe, qui devra travailler en Ã©troite collaboration avec OSOR, lâ□□OSPO interne de la Commission, et apporter son expertise lors des initiatives lÃ©gislatives Ã venir qui concerneront le logiciel libre.

Enfin, nous devons collectivement favoriser une meilleure comprÃ©hension, au sein de nos institutions, des enjeux du numÃ©rique ouvert et des dynamiques technologiques et Ã©conomiques complexes qui caractÃ©risent lâ□□Ã©cosystÃ¨me du logiciel libre. Cela passe par une formation renforcÃ©e des dÃ©cideurs politiques sur ces questions, mais aussi par une meilleure prise en compte de lâ□□expertise technologique interne et externe dans les processus dÃ©cisionnels.

DÃ©but 2024: Le texte sera probablement adoptÃ© dÃ©finitivement.