La France doit protéger sa filière du logiciel libre des effets de bord du Cyber Resilience Act (CRA)

Paris, le 7 septembre 2023 - Pour diffusion immédiate.

Les institutions européennes entament la phase finale des négocations autour du CRA (*Cyber Resilience Act*), une initiative réglementaire dans le domaine de la cyber-sécurité qui risque, dans l'état actuel de certaines versions du texte, d'avoir un impact négatif considérable sur la façon dont les logiciels libres sont écrits, diffusés et utilisés en Europe, et par conséquent sur le dynamisme de la filière professionnelle de l'open source. Les logiciels libres, essentiels à l'économie numérique française et à notre souveraineté numérique, nécessitent en effet une stratégie claire et une protection juridique. Le CNLL demande donc à ce que le gouvernement français fasse tous les efforts nécessaires pour que soient clarifiées les questions de responsabilité pour les créateurs de logiciels et composants open source, afin d'éviter tout risques juridiques et de minimiser l'impact du CRA sur l'économie et la souveraineté numériques.

Le CNLL a publié une étude détaillée de l'impact du CRA sur la filière du logiciel libre et pointe les éléments qui peuvent encore en limiter les conséquences négatives s'ils sont pris en compte lors du trilogue.

Ce qui suit en résume les points clefs.

Contexte

Le *Cyber Resilience Act* (CRA) est une initiative réglementaire européenne visant à obliger les fabricants, les distributeurs et les importateurs de produits comportant des composants numériques à respecter des normes de sécurité pour leurs produits ou services dès la phase de conception et tout au long du cycle de vie du produit.

Le CNLL soutient les objectifs du CRA visant à accroître la qualité et les normes de sécurité des matériels et des services en ligne. En outre, les entreprises membres de notre association ont tout intérêt à s'inscrire dans une démarche responsable de renforcement de la sécurité des logiciels.

Mais le CNLL s'inquiète vivement des risques, exposés ci-dessous, que constituerait une rédaction finale du CRA inappropriée eu égard à la réalité des

modèles économiques et de développement de la filière open source, et demande au gouvernement français de peser sur les négociations finales afin de protéger sa filière nationale du logiciel libre, qui représente près de 6 Mrds d'euros de CA annuel et 64 000 emplois directs en 2023.

Constats

Si le texte final n'est pas « débuggé », l'écosystème open source, et en aval, l'économie numérique européenne, subira de plein fouet les conséquences négatives suivantes (entre autres):

- **Surréglementation**: Le CRA ne prend pas suffisamment en compte les modèles spécifiques des logiciels libres, mettant ainsi des exigences disproportionnées sur les petites entreprises et les projets non commerciaux qui n'ont pas les ressources, notamment financières, pour y répondre.
- **Insécurité juridique**: En raison de la formulation ambiguë du CRA, il existe une grande incertitude sur la manière dont la réglementation va s'appliquer aux logiciels libres. Sans une guidance claire, de nombreuses entreprises, grandes et petites, annoncent déjà envisager de s'abstenir de développer ou de diffuser des logiciels libres en Europe de peur d'enfreindre accidentellement les règles.
- **Effet paralysant sur l'écosystème open source**: Le CRA risque de décourager la participation des entreprises européennes à des projets de logiciels libres et entraîner un retrait des fournisseurs de composants open source non européens du marché européen, nuisant ainsi à la collaboration, à l'innovation, à la compétitivité et à la souveraineté des économies française et européenne.
- **Menace sur l'économie et à la souveraineté numérique**: Par son impact sur l'écosystème du logiciel libre, lui-même facteur d'innovation, de croissance et de souveraineté numérique, le CRA risque de ralentir la croissance et l'innovation, en particulier pour les PME et les start-ups, ayant ainsi des conséquences négatives sur la concurrence et le développement économique. Il y a aussi un risque clair de mettre les entreprises européennes, notamment les PME, dans une situation de désavantage concurrentiel fort par rapport à la compétition internationale, et notamment aux *hyperscalers* (« GAFAM »).

Recommandations

Le CNLL demande donc au gouvernement français, ainsi qu'à toutes les parties prenantes du trilogue visant à finaliser le texte, de prendre en compte les points suivants:

- **Protéger l'écosystème open source**: Veiller à ce que l'écosystème open source, qui est essentiel pour l'économie informatique française et européenne et pour la souveraineté numérique de la France, soit protégé de manière adéquate et dans toute sa diversité, dans le CRA.
- **Clarifier les responsabilités**: S'assurer que, lorsqu'il s'agit d'entités différentes, le créateur d'un logiciel ou d'un composant open source ne soit pas tenu pour responsable, mais plutôt le « metteur en circulation » ou l'entreprise qui offre un service avec ce logiciel, notamment s'il est facturé ou si un modèle commercial est basé dessus.
- **Se baser sur les formulations du Conseil européen et du comité IMCO**: Privilégier les formulations du texte final du Conseil européen et les recommandations antérieures du comité IMCO du Parlement européen, qui semblent mieux protéger l'écosystème des logiciels libres, par rapport aux formulations de la commission ITRE.
- **Engager une collaboration avec les experts de l'industrie**: Favoriser un échange continu avec les représentants de la filière professionnelle des logiciels libres, en exploitant notamment l'expertise offerte par le CNLL au niveau français et de l'APELL au niveau européen, pour assurer que les décisions prises tiennent compte de la réalité des modèles économiques et de collaboration, et des besoins, du secteur open source.

Références et documents complémentaires

- Déclaration du CNLL sur le CRA (Cyber Resilience Act) - CNLL (sept. 2023)
- Diverse Open Source uses highlight need for precision in Cyber Resilience Act - Open Source Initiative (sept. 2023)
- Le CNLL alerte sur les dangers du Cyber Resilience Act pour la filière du logiciel libre en Europe - CNLL (juil. 2023)
- Etude 2022 : Le marché de l'open source en France et Europe - CNLL (nov. 2022).

A propos du CNLL

Le CNLL, Union des Entreprises du Logiciel Libre et du Numérique Ouvert, est l'instance représentative de la filière du logiciel libre en France. Issu du groupement de 12 clusters régionaux, il représente plus de 300 entreprises « pure players » (spécialisées ou avec une activité significative dans le logiciel libre et l'open source): éditeurs, intégrateurs, sociétés de conseil, etc. Il assure la promotion de l´écosystème professionnel du logiciel libre, de son offre de logiciels et de services, de ses atouts spécifiques, et de ses besoins, notamment en termes d'emploi et de formation. Il permet à la communauté des acteurs de la filière d'échanger et de travailler ensemble au développement du marché, dans le respect de valeurs communes.

Plus d'info : https://www.cnll.fr/