Déclaration du CNLL sur le CRA (Cyber Resilience Act)

Version: 1.1 (8 septembre 2023)

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.

Le CNLL participe activement aux réflexions sur les initiatives à mener et les financements à trouver pour assurer la soutenabilité et la sécurisation de la chaîne d'approvisionnement open source, par exemple, en ayant contribué au workshop « Building Sustainable Open Source Ecosystems for an Interoperable Europe » organisé par la Commission en 2022.

Dans ce contexte, 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.

I. Constats

Importance des logiciels libres pour l'innovation, la concurrence, l'économie en général et la souveraineté numérique

L'immense majorité (de 78 à 96 % selon les sources) de tous les logiciels contiennent aujourd'hui des composants open source. Cela signifie que les logiciels libres jouent un rôle décisif dans l'industrie des technologies de l'information et dans l'économie dans son ensemble - rien ne fonctionne sans logiciels libres. Une étude publiée par la Commission européenne en 2021 confirme cette influence significative des logiciels libres sur la compétitivité des entreprises européennes, sur la croissance économique, sur le développement des start-up et des PME, et sur l'indépendance technologique de l'Europe. L'open source contribue de manière significative au produit intérieur brut (PIB) de l'UE : environ 1 milliard

d'euros investis dans l'open source par les entreprises de l'UE en 2018 a entraîné une valeur ajoutée économique de 65 à 95 milliards d'euros, selon l'étude.

L'utilisation de logiciels libres est également d'une importance capitale pour renforcer la souveraineté numérique dans l'administration publique ainsi que dans les entreprises. En effet, les logiciels libres garantissent que les systèmes utilisés peuvent être vérifiés, conçus et remplacés de manière indépendante. Ils permettent ainsi aux administrations publiques de « préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information », selon les termes de la loi République Numérique de 2016. Ce rôle important a été souligné notamment par la circulaire Ayrault de 2012, la circulaire Castex de 2021, ou encore les rapports parlementaires du député Philippe Latombe et de la sénatrice Catherine Morin-Desailly sur la souveraineté numérique.

La difficile délimitation des « logiciels open source commerciaux » dans la CRA

Le CRA semble avoir été rédigé principalement sous le prisme du logiciel propriétaire. Par conséquent, les exigences à respecter sont également formulées en fonction des modèles de développement et de distribution des logiciels propriétaires, alors que dans le cas des logiciels libres, l'approche ouverte et coopérative et les libertés accordées par les licences modifient considérablement ces modèles.

Par exemple, bien que les créateurs et les éditeurs qui développent des logiciels libres puissent contrôler les logiciels qu'ils fournissent à leurs clients dans le cadre de contrats commerciaux, ils n'ont qu'une influence indirecte sur les logiciels, qui peuvent librement être téléchargés par des tiers et éventuellement modifiés et redistribués à des fins totalement différentes. Elles ne devraient donc pas être tenues responsables des produits ou logiciels de tiers qui utilisent tout ou partie de leur code logiciel original.

En outre, dans le cas de logiciels propriétaires sans accès au code source, on peut facilement comprendre qu'il soit impossible de faire porter la responsabilité à quiconque autre que l'éditeur originel. Ce n'est toutefois pas le cas avec un logiciel libre dont l'intégration à un produit ou à un service se fait sous le contrôle d'un tiers qui dispose de tous les moyens pour s'assurer de sa sécurité. La logique du CRA consistant à faire porter la responsabilité au créateur, faute d'alternative, ne doit pas s'appliquer au logiciel libre.

Le CRA prévoit une exemption pour les logiciels libres, à condition qu'ils ne soient pas utilisés dans le cadre d'activités commerciales. Le problème réside toutefois dans la définition concrète du terme « commercial ». Il est difficile d'établir une démarcation claire et il existe trop de zones grises qui laissent place à l'interprétation, et donc à l'incertitude juridique. En réalité, les composants et solutions open source sont le plus souvent développés et maintenus :

- par des employés rémunérés d'une entreprise à but lucratif :
  - dans le cadre d'une activité commerciale (directement génératrice de revenus) ;

  - dans le cadre d'une activité de support ou de R&D&I qui n'est pas directement génératrice de revenus ;
- dans un contexte de recherche scientifique par des chercheurs rémunérés par des universités, des structures privées, etc. ;
- dans l'enseignement par des enseignants rémunérés ;
- par l'administration publique ;
- par des milliers de bénévoles pendant leur temps libre, sans intérêt commercial propre ;
- etc.

Souvent, les composants et solutions open source sont également développés dans le cadre d'une coopération entre plusieurs, voire tous ces différents types d'acteurs, de sorte qu'il n'est pas toujours facile d'établir une distinction claire entre « commercial » et « non commercial ». L'imbrication d'acteurs et d'organisations bénévoles et commerciaux est inhérente à l'écosystème des logiciels libres. Il existe en Europe plus de 1000 éditeurs de logiciels libres dont les logiciels reposent sur ce type de coopération.

En outre, le CRA n'indique pas explicitement si la fourniture de services purement liés aux produits open source (développements spécifiques, service d'assistance de deuxième niveau, etc.) est déjà considérée comme une activité commerciale, de sorte que les fournisseurs de ces services tombent automatiquement sous le coup des obligations du CRA. Là encore, il convient de clarifier les choses. S'il est éventuellement envisageable que les entreprises qui commercialisent des services autour de logiciels libres puissent entrer dans le champ d'application du CRA, selon le CNLL, l'exemption pour la publication de logiciels libres par des éditeurs de logiciels libres, quelle que soit leur structure juridique, doit encore être améliorée. Les tentatives faites jusqu'à présent pour délimiter plus explicitement l'exception relative aux logiciels libres dans le CRA n'ont pas encore permis de résoudre le problème de l'incertitude juridique imminente et de la surréglementation.

Selon le CNLL, et en application d'un principe de subsidiarité, la publication en tant que telle d'un logiciel libre ne devrait pas faire porter de responsabilité au créateur (l'ayant droit), quelle que soit sa nature, car, contrairement à un logiciel propriétaire, la nature libre du logiciel permet au fabricant du produit matériel de s'assurer de l'absence de failles de sécurité. L'impact économique d'une responsabilisation des ayants droits conduirait par ailleurs à restreindre l'offre de logiciels libres et à détruire de l'emploi, ce qui serait contraire aux objectifs de résilience du CRA et aux principes généraux que doit respecter une directive européenne.

Danger de surréglementation

Le CRA ne tient actuellement pas suffisamment compte des modèles particuliers de développement et de distribution des logiciels libres, ce qui signifie que les réglementations prévues par le CRA sont difficiles à appliquer aux logiciels libres dans de nombreux cas ou qu'elles entraînent une surréglementation involontaire. La formulation actuelle du CRA fait

que de nombreux projets de logiciels libres de petite taille et non commerciaux (mais soutenus, en tout ou partie, par des structures commerciales) seraient également soumis aux exigences qu'elle définit, alors qu'ils n'ont pas les ressources, notamment financières, dans le cas des PME, nécessaires pour y répondre.

Dans la pêche, la taille des mailles du filet doit correspondre exactement à la taille du poisson à attraper. Dans le cas du CRA, les mailles sont actuellement beaucoup trop étroites, de sorte que trop de projets de logiciels libres développés par des entreprises hors d'un cadre strictement commercial, par des petits groupes d'individus plus ou moins bénévoles, ou issus de la recherche et de l'enseignement, notamment, se voient responsabilisés par le CRA alors qu'ils n'appartiennent pas au groupe cible du CRA.

Risque d'insécurité juridique

La marge d'interprétation et l'incertitude juridique engendrées par la formulation peu claire de l'exception relative aux logiciels libres signifient que les petits projets de logiciels libres, qui ne disposent généralement pas de conseillers juridiques professionnels, ne peuvent pas savoir avec certitude si l'exception relative aux logiciels libres s'applique à eux ou non. Par prudence et pour éviter des actions en responsabilité inabordables, ces entreprises ou initiatives s'abstiendraient alors, le cas échéant, de développer des logiciels libres.

C'est également le cas des grandes entreprises dont les services juridiques vont interdire aux services R&D&I de publier leur code source en open source, ou de participer à des projets open source, en présence de la moindre incertitude juridique.

Les fournisseurs de logiciels libres non européens pourraient aussi se retirer du marché européen et les entreprises françaises cesseraient de participer à des projets de logiciels libres dont l'industrie, la science et l'administration tirent actuellement d'immenses bénéfices.

Le CRA menace donc de créer un effet paralysant et de nuire considérablement à l'ensemble de l'écosystème de l'open source. Comme d'innombrables produits et solutions numériques sont construits sur des composants open source, on peut s'attendre à un effet domino négatif pour l'ensemble de l'économie du logiciel.

Menace d'atteinte à l'économie et à la souveraineté numérique

Cela ralentirait les PME et les start-up en particulier et aurait des effets négatifs significatifs sur la concurrence et la vitesse d'innovation. Comme les logiciels libres jouent également un rôle central dans la science, l'incertitude juridique ou la surréglementation causée par la CRA aurait également des conséquences négatives sur la recherche et l'enseignement, ainsi que sur la collaboration et le transfert de l'innovation entre la recherche et l'industrie. Les fondations open source, qui jouent un rôle central (sans but lucratif) pour de nombreux projets open source, seraient également menacées par le CRA.

Concernant les logiciels libres, le CRA manquerait donc son objectif et atteindrait le contraire de ce pour quoi il a été conçu. Au lieu d'avoir des logiciels libres plus sûrs, nous aurions des logiciels libres moins nombreux et surtout moins sûrs.

II. Nos recommandations pour le trilogue

Afin d'éviter ces effets secondaires indésirables, quelques suggestions concrètes sont présentées ci-dessous sur la manière dont les formulations actuelles, encore floues ou problématiques, peuvent être améliorées afin que la collaboration des parties commerciales et non commerciales de l'écosystème du logiciel libre dans le cadre du CRA puisse également être autorisée à l'avenir.

1) Modèle de développement - Considérant 10

Le texte de la commission ITRE du Parlement européen dispose que « *la question de savoir si un produit libre a été mis à disposition dans le cadre d'une activité commerciale devrait être évaluée produit par produit, en examinant à la fois le modèle de développement et la phase de fourniture du produit libre comportant des éléments numériques* ».

Cependant, un logiciel open source commercial est constitué de nombreux composants qui ont été développés de diverses manières (y compris sur une base bénévole). Le processus de développement est une longue chaîne qui peut durer plusieurs années et impliquer un nombre incalculable d'acteurs et d'organisations. Le fournisseur du produit final peut n'avoir été impliqué que dans une partie du processus de développement, voire pas du tout. Il est donc pratiquement impossible pour le vendeur de disposer de toutes les informations relatives à chaque étape du processus de développement et de décider si l'exception relative aux logiciels libres s'applique ou non à son cas. La complexité des différents modèles de développement open source n'est donc pas suffisamment prise en compte par le CRA à ce stade.

Le texte du Conseil de l'Union européenne est donc plus approprié : "*Les circonstances dans lesquelles le produit a été développé ou la manière dont le développement a été financé ne devraient pas être prises en compte pour déterminer la nature commerciale ou non commerciale de cette activité.*

Le modèle de développement ne doit pas jouer un rôle dans le fait qu'un produit soit considéré comme « commercial ». La proposition de texte du de l'Union européenne doit donc être privilégiée dans le trilogue.

2) Développement et maintenance par une seule organisation - Considérant 10 bis

Le texte de la commission ITRE du Parlement européen dispose que "*par exemple, un modèle de développement entièrement décentralisé, dans lequel aucune entité commerciale n'exerce de*

contrôle sur ce qui est accepté dans la base de code du projet, devrait être considéré comme une indication que le produit a été développé dans un cadre non commercial.

En revanche, lorsque des logiciels libres sont développés par une seule organisation ou par une communauté asymétrique, où une seule organisation génère des revenus à partir de l'utilisation de ces logiciels dans le cadre de relations commerciales, il faut considérer qu'il s'agit d'une activité commerciale.

Ce cas des logiciels libres qui ne sont développés et maintenus que par une seule organisation ou une communauté dominée par l'engagement d'une seule organisation s'applique à une grande partie des projets open source, en particulier aux PME du secteur des logiciels libres.

En revanche, certaines grandes entreprises telles que les GAFAM bénéficieraient de la formulation et, en cas de doute, il leur est possible de contourner cette exigence par le biais de filiales, etc., tandis que la majorité des PME ne relèveraient pas de l'exception relative aux logiciels libres et seraient donc touchées de manière disproportionnée.

La définition « lorsque les logiciels libres sont développés par une seule organisation… » doit donc être supprimée.

3) Développeurs de logiciels employés par des projets commerciaux - Considérant 10a.

Le texte de la commission ITRE du Parlement européen précise au considérant 10a : « *De même, lorsque les principaux contributeurs à des projets de logiciels libres sont des développeurs employés par des entités commerciales et lorsque ces développeurs ou l'employeur peuvent exercer un contrôle sur les modifications qui sont acceptées dans la base de code, le projet devrait généralement être considéré comme étant de nature commerciale* ».

Cela ferait automatiquement tomber sous le coup du CRA de nombreux projets open source dans lesquels des personnes participent au développement et à la maintenance du logiciel et qui sont employées et rémunérées pour leur travail dans ce contexte ou dans un autre. En d'autres termes, dès que l'un des développeurs a un emploi, quel qu'il soit, le projet open source est considéré comme « commercial ».

Cette définition pose problème, car de nombreux développeurs à temps plein participent également, à titre bénévole, à d'autres projets open source, dont certains sont complètement différents. Cela s'applique également, par exemple, à de nombreuses personnes impliquées dans les grandes fondations open source. De nombreuses entreprises, dont beaucoup de PME et de micro-entreprises, profitent énormément du travail bénévole des initiatives open source et vice versa. Les entreprises, à leur tour, participent à la maintenance et à la sécurité des logiciels en demandant à leurs employés de contribuer à des projets bénévoles individuels. Cette participation du plus grand nombre possible de développeurs aux projets open source est dans l'intérêt de toutes les parties concernées et

contribue à l'amélioration des logiciels. L'imbrication d'acteurs et d'organisations bénévoles et commerciaux constitue l'écosystème de l'open source.

Dans la pratique, cependant, la règle proposée aurait pour conséquence que les personnes employées (éventuellement ailleurs) cesseraient de s'impliquer dans des projets open source bénévoles. En somme, cela conduirait à des logiciels moins sûrs plutôt qu'à des logiciels plus sûrs.

La formulation du texte de l'Union européenne déjà mentionnée au point 1) est donc la meilleure ici aussi : « *Les circonstances dans lesquelles le produit a été développé ou la manière dont le développement a été financé ne devraient pas être prises en compte pour déterminer la nature commerciale ou non commerciale de cette activité* ».

La définition « lorsque les principaux participants aux projets libres et open source sont des développeurs employés par des sociétés commerciales » doit donc être supprimée. La proposition de texte de l'Union européenne doit être privilégiée dans le trilogue.

4) Dons - Considérant 10 ter

Le texte de la commission ITRE dispose que les dons à un projet open source peuvent constituer une « activité commerciale » : « *L'acceptation de dons sans intention de réaliser un profit ne devrait pas être considérée comme une activité commerciale, à moins que ces dons ne soient faits par des entités commerciales et qu'ils soient récurrents par nature*. »

Une grande partie des projets open source repose sur des dons (provenant également d'acteurs commerciaux), ce qui est vrai pour les projets logiciels individuels, les grandes fondations open source telles que la Fondation Linux, la Fondation Eclipse, la Fondation Apache, la Fondation Python, la *Free Software Foundation* et bien d'autres encore, ainsi que pour les développeurs bénévoles individuels. Un projet logiciel stable et durable préférera les « dons récurrents » pour son financement, car cela garantit la prévisibilité et la stabilité à long terme du projet. La stabilité des projets open source est dans l'intérêt de toutes les parties concernées et contribue à rendre les logiciels plus sûrs, ce dont dépendent de larges pans de l'économie du numérique.

De nombreuses entreprises utilisent des logiciels ou des composants logiciels développés par des particuliers et des organisations qui s'appuient sur des dons récurrents. Par conséquent, si ces organisations devaient cesser de fonctionner parce qu'elles sont soumises aux exigences du CRA mais ne peuvent pas les respecter (de nombreuses fondations ou projets ne disposent pas des ressources et du personnel suffisants pour le faire), la définition mentionnée ici couperait une grande partie des entreprises du secteur du logiciel de leur chaîne d'approvisionnement en logiciels libres.

La définition basée sur les dons récurrents d'organisations commerciales doit donc être supprimée.

5) Gestionnaire de paquets (« package managers ») - Considérant 10

Le texte de la commission ITRE du Parlement européen dispose que « *le seul fait d'héberger des logiciels libres sur des dépôts ouverts ne constitue pas en soi une mise à disposition sur le marché d'un produit contenant des éléments numériques. En tant que tels, la plupart des gestionnaires de paquets, des plateformes d'hébergement de code et de collaboration ne devraient pas être considérés comme des distributeurs au sens du présent règlement.* »

Le terme « la plupart » signifie ici qu'il n'est pas du tout clair quels gestionnaires de paquets relèvent de l'exception et lesquels n'en relèvent pas. Il en résulte une grande insécurité juridique. Il est donc urgent de supprimer le terme « la plupart ».

Le texte du Conseil de l'Union européenne est un peu plus clair : « *Un gestionnaire de paquets, un hébergeur de code ou une plateforme de collaboration qui facilite le développement et la fourniture de logiciels n'est considéré comme un distributeur que s'il met ce logiciel à disposition sur le marché et le fournit donc pour distribution ou utilisation sur le marché de l'Union dans le cadre d'une activité commerciale* ». En effet, il est précisé ici dans quels cas concrets l'exception ne doit pas s'appliquer.

Bien que les deux versions laissent place à l'interprétation, et donc à des incertitudes juridiques, la proposition de texte du Conseil de l'Union européenne, qui définit concrètement les cas dans lesquels les gestionnaires de paquets ne sont pas concernés par l'exception, devrait être privilégiée.

III. Nos recommandations au gouvernement français

Maintenant que la commission compétente au Parlement européen (ITRE) et le Conseil de l'Union européenne ont finalisé leurs positions à la mi-juillet 2023, les négociations finales du trilogue sur le CRA devraient débuter en septembre 2023.

Lors des prochaines négociations du trilogue, le gouvernement français doit veiller à ce que l'écosystème open source et donc des parties importantes de l'économie informatique française et européenne, ainsi que la souveraineté numérique de la France, soient protégés de manière adéquate dans le CRA. À cette fin, un échange avec les représentants de l'industrie des logiciels libres est essentiel.

La CRA ne devrait pas tenir pour responsable le créateur d'un logiciel open source, mais le « metteur en circulation » ou l'utilisateur qui offre un service avec ce logiciel, s'il est facturé ou si un modèle commercial est basé sur ce logiciel.

Lors des négociations au Parlement européen, le comité consultatif pour le marché intérieur et la protection des consommateurs (IMCO) avait formulé une bien meilleure exception pour les logiciels libres. Les formulations du texte final du de l'Union européenne sont également en partie mieux adaptées à la protection de l'écosystème des logiciels libres.

Elles devraient servir de base au trilogue et être préférées aux formulations de la commission ITRE.

Le CNLL offre son expertise dans la perspective des négociations du trilogue et est toujours disponible pour des échanges et des consultations.

A propos de ce document

Cette prise de position sur le CRA a été élaborée par le CNLL sur la base de nos discussions avec de nombreuses organisations de l'écosystème open source, et notamment nos partenaires européens réunis au sein de l' APELL (Association Professionnelle Européenne du Logiciel Libre) qui représente la filiere européenne du logiciel libre à Bruxelles.

Nous avons notamment utilisé le document Stellungnahme zum Cyber Resilience Act de l'OSBA, notre homologue allemand, comme point de départ de ce texte.

Voir aussi

- 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)