

## Le Cyber Resilience Act adopté en trilogue, le logiciel libre est-il sauvé ?

### Description

**Amendée au fil des mois de discussions, la version du règlement qui a fait consensus au sein des instances européennes répond en partie aux critiques exprimées par les acteurs du monde du logiciel libre ou open source. Restent quelques éléments de flou quant à la portée précise de certains amendements.**

Connu sous son nom anglais de Cyber Resilience Act (CRA), le projet de règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques risquait « de nuire à l'écosystème du logiciel libre ou open source », notamment par l'imposition d'obligations difficilement compatibles avec le mode de fonctionnement de ce dernier ([voir La rem n°65-66, p.21](#)). Plusieurs associations de défense du logiciel libre ou open source avaient fait part, dans une lettre ouverte adressée le 17 avril 2023 à la Commission européenne, de leur profonde inquiétude quant à l'avenir du secteur en cas d'adoption en l'état de la proposition initiale<sup>1</sup>. Depuis, au fil des débats au sein du Parlement européen et du Conseil de l'Union européenne, puis du trilogue conclu par un accord politique le 30 novembre 2023 entre ces deux institutions et la Commission européenne, le texte a évolué<sup>2</sup>. Plusieurs propositions visant à offrir des garanties de sécurité juridique aux projets de logiciel libre ou open source, dont les caractéristiques compliquent la conformité aux mesures prévues dans le CRA, ont été introduites. Sont-elles suffisantes pour répondre à toutes les craintes émises par le secteur ? Si les groupes d'intérêt qui défendent le logiciel libre ou open source s'annoncent satisfaits dans l'ensemble<sup>3</sup>, il demeure toutefois quelques zones d'ombre, notamment autour de l'introduction de nouveaux termes, comme celui de « *open source software steward* » (que nous pourrions traduire par « intendant de logiciel open source » en l'attente de la traduction officielle du compromis adopté en trilogue).

### Une proposition initiale inadaptée au modèle de développement du libre ou de l'open source

Jusqu'ici, la plupart des textes européens portant sur le fonctionnement de produits et services numériques ont encadré les usages. Le règlement général de protection des données (RGPD) oblige les responsables du traitement de données à caractère personnel à respecter certains principes, comme la transparence des traitements à l'égard des personnes concernées, la possibilité pour celles-ci d'exercer certains droits – notamment celui d'accéder à leurs données –, ainsi qu'à mettre en place une démarche de conformité par la tenue de registres. Les directives NIS (Network & Information Security) puis NIS2 ont imposé le respect de mesures de sécurité informatique à des opérateurs de services essentiels et de secteurs critiques. Mais ces textes ne s'appliquent pas, pour l'essentiel, aux producteurs de matériel informatique et de logiciels qui sont utilisés. C'est ce que la proposition de CRA vise à corriger, en imposant à ces derniers des obligations en matière de cybersécurité allant de la recherche de vulnérabilité à l'analyse de risques en passant par des

---

obligations de certification ou encore de notification de vulnérabilités à un centre de réponse aux incidents de sécurité informatique.

Le CRA attribue ainsi des responsabilités aux fabricants de produits informatiques, dont les logiciels. Dans l'univers des logiciels dits « propriétaires », l'identification du fabricant ne pose généralement pas de difficulté, et celui-ci dispose en principe de moyens financiers tirés de la commercialisation de ses produits, qu'il peut réinvestir dans une démarche de conformité qu'il contrôle. Ce n'est majoritairement pas le cas pour les logiciels libres, souvent disponibles gratuitement, et dont le développement repose souvent sur la contribution d'un nombre important de contributeurs souvent volontaires<sup>4</sup>. Les acteurs du secteur ont exprimé la crainte que leur activité soit interdite si le texte de la proposition initiale de la Commission était adopté en l'état.

Seul le considérant 10 de la proposition initiale précisait qu'« *afin de ne pas entraver l'innovation ou la recherche, les logiciels libres et ouverts développés ou fournis en dehors du cadre d'une activité commerciale ne devraient pas être couverts par le présent règlement* ». Cette formule est apparue très restrictive, d'autant que la notion d'activité commerciale n'était même pas clairement définie. De plus, cette exemption, présente dans les considérants, n'était pas reprise à l'article 2 définissant le champ d'application matériel du CRA. Or, conformément à une jurisprudence constante de la Cour de justice de l'Union européenne, si les considérants permettent d'aider à l'interprétation des articles des actes dérivés adoptés par l'Union, ils sont dépourvus de valeur juridique indépendante.

### **Une meilleure sécurité juridique à l'égard du libre et de l'open source malgré quelques interrogations persistantes**

Le compromis issu des négociations en trilogie – et qui sera probablement adopté et promulgué en l'état – introduit des évolutions substantielles touchant à la fois au champ d'application matériel du CRA et à la façon dont il entend encadrer le respect par les acteurs du logiciel libre ou open source de leurs obligations en matière de cybersécurité.

En premier lieu, l'article 2 paragraphe 1 du compromis prévoit que le texte ne s'applique qu'aux seuls produits comportant des éléments numériques « mis sur le marché » (« *made available on the market* »). L'article 3 (23) précise que la « mise sur le marché », à titre onéreux ou gratuit, doit être entendue comme étant liée à une activité commerciale. Le considérant 10 amendé précise que, bien qu'une prestation payante de services en lien avec un logiciel distribué gratuitement soit une activité commerciale couverte par le règlement, cela ne vaut que si le service est facturé au-delà de son prix de revient. De plus, plusieurs nouveaux considérants, pour l'instant numérotés 10b à 10f, indiquent que le règlement doit être interprété dans un sens qui tienne compte des caractéristiques particulières du modèle de développement libre ou open source, décrites en reformulant les fameuses « quatre libertés » du logiciel libre telles que définies par Richard Stallman<sup>6</sup> : liberté d'utiliser, de modifier, de redistribuer et de partager ses améliorations. Le simple fait qu'un projet libre ou open source reçoive des financements pour aider à son développement ne suffit pas à faire de ce projet une activité commerciale. Les personnes physiques qui contribuent bénévolement sans

---

avoir le moindre contrôle sur le projet dans son ensemble ne sont pas concernées par les obligations du CRA en revanche, les personnes qui intègrent des logiciels libres dans le cadre d'une activité commerciale le seront. Par exemple, Alphabet (Google), qui intègre le noyau Linux dans son système d'exploitation Android, devra se conformer au texte. En revanche, la Linux Foundation, qui soutient sans but lucratif le développement de ce noyau de système d'exploitation Linux, ne sera concernée que par les dispositions applicables aux « *open-source software stewards* », que nous traduirons ici, en l'attente d'une traduction officielle publiquement disponible, par l'expression d'« intendants de logiciels open source ».

Un nouvel article – actuellement numéroté 17a – prévoit des obligations allégées à l'égard de ces « *open-source software stewards* ». Ils devront publier une politique de cybersécurité, coopérer avec les autorités de surveillance du marché (en France, la DGCCRF, Direction générale de la concurrence, de la consommation et de la répression des fraudes) et notifier les vulnérabilités dont ils auront connaissance aux centres de réponse aux incidents de sécurité informatique. Ils ne pourront en revanche pas, aux termes des dispositions de l'article 53 (10a), être l'objet d'amendes administratives. Enfin, l'article 17b prévoit une possibilité de certification volontaire des logiciels libres ou open source, selon des modalités que la Commission devra établir par acte délégué.

L'ensemble des amendements relatifs au logiciel libre ou open source retenus à l'issue du trilogue sont marqués par une intention claire de ne pas entraver le développement de ces « communs numériques », auquel le nouveau considérant 10d attribue un rôle majeur dans le niveau général de cybersécurité. Cet objectif a toutefois été équilibré en évitant que des logiciels, y compris des logiciels libres, faisant l'objet d'une exploitation commerciale, ne soient exclus du champ d'application du CRA. L'ensemble des dispositions paraît globalement protecteur pour les acteurs du secteur. Néanmoins, certains nouveaux concepts, comme celui d'« *open-source software steward* », prêtent encore à interprétation. Conscients de la confusion que le texte peut engendrer, les auteurs du texte de compromis ont prévu, à l'article actuellement numéroté 17c (2) (a), d'enjoindre la Commission à publier des lignes directrices clarifiant la manière dont le CRA s'appliquera au logiciel libre ou open source.

Sources :

1. « Open Letter to the European Commission on the Cyber Resilience Act », fondation Eclipse, [newsroom.eclipse.org](https://newsroom.eclipse.org), April 17, 2023.
2. Notre analyse ici se fonde sur la note 17000/23 du Conseil de l'Union européenne, rédigé le 20 décembre 2023 par le secrétariat général du Conseil. Ce texte a été approuvé par la commission ITRE (Commission de l'industrie, de la recherche et de l'énergie) du Parlement européen, en charge du dossier, le 23 janvier 2024, mais le vote en session plénière et la promulgation du texte n'étaient pas encore intervenus au moment d'écrire ces lignes.
3. Voir le communiqué de presse d'OpenForum Europe, [openforumeurope.org/eu-cyber-resilience-act-takes-a-leap-forward](https://openforumeurope.org/eu-cyber-resilience-act-takes-a-leap-forward)
4. Broca Sébastien, *Utopie du logiciel libre. Du bricolage informatique à la réinvention sociale*, Le Passager clandestin, 2013.
5. Klimas Tadas, Vaiciukaite Jurate, « The Law of Recitals in European Community Legislation », *ILSA Journal of International & Comparative Law*

, vol. 15, July 14, 2008.

6. Broca Sébastien, *Utopie du logiciel libre*, *op. cit.*

### **Categorie**

1. Droit

**date créée**

3 mai 2023

**Auteur**

julienrossi