Le Cyber Resilience Act adoptÃ© en trilogue, le logiciel libre est-il sauvÃ© ?

Description

AmendÃ©e au fil des mois de discussions, la version du rÃ¨glement qui a fait consensus au sein des instances europÃ©ennes rÃ©pond en partie aux critiques exprimÃ©es par les acteurs du monde du logiciel libre ou open source. Restent quelques Ã©lÃ©ments de flou quant Ã la portÃ©e prÃ©cise de certains amendements.

Connu sous son nom anglais de Cyber Resilience Act (CRA), le projet de rÃ¨glement concernant des exigences horizontales en matiÃ¨re de cybersÃ©curitÃ© pour les produits comportant des Ã©lÃ©ments numÃ©riques risquait Â« de nuire Ã lâ€™Ã©cosystÃ¨me du logiciel libre ou open source Â», notamment par lâ€™imposition dâ€™obligations difficilement compatibles avec le mode de fonctionnement de ce dernier (voirÂ *La remÂ* nÂ°65-66, p.21). Plusieurs associations de dÃ©fense du logiciel libre ou open source avaient fait part, dans une lettre ouverte adressÃ©e le 17 avril 2023 Ã la Commission europÃ©enne, de leur profonde inquiÃ©tude quant Ã lâ€™avenir du secteur en cas dâ€™adoption en lâ€™Ã©tat de la proposition initiale[1]. Depuis, au fil des dÃ©bats au sein du Parlement europÃ©en et du Conseil de lâ€™Union europÃ©enne, puis du trilogue conclu par un accord politique le 30 novembre 2023 entre ces deux institutions et la Commission europÃ©enne, le texte a Ã©voluÃ©[2].Â Plusieurs propositions visant Ã offrir des garanties de sÃ©curitÃ© juridique aux projets de logiciel libre ou open source, dont les caractÃ©ristiques compliquent la conformitÃ© aux mesures prÃ©vues dans le CRA, ont Ã©tÃ© introduites.Â Sont-elles suffisantes pour rÃ©pondre Ã toutes les craintes Ã©mises par le secteur ? Si les groupes dâ€™intÃ©rÃªt qui dÃ©fendent le logiciel libre ou open source sâ€™annoncent satisfaits dans lâ€™ensemble[3],Â il demeure toutefois quelques zones dâ€™ombre,Â notamment autour de lâ€™introduction de nouveaux termes, comme celui de Â«Â *open source software stewardÂ* Â» (que nous pourrions traduire par Â« intendant de logiciel open source Â» en lâ€™attente de la traduction officielle du compromis adoptÃ© en trilogue).

Une proposition initiale inadaptÃ©e au modÃ¨le de dÃ©veloppement du libre ou de lâ€™open source

Jusquâ€™ici, la plupart des textes europÃ©ens portant sur le fonctionnement de produits et services numÃ©riques ont encadrÃ© les usages. Le rÃ¨glement gÃ©nÃ©ral de protection des donnÃ©es (RGPD) oblige les responsables du traitement de donnÃ©es Ã caractÃ¨re personnel Ã respecter certains principes, comme la transparence des traitements Ã lâ€™Ã©gard des personnes concernÃ©es, la possibilitÃ© pour celles-ci dâ€™exercer certains droits â€“ notamment celui dâ€™accÃ©der Ã leurs donnÃ©es â€“, ainsi quâ€™Ã mettre en place une dÃ©marche de conformitÃ© par la tenue de registres. Les directives NIS (Network & Information Security) puis NIS2 ont imposÃ© le respect de mesures de sÃ©curitÃ© informatique Ã des opÃ©rateurs de services essentiels et de secteurs critiques. Mais ces textes ne

sâ€™appliquent pas, pour lâ€™essentiel, aux producteurs de matÃ©riel informatique et de logiciels qui sont utilisÃ©s. Câ€™est ce que la proposition de CRA vise Ã corriger, en imposant Ã ces derniers des obligations en matiÃ¨re de cybersÃ©curitÃ© allant de la recherche de vulnÃ©rabilitÃ© Ã lâ€™analyse de risques en passant par des obligations de certification ou encore de notification de vulnÃ©rabilitÃ©s Ã un centre de rÃ©ponse aux incidents de sÃ©curitÃ© informatique.

Le CRA attribue ainsi des responsabilitÃ©s aux fabricants de produits informatiques, dont les logiciels.Â Dans lâ€™univers des logiciels dits Â« propriÃ©taires Â», lâ€™identification du fabricant ne pose gÃ©nÃ©ralement pas de difficultÃ©, et celui-ci dispose en principe de moyens financiers tirÃ©s de la commercialisation de ses produits, quâ€™il peut rÃ©investir dans une dÃ©marche de conformitÃ© quâ€™il contrÃ´le.Â Ce nâ€™est majoritairement pas le cas pour les logiciels libres, souvent disponibles gratuitement,Â et dont le dÃ©veloppement repose souvent sur la contribution dâ€™un nombre important de contributeurs souvent volontaires[4]. Les acteurs du secteur ont exprimÃ© la crainte que leur activitÃ© soit interdite si le texte de la proposition initiale de la Commission Ã©tait adoptÃ© en lâ€™Ã©tat.

Seul le considÃ©rant 10 de la proposition initiale prÃ©cisait quâ€™Â«Â *afin de ne pas entraver lâ€™innovation ou la recherche, les logiciels libres et ouverts dÃ©veloppÃ©s ou fournis en dehors du cadre dâ€™une activitÃ© commerciale ne devraient pas Ãªtre couverts par le prÃ©sent rÃ¨glementÂ* Â». Cette formule est apparue trÃ¨s restrictive, dâ€™autant que la notion dâ€™activitÃ© commerciale nâ€™Ã©tait mÃªme pas clairement dÃ©finie. De plus, cette exemption, prÃ©sente dans les considÃ©rants, nâ€™Ã©tait pas reprise Ã lâ€™article 2 dÃ©finissant le champ dâ€™application matÃ©riel du CRA. Or, conformÃ©ment Ã une jurisprudence constante de la Cour de justice de lâ€™Union europÃ©enne, si les considÃ©rants permettent dâ€™aider Ã lâ€™interprÃ©tation des articles des actes dÃ©rivÃ©s adoptÃ©s par lâ€™Union, ils sont dÃ©pourvus de valeur juridique indÃ©pendante.

Une meilleure sÃ©curitÃ© juridique Ã lâ€™Ã©gard du libre et de lâ€™open source malgrÃ© quelques interrogations persistantes

Le compromis issu des nÃ©gociations en trilogue â€“ et qui sera probablement adoptÃ© et promulguÃ© en lâ€™Ã©tat â€“ introduit des Ã©volutions substantielles touchant Ã la fois au champ dâ€™application matÃ©riel du CRA et Ã la faÃ§on dont il entend encadrer le respect par les acteurs du logiciel libre ou open source de leurs obligations en matiÃ¨re de cybersÃ©curitÃ©.

En premier lieu, lâ€™article 2 paragraphe 1 du compromis prÃ©voit queÂ le texte ne sâ€™applique quâ€™aux seuls produits comportant des Ã©lÃ©ments numÃ©riques Â« mis sur le marchÃ© Â»Â (Â«Â *made available on the marketÂ* Â»). Lâ€™article 3 (23) prÃ©cise que la Â« mise sur le marchÃ© Â», Ã titre onÃ©reux ou gratuit, doit Ãªtre entendue comme Ã©tant liÃ©e Ã une activitÃ© commerciale. Le considÃ©rant 10 amendÃ© prÃ©cise que, bien quâ€™une prestation payante de services en lien avec un logiciel distribuÃ© gratuitement soit une activitÃ© commerciale couverte par le rÃ¨glement, cela ne vaut que si le service est facturÃ© au-delÃ de son prix de revient. De plus, plusieurs nouveaux considÃ©rants, pour lâ€™instant numÃ©rotÃ©s 10b Ã 10f, indiquent que le rÃ¨glement doit Ãªtre interprÃ©tÃ© dans un

sens qui tienne compte des caractÃ©ristiques particuliÃ¨res du modÃ¨le de dÃ©veloppement libre ou open source, dÃ©crites en reformulant les fameuses Â« quatre libertÃ©s Â» du logiciel libre telles que dÃ©finies par Richard Stallman[6]Â : libertÃ© dâ€™utiliser, de modifier, de redistribuer et de partager ses amÃ©liorations.Â Le simple fait quâ€™un projet libre ou open source reÃ§oive des financements pour aider Ã son dÃ©veloppement ne suffit pas Ã faire de ce projet une activitÃ© commerciale.Â Les personnes physiques qui contribuent bÃ©nÃ©volement sans avoir le moindre contrÃ´le sur le projet dans son ensemble ne sont pas concernÃ©es par les obligations du CRA en revanche, les personnes qui intÃ¨grent des logiciels libres dans le cadre dâ€™une activitÃ© commerciale le seront. Par exemple, Alphabet (Google), qui intÃ¨gre le noyau Linux dans son systÃ¨me dâ€™exploitation Android, devra se conformer au texte. En revanche, la Linux Foundation, qui soutient sans but lucratif le dÃ©veloppement de ce noyau de systÃ¨me dâ€™exploitation Linux, ne sera concernÃ©e que par les dispositions applicables aux Â«Â *open-source software stewardsÂ* Â», que nous traduirons ici, en lâ€™attente dâ€™une traduction officielle publiquement disponible, par lâ€™expression dâ€™Â« intendants de logiciels open source Â».

Un nouvel article â€“ actuellement numÃ©rotÃ© 17a â€“ prÃ©voit des obligations allÃ©gÃ©es Ã lâ€™Ã©gard de ces Â«Â *open-source software stewardsÂ* Â».Â Ils devront publier une politique de cybersÃ©curitÃ©, coopÃ©rer avec les autoritÃ©s de surveillance du marchÃ© (en France, la DGCCRF, Direction gÃ©nÃ©rale de la concurrence, de la consommation et de la rÃ©pression des fraudes) et notifier les vulnÃ©rabilitÃ©s dont ils auront connaissance aux centres de rÃ©ponse aux incidents de sÃ©curitÃ© informatique. Ils ne pourront en revanche pas, aux termes des dispositions de lâ€™article 53 (10a), Ãªtre lâ€™objet dâ€™amendes administratives. Enfin, lâ€™article 17b prÃ©voit une possibilitÃ© de certification volontaire des logiciels libres ou open source, selon des modalitÃ©s que la Commission devra Ã©tablir par acte dÃ©lÃ©guÃ©.

Lâ€™ensemble des amendements relatifs au logiciel libre ou open source retenus Ã lâ€™issue du trilogue sont marquÃ©s par une intention claire deÂ ne pas entraver le dÃ©veloppement de ces Â« communs numÃ©riques Â»,Â auquel le nouveau considÃ©rant 10d attribue un rÃ´le majeur dans le niveau gÃ©nÃ©ral de cybersÃ©curitÃ©. Cet objectif a toutefois Ã©tÃ© Ã©quilibrÃ© en Ã©vitant que des logiciels, y compris des logiciels libres, faisant lâ€™objet dâ€™une exploitation commerciale, ne soient exclus du champ dâ€™application du CRA. Lâ€™ensemble des dispositions paraÃ®t globalement protecteur pour les acteurs du secteur. NÃ©anmoins, certains nouveaux concepts, comme celui dâ€™Â«Â *open-source software stewardÂ* Â», prÃªtent encore Ã interprÃ©tation. Conscients de la confusion que le texte peut engendrer, les auteurs du texte de compromis ont prÃ©vu, Ã lâ€™article actuellement numÃ©rotÃ© 17c (2) (a), dâ€™enjoindre la Commission Ã publier des lignes directrices clarifiant la maniÃ¨re dont le CRA sâ€™appliquera au logiciel libre ou open source.

Sources :

1. Â« Open Letter to the European Commission on the Cyber Resilience Act Â», fondation Eclipse, newsroom.eclipse.org, April 17, 2023.
2. Notre analyse ici se fonde sur la note 17000/23 du Conseil de lâ€™Union europÃ©enne, rÃ©digÃ© le 20 dÃ©cembre 2023 par le secrÃ©tariat gÃ©nÃ©ral du Conseil. Ce texte a Ã©tÃ© approuvÃ©

par la commission ITRE (Commission de lâ€™industrie, de la recherche et de lâ€™Ã©nergie) du Parlement europÃ©en, en charge du dossier, le 23 janvier 2024, mais le vote en session plÃ©niÃ¨re et la promulgation du texte nâ€™Ã©taient pas encore intervenus au moment dâ€™Ã©crire ces lignes.
3. Voir le communiquÃ© de presse dâ€™OpenForum Europe, openforumeurope.org/eu-cyber-resilience-act-takes-a-leap-forward
4. Broca SÃ©bastien,Â *Utopie du logiciel libre. Du bricolage informatique Ã la rÃ©invention sociale*, Le Passager clandestin, 2013.
5. Klimas Tadas, Vaiciukaite Jurate, Â« The Law of Recitals in European Community Legislation Â»,Â *ILSA Journal of International & Comparative Law*, vol. 15, July 14, 2008.
6. Broca SÃ©bastien,Â *Utopie du logiciel libre, op. cit.*

Categorie

1. Droit

date crÃ©Ã©e
3 mai 2023
Auteur
julienrossi