Le Cyber Resilience ActÂ : une menace pour leÂ logiciel libreÂ ?

Description

Le 17 avril 2023, treize groupes dâ€™intÃ©rÃªt du secteur du logiciel libre et de lâ€™open source ont signÃ© une lettre ouverte adressÃ©e Ã la Commission europÃ©enne[1]Â pour lâ€™alerter sur leurs craintes Ã lâ€™Ã©gard de la proposition de rÃ¨glement concernant des exigences horizontales en matiÃ¨re de cybersÃ©curitÃ© pour les produits comportant des Ã©lÃ©ments numÃ©riques et modifiant le rÃ¨glement (UE) 2019/1020[2].

PrÃ©sentÃ© en septembre 2022, le projet de rÃ¨glement connu sous le nom anglais de Cyber Resilience Act (CRA) prÃ©voit des obligations en matiÃ¨re de sÃ©curitÃ© Ã tous lesÂ *Â«Â produits comportant des Ã©lÃ©ments numÃ©riques dont lâ€™utilisation prÃ©vue ou raisonnablement prÃ©visible comprend une connexion directe ou indirecte, logique ou physique, Ã un dispositif ou Ã un rÃ©seauÂ Â»*Â (art. 2 (1) du rÃ¨glement proposÃ©).Â En clairÂ : il vise Ã sâ€™assurer que tous les logiciels et matÃ©riels connectÃ©s mis sur le marchÃ© dans lâ€™Union europÃ©enne (UE) apportent des garanties minimales en matiÃ¨re de sÃ©curitÃ© informatique.

De nombreux cas existent dÃ©jÃ , pour lesquels des obligations de sÃ©curitÃ© informatique sâ€™imposent. Câ€™est le cas en vertu de lâ€™article 32 du rÃ¨glement gÃ©nÃ©ral de protection des donnÃ©es (RGPD), applicable au traitement des donnÃ©es Ã caractÃ¨re personnel. Câ€™est aussi le cas pour les opÃ©rateurs de services essentiels, couverts par la directive Network Information Security (NIS)[3]. Mais de nombreux logiciels, dont ceux embarquÃ©s dans des objets connectÃ©s, ne sont toujours soumis Ã aucune rÃ©glementation spÃ©cifique en matiÃ¨re de cybersÃ©curitÃ©.

Le souhait dâ€™une amÃ©lioration de la sÃ©curitÃ© des produits numÃ©riques en Europe est partagÃ© par les signataires de la lettre ouverte. Alors pourquoi craignent-ils les effets de cette proposition de rÃ¨glement ?

Pour le comprendre, il est utile de rappeler les caractÃ©ristiques du logiciel libre ou open source, de son modÃ¨le de dÃ©veloppement et de ses modÃ¨les dâ€™affaires. Nous verrons ainsi que le projet de Cyber Resilience Act lâ€™apprÃ©hende difficilement, justifiant des amendements qui visent Ã crÃ©er une exemption au bÃ©nÃ©fice du logiciel libre ou open source plus large que celle actuellement prÃ©vue.

Les logiciels libres : des biens communs souvent dÃ©veloppÃ©s par uneÂ communautÃ© informelle

Le mouvement du logiciel libre est nÃ© dâ€™abord aux Ã‰tats-Unis dans les annÃ©es 1980. Il conÃ§oit les logiciels comme des biens communs[4]. Il sâ€™est structurÃ© autour de la Free Software Foundation,

fondÃ©e en 1985 par lâ€™informaticien Richard Stallman. Celui-ci dÃ©finit le logiciel libre comme rÃ©pondant Ã quatre caractÃ©ristiques socio-techniques, quâ€™il appelle lesÂ Â«Â quatre libertÃ©sÂ Â», usuellement numÃ©rotÃ©es de 0 Ã 3[5]Â :

1. la libertÃ© dâ€™utiliser le logiciel pour tout usage ;
2. la libertÃ© dâ€™Ã©tudier le logiciel pour en comprendre le fonctionnement et le modifier pour lui faire faire ce que veut son utilisateur ;
3. la libertÃ© de redistribuer le logiciel et dâ€™en faire des copies, dans un objectif altruiste de partage ;
4. la libertÃ© dâ€™amÃ©liorer le programme et de partager ses amÃ©liorations avec le public.

Cette dÃ©finition est dâ€™ailleurs rappelÃ©e au considÃ©rant 10Â du projet de Cyber Resilience Act, qui dÃ©finit les logiciels libres commeÂ *Â«Â logiciels, y compris leurs codes sources et versions modifiÃ©es, qui sont librement partagÃ©s et accessibles, utilisables, modifiables et redistribuablesÂ Â»*.

Les logiciels ditsÂ Â«Â open sourceÂ Â»Â ont gÃ©nÃ©ralement les mÃªmes caractÃ©ristiques, mais ce terme est considÃ©rÃ© comme plus neutre idÃ©ologiquement. Il a Ã©tÃ© inventÃ© pour rendre la mÃ©thode de dÃ©veloppement des logiciels libres[6]Â â†’ qui repose sur lâ€™interaction entre un noyau dur de dÃ©veloppeurs et des contributions dâ€™une communautÃ© dâ€™utilisateurs[7]Â â†’, acceptable aux yeux des dirigeants dâ€™entreprises. Parler deÂ Â«Â logiciel open sourceÂ Â»Â revient donc Ã parler deÂ Â«Â logiciel libreÂ Â», sans revendiquer le projet politique portÃ© par la Free Software Foundation.

Pour rÃ©sister Ã lâ€™extension du droit de la propriÃ©tÃ© intellectuelle aux programmes dâ€™ordinateurs accÃ©lÃ©rÃ©e par lâ€™adoption du Computer Software Copyright Act de 1980 aux Ã‰tats-Unis, Richard Stallman a inventÃ© leÂ *copyleft*.Â Il sâ€™agit dâ€™une clause insÃ©rÃ©e dans un contrat de licence, obligeant quiconque modifiant ou redistribuant un logiciel libre Ã le faire selon les mÃªmes conditions. Elle sert Ã empÃªcher la privatisation dâ€™un logiciel que ses auteurs considÃ¨rent comme un bien commun. Ainsi, avant dâ€™Ãªtre une innovation technique, le logiciel libre est surtout une innovation juridique. Les logiciels open source, câ€™est-Ã -dire ceux qui ne revendiquent pas la dimension politique et militante du logiciel libre, prÃ©fÃ¨rent en gÃ©nÃ©ral dâ€™autres licences que la GNU General Public Licence de la Free Software Foundation, comme la licence BSD, qui ne contiennent pas deÂ *copyleft*[8]. En France comme dans le reste de lâ€™Union europÃ©enne[9], la violation dâ€™un contrat de licence dâ€™un logiciel libre constitue une contrefaÃ§on[10]. Toute la difficultÃ© rÃ©side dans lâ€™identification des auteurs et titulaires de droits dâ€™auteurs, qui, avec le Cyber Resilience Act, se doublera dâ€™une difficultÃ© Ã identifier un unique fabricant.

Lâ€™Ã©diteur dâ€™un logiciel propriÃ©taire est gÃ©nÃ©ralement clairement identifiÃ©. Celui-ci signe des contrats avec ses employÃ©s, ses sous-traitants, et ses clients, qui peuvent, en cas de dysfonctionnement, engager sa responsabilitÃ© contractuelle. Les choses se compliquent avec le logiciel libre. Ã€ titre dâ€™exemple, les contributeurs Ã la version 5.10 de Linux, noyau du systÃ¨me dâ€™exploitation GNU/Linux, auraient Ã©tÃ© prÃ¨s de deux mille[11]. La majeure partie nâ€™est pas

employÃ©e par la Linux Foundation. La plupart des projets libres ou open source, comme Yarn â^’ un gestionnaire de modules initialement crÃ©Ã© par Facebook et utilisÃ© dans de nombreux logiciels Javascript â^’ ou OpenSSL â^’ une bibliothÃ¨que de chiffrement trÃ¨s largement utilisÃ©e pour sÃ©curiser les sites web â^’, sont maintenus par des communautÃ©s informelles de contributeurs parfois bÃ©nÃ©voles, parfois payÃ©s par un employeur qui voit un intÃ©rÃªt au suivi dâ€™une brique technique Ã©lÃ©mentaire dont il dÃ©pend.

Or, les logiciels libres ne sont pas immunisÃ©s contre les failles de sÃ©curitÃ©. En 2014, la faille Heartbleed, dÃ©tectÃ©e dans la librairie OpenSSL, avait affectÃ© de trÃ¨s nombreux sites web, y compris ceux de Facebook, Google et Twitter[12].Â Les auteurs de logiciels libres ou open source nâ€™ont toutefois, Ã ce jour, aucune obligation ou responsabilitÃ© Ã lâ€™Ã©gard de leurs utilisateurs, sauf si une faute intentionnelle est dÃ©montrÃ©e.

Une volontÃ© de responsabiliser les fabricants de logiciels qui peinent Ã Â sâ€™adapter au logiciel libre

Le RGPD, le Digital Services Act et le Digital Markets Act sont des textes emblÃ©matiques de la politique de lâ€™Union europÃ©enne dans le secteur du numÃ©rique ces derniÃ¨res annÃ©es. Aucun de ces textes nâ€™impose toutefois dâ€™obligations aux Ã©diteurs de logiciels en tant que tels. Les rÃ©centes propositions de rÃ¨glement sur lâ€™intelligence artificielle (IA)[13], le projet de directive sur la responsabilitÃ© en matiÃ¨re dâ€™IA[14], la proposition de directive relative Ã la responsabilitÃ© du fait des produits dÃ©fectueux[15]Â et le projet de Cyber Resilience Act suivent une logique diffÃ©rente.

Ainsi, la proposition de Cyber Resilience Act, par son article 10, entend imposer aux fabricants de produits (*hardware*Â commeÂ *software*) comportant des Ã©lÃ©ments numÃ©riques une si longue liste dâ€™obligations que nous relevons ici seulement les plus importantes dâ€™entre elles.Â Un fabricant devra ainsi sâ€™assurer que son produit est livrÃ© sans vulnÃ©rabilitÃ© connue, il devra conduire une Ã©valuation des risques, introduire des paramÃ¨tres par dÃ©faut sÃ©curisÃ©s et des mÃ©canismes pour rÃ©duire les consÃ©quences dâ€™une faille de sÃ©curitÃ©, conduire une Ã©valuation de la conformitÃ© selon une procÃ©dure Ã©tablie Ã lâ€™article 24 de la proposition, fournir les informations relatives Ã la sÃ©curitÃ© et garantir que les vulnÃ©rabilitÃ©s dÃ©couvertes feront lâ€™objet de mises Ã jour de sÃ©curitÃ©. Certaines obligations paraissent mÃªme un peu superflues car redondantes avec des rÃ¨gles prÃ©existantes. Ainsi, lâ€™annexe I, dans son alinÃ©a 1 (1) (3) (e), prÃ©voit que le fabricant respecte le principe de minimisation des donnÃ©esÂ *Â«Â Ã caractÃ¨re personnel ou autres*Â [sic]*Â Â»*[16] Â prÃ©vu Ã lâ€™article 5 du RGPD.

La conformitÃ© au Cyber Resilience Act risque dâ€™Ãªtre structurellement difficile pour les projets de logiciels libres ou open source, Ã©tant donnÃ© le mode de fonctionnement que nous avons prÃ©cÃ©demment exposÃ©. Une interprÃ©tation stricte du texte, sâ€™il Ã©tait adoptÃ© dans une version proche de la proposition initiale de la Commission, risquerait dâ€™aboutir Ã lâ€™interdiction dâ€™un grand nombre de briques logicielles libres pourtant essentielles au bon fonctionnement de

lâ€™Ã©cosystÃ¨me numÃ©rique, comme OpenSSL.Â Ceci amÃ¨ne certains Ã plaider pour une exemption trÃ¨s large au bÃ©nÃ©fice du logiciel libre.

Il nâ€™en existe guÃ¨re dans les articles de la proposition initiale.Â Seul le considÃ©rant 10 prÃ©cise 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 paraÃ®t trÃ¨s restrictive, puisquâ€™elle peut Ãªtre interprÃ©tÃ©e comme Ã©nonÃ§ant deux conditions cumulativesÂ : une finalitÃ© dâ€™innovation ou de recherche, et lâ€™absence dâ€™activitÃ© commerciale.

Ignorons la premiÃ¨re condition, que lâ€™on peut aussi comprendre comme une simple dÃ©claration dâ€™intention dÃ©pourvue de portÃ©e juridique, telle quâ€™il arrive dâ€™en trouver dans des considÃ©rants. Dans cette hypothÃ¨se, il est vrai que cette exemption concernera un grand nombre de personnes et, notamment, lâ€™ensemble des contributeurs bÃ©nÃ©voles Ã des projets de logiciels libres, ou toutes les associations Ã but non lucratif qui offrent un soutien matÃ©riel Ã certains de ces projets.Â Mais que se passe-t-il si, par exemple, un contributeur bÃ©nÃ©vole facture des prestations de conseils tirÃ©es de sa compÃ©tence sur le logiciel libre auquel il a contribuÃ© ?Â Il devrait alors sâ€™assurer de la conformitÃ© du logiciel auquel il contribue au Cyber Resilience Act, alors mÃªme quâ€™il nâ€™a en aucune maniÃ¨re de contrÃ´le effectif sur le projet dans son ensemble, ni les moyens â€“ voire les compÃ©tences â€“ de sâ€™assurer de la conformitÃ© du produit.

Pourtant, lâ€™activitÃ© commerciale est dÃ©finie de faÃ§on trÃ¨s large par la proposition. Le considÃ©rant 10 poursuit en effet en indiquant queÂ *Â«Â lâ€™activitÃ© commerciale peut Ãªtre caractÃ©risÃ©e non seulement par le prix facturÃ© pour un produit, mais Ã©galement par le prix des services dâ€™assistance technique, par la fourniture dâ€™une plateforme logicielle par lâ€™intermÃ©diaire de laquelle le fabricant monÃ©tise dâ€™autres services, ou par lâ€™utilisation de donnÃ©es Ã caractÃ¨re personnel pour des raisons autres quâ€™aux seules fins dâ€™amÃ©liorer la sÃ©curitÃ©, la compatibilitÃ© ou lâ€™interopÃ©rabilitÃ© du logicielÂ Â»*.

Or, ce nâ€™est pas parce que les logiciels libres ou open source sont librement disponibles quâ€™ils ne font lâ€™objet dâ€™aucune activitÃ© commerciale. En 2018, la sociÃ©tÃ© Red Hat Linux, avant son rachat par IBM, avait dÃ©clarÃ© un chiffre dâ€™affaires de prÃ¨s de 3 milliards de dollars[17]. La Commission estime sans doute quâ€™une telle entreprise devrait Ãªtre en mesure de supporter les coÃ»ts de la conformitÃ©, ce qui nous semble raisonnable. Mais tel nâ€™est pas le cas de la majoritÃ© des entreprises qui proposent des services commerciaux autour de logiciels libres. Une petite entreprise qui aide Ã dÃ©ployer correcÂtement une librairie comme OpenSSL, ou un designer web en freelance qui dÃ©ploie une installation dâ€™un systÃ¨me de gestion de contenus (Content Management System en anglais, ou CMS) libre comme WordPress ou Drupal devra-t-il supporter les coÃ»ts de la conformitÃ© du produit pour lequel il propose des services commerciaux ?

On le voit bien, le Cyber Resilience Act soulÃ¨ve de nombreuses interrogations. Il a Ã©tÃ© pensÃ© pour

imposer aux fabricants de logiciels propriÃ©taires, dont le code, fermÃ©, nâ€™est pas susceptible dâ€™audit, des rÃ¨gles horizontales de cybersÃ©curitÃ©. Mais, ce faisant, interprÃ©tÃ© strictement,Â il risque de nuire Ã lâ€™Ã©cosystÃ¨me du logiciel libre ou open source, alors que, de lâ€™aveu mÃªme de la Commission europÃ©enne, leÂ *Â«Â code source ouvert offre davantage de possibilitÃ©s pour renforcer la sÃ©curitÃ©, puisque le code peut Ãªtre librement inspectÃ© et amÃ©liorÃ©Â Â»*[18].

Plusieurs amendements visant Ã Ã©largir lâ€™exemption accordÃ©e au logiciel libre ou open source, et Ã lâ€™introduire dans les articles du rÃ¨glement ont Ã©tÃ© dÃ©posÃ©s en commission IMCO (Commission du marchÃ© intÃ©rieur et de la protection des consommateurs) et en commission ITRE (Commission de lâ€™industrie, de la recherche et de lâ€™Ã©nergie) du Parlement europÃ©en. Pour lâ€™heure, il est trop tÃ´t pour faire des pronostics sur les chances dâ€™aboutir de tels amendements.

SourcesÂ :

1. Lettre datÃ©e du 17 avril 2023, intitulÃ©e Â« Open Letter to the European Commission on the Cyber Resilience Act Â», disponible sur le site de la fondation Eclipse, newsroom.eclipse.org.
2. Voir la procÃ©dure 2022/0272 (COD).
3. Directive (UE) 2016/1148 du Parlement europÃ©en et du Conseil du 6 juillet 2016 concernant des mesures destinÃ©es Ã assurer un niveau Ã©levÃ© commun de sÃ©curitÃ© des rÃ©seaux et des systÃ¨mes dâ€™information dans lâ€™Union europÃ©enne.
4. Ce mouvement est Ã©tudiÃ© en France par SÃ©bastien Broca, auteur de lâ€™ouvrage *Utopie du logiciel libreÂ : du bricolage informatique Ã la rÃ©invention sociale*, Ã‰ditions du Passager clandestin, 2013.
5. Voir SÃ©bastien Broca,Â *Ibid*.
6. Mathias Klang, Â« Free software and open source : The freedom debate and its consequences Â», First Monday, vol. 10, nÂ° 5, mars 2005, firstmonday.org.
7. Eric Raymond, *The Cathedral and the Bazaar*, Sebastopol CA, Oâ€™Reilly, 1999.
8. Mathias Klang,Â *Ibid*.
9. CJUE, 5e ch., 18 dÃ©cembre 2019, IT Development SAS contre Free Mobile SAS, Aff. C-666/18.
10. Cass. 1re ch. civ., 5 octobre 2022, Entrâ€™Ouvert contre Orange, pourvoi nÂ° 21-15.386.
11. Jonathan Corbet, Â« Statistics from the 5.10 kernel development cycle Â», LWM.net, lwn.net, 14 December 2020.
12. MichaÃ«l Szadkowski, Â« Faille Heartbleed : les sites pour lesquels il est conseillÃ© de changer son mot de passe Â», lemonde.fr. 11 avril 2014.
13. Proposition de rÃ¨glement du Parlement europÃ©en et du Conseil Ã©tablissant des rÃ¨gles harmonisÃ©es concernant lâ€™intelligence artificielle et modifiant certains actes lÃ©gislatifs de lâ€™Union, COM (2021) 206 FINAL.
14. Proposition de directive du Parlement europÃ©en et du Conseil relative Ã lâ€™adaptation des rÃ¨gles en matiÃ¨re de responsabilitÃ© civile extracontractuelle au domaine de lâ€™intelligence

artificielle, COM/2022/496 FINAL.
15. Proposition de directive du Parlement europÃ©en et du Conseil relative Ã la responsabilitÃ© du fait des produits dÃ©fectueux, COM (2022) 495 FINAL.
16. Il est difficile dâ€™interprÃ©ter les termes Â« ou autres Â» introduits Ã lâ€™alinÃ©a 1 (1) (3) (e) de lâ€™annexe I de la proposition de la Commission, dans la mesure oÃ¹ le principe de minimisation des donnÃ©es ne sâ€™applique quâ€™aux donnÃ©es Ã caractÃ¨re personnel.
17. Â« Red Hat Reports Fourth Quarter and Fiscal Year 2018 Results Â», redhat.com, March 26, 2018.
18. Commission europÃ©enne, Â« StratÃ©gie europÃ©enne en matiÃ¨re de logiciels libres 2020 â€“ 2023 â€“ lâ€™esprit dâ€™ouverture Â», C (2020) 7149 FINAL, p. 2, commission.europa.eu.

Categorie

1. Droit

date crÃ©Ã©e
28 septembre 2023
Auteur
julienrossi