La protection qui hiérarchise

Le Cyber Resilience Act européen entend protéger les contributeurs bénévoles du logiciel libre en les excluant de son périmètre. En créant le statut juridique d'« Open Source Software Steward » réservé aux fondations, il introduit pourtant une hiérarchie inédite dans un écosystème historiquement polycentrique. Dès le 11 septembre 2026, les obligations de signalement des vulnérabilités s'appliqueront à tous les fabricants. Entre fondations protégées, intégrateurs contraints et mainteneurs isolés, la chaîne de valeur du logiciel libre se reconfigure sous pression réglementaire.

Par Alexandre Berge · 16 avril 2026 · 19 min de lecture · Analyse

Trois régimes pour un seul écosystème

Le règlement (UE) 2024/2847, publié au Journal officiel le 20 novembre 2024 et entré en vigueur le 10 décembre suivant, introduit des exigences horizontales de cybersécurité pour tous les « produits comportant des éléments numériques » commercialisés dans l'Union. Ses 71 articles et 130 considérants dessinent une architecture réglementaire qui traite l'open source selon trois régimes distincts dont l'asymétrie mérite examen.

Le premier régime concerne les **fabricants commerciaux** (article 13). Toute entreprise intégrant des composants open source dans un produit commercial est soumise à l'ensemble des obligations : évaluation des risques cyber, documentation technique, marquage CE, mise à disposition de correctifs de sécurité pendant au moins cinq ans. L'article 13, paragraphe 5, impose une obligation de diligence raisonnable lors de l'intégration de composants tiers, « y compris les composants de logiciels libres et ouverts qui n'ont pas été mis à disposition sur le marché dans le cadre d'une activité commerciale ». Plus notable encore, l'article 13, paragraphe 6, crée une obligation explicite de **partage des correctifs en amont** : le fabricant qui développe un correctif pour une vulnérabilité dans un composant open source doit partager « le code ou la documentation pertinents » avec la personne ou l'entité assurant la maintenance du composant d'origine.

Le deuxième régime s'applique aux « Open Source Software Stewards », définis à l'article 3, paragraphe 14, comme des personnes morales qui fournissent un soutien systématique et durable au développement de logiciels libres destinés à des activités commerciales. Les fondations Eclipse, Apache, Linux Foundation Europe, OW2 ou Python Software Foundation

relèvent de cette catégorie. L'article 24 leur impose des obligations allégées : documenter une politique de cybersécurité, coopérer avec les autorités de surveillance, signaler les vulnérabilités activement exploitées dans les conditions de l'article 14. Elles ne sont soumises ni au marquage CE, ni à l'évaluation de conformité, ni aux exigences essentielles de cybersécurité de l'annexe I. L'article 64, paragraphe 10, les **exempte de toute amende administrative**.

Le troisième régime est une absence de régime. Le considérant 18 exclut explicitement du champ d'application les logiciels libres non monétisés par leurs auteurs. Le simple fait de recevoir des dons sans intention lucrative ne constitue pas une activité commerciale. Le considérant 20 précise que le fait d'héberger du code sur une plateforme collaborative ne constitue pas en soi une mise sur le marché. Un mainteneur bénévole individuel qui publie du code sur GitHub sans en tirer de revenus n'est ni fabricant, ni steward. Le CRA ne lui impose rien.

L'asymétrie entre ces trois régimes se résume nettement. Le fabricant de l'article 13 supporte l'intégralité du dispositif (marquage CE, diligence raisonnable complète, signalement en 24 heures, partage upstream obligatoire en vertu de l'article 13, paragraphe 6, amende possible jusqu'à 15 millions d'euros ou 2,5 % du chiffre d'affaires). Le steward de l'article 24 n'est tenu qu'à la documentation d'une politique de cybersécurité et au signalement des vulnérabilités activement exploitées dans les projets qu'il soutient, sans marquage CE, sans diligence raisonnable sur les composants intégrés, et avec une immunité d'amende administrative (article 64, paragraphe 10). Le mainteneur bénévole reste hors champ.

> **Calendrier d'application du CRA**
>
> 1. 10 décembre 2024 : entrée en vigueur du règlement
> 2. 11 juin 2026 : application des dispositions sur la notification des organismes d'évaluation de conformité
> 3. 11 septembre 2026 : application des obligations de signalement des vulnérabilités (article 14)
> 4. 11 décembre 2027 : application complète de l'ensemble des obligations

Cette tripartition semble logique. Elle soulève pourtant une question que l'architecture réglementaire laisse ouverte : que se passe-t-il dans les interstices ? Le mainteneur de xz-utils, Lasse Collin, développeur finlandais bénévole qui maintenait seul un composant de compression intégré dans la quasi-totalité des distributions Linux, ne relevait d'aucun des trois régimes. L'attaque par ingénierie sociale qui a conduit à l'insertion d'une porte dérobée (CVE-2024-3094, score CVSS **10.0**) en mars 2024 a exploité précisément cette zone grise : un composant critique, un mainteneur épuisé qui déclarait publiquement que « cette activité n'est pas rémunérée », et un attaquant patient qui a construit sa crédibilité pendant trois ans avant de frapper. Le CRA place la responsabilité de la diligence raisonnable sur les fabricants

qui intègrent ce type de composant. Mais il ne crée aucun mécanisme de soutien pour le mainteneur lui-même, celui dont la défaillance compromet toute la chaîne.

L'isomorphisme institutionnel, grille de lecture d'une norme qui uniformise

> **Concept central : l'isomorphisme institutionnel (DiMaggio et Powell, 1983)**
>
> Dans « The Iron Cage Revisited : Institutional Isomorphism and Collective Rationality in Organizational Fields » (*American Sociological Review*, 48(2), p. 147-160), Paul DiMaggio et Walter Powell identifient trois mécanismes par lesquels les organisations d'un même champ institutionnel tendent à adopter des structures formelles similaires, indépendamment de leur efficacité fonctionnelle. L'isomorphisme **coercitif** résulte de pressions réglementaires et légales. L'isomorphisme **mimétique** procède de l'imitation en situation d'incertitude. L'isomorphisme **normatif** découle de la professionnalisation et de la standardisation. Le concept éclaire les situations où des acteurs très hétérogènes sont contraints de se conformer à des modèles organisationnels convergents.

Le CRA constitue un cas d'école d'isomorphisme coercitif appliqué aux communs numériques. La régulation européenne impose à des acteurs dont les formes organisationnelles, les motivations et les capacités diffèrent radicalement de converger vers des pratiques formelles homogènes : politique de cybersécurité documentée, traçabilité des vulnérabilités, processus de signalement en 24 heures via la plateforme unique de l'ENISA. Même le régime allégé des stewards exige une documentation « vérifiable » de la politique de cybersécurité (article 24, paragraphe 1), ce qui présuppose une organisation dotée de capacités juridiques et administratives.

Cette dynamique d'uniformisation heurte une caractéristique fondamentale de l'écosystème open source, décrite par Elinor Ostrom (*Governing the Commons*, 1990) et Yochai Benkler (*The Wealth of Networks*, 2006) : sa **gouvernance polycentrique**. Les communs logiciels fonctionnent historiquement grâce à une pluralité de modes d'organisation dont la diversité même garantit la résilience. Fondations formelles, communautés informelles, entreprises contributrices, développeurs indépendants coexistent dans des arrangements hétérogènes, adaptés localement. Le CRA, en créant une catégorie juridique formelle, tend à concentrer la légitimité réglementaire dans un petit nombre de fondations capables de satisfaire ses exigences documentaires.

L'Open Regulatory Compliance Working Group (ORC WG), lancé par la Fondation Eclipse en septembre 2024, illustre concrètement ce processus. Ce groupe rassemble plus de **50 membres** (Microsoft, Red Hat, GitHub, Google, Nokia, Mercedes-Benz, ainsi que les fondations Apache, Python, Blender et Rust). Il dispose d'une liaison formelle avec les organismes de normalisation CEN et CENELEC. Il participe au groupe d'experts CRA de la

Commission européenne (~60 membres). Il produit des spécifications, des livres blancs, des outils de conformité. En parallèle, l'OpenSSF et la Linux Foundation Europe ont lancé en janvier 2025 une initiative conjointe de préparation au CRA, assortie d'un cours gratuit et d'un groupe de travail « Global Cyber Policy » à réunions bimensuelles. Au FOSDEM 2026, le DevRoom « CRA in Practice » coorganisé par l'OpenSSF a permis à des acteurs comme Deutsche Bahn de présenter leurs processus de mise en conformité.

Ces initiatives sont utiles et témoignent d'une mobilisation efficace de l'écosystème. Elles posent toutefois une question d'économie politique. **Qui définit les normes de conformité applicables à l'ensemble des projets open source européens ?** Quelques fondations anglophones, disposant de budgets juridiques conséquents et d'un accès direct aux institutions bruxelloises, façonnent de facto les standards que devront respecter des dizaines de milliers de projets dans le monde. DiMaggio et Powell identifiaient déjà ce risque : l'isomorphisme institutionnel ne produit pas nécessairement l'efficacité, il produit la conformité formelle. Meyer et Rowan (1977) nommaient « découplage » le risque que des structures adoptées pour satisfaire des exigences réglementaires se déconnectent des pratiques réelles de sécurité. Un projet qui documente une politique de cybersécurité « vérifiable » sans disposer des moyens de l'appliquer satisfait la lettre du CRA sans en réaliser la finalité.

Le parallèle avec l'histoire de la régulation technologique renforce cette analyse. Dans les années 1990, les contrôles à l'exportation américains sur le chiffrement, conçus pour des munitions physiques, se sont révélés contre-productifs lorsqu'ils ont été appliqués au logiciel. Le CRA importe le modèle du marquage CE et de la directive Machines (conçu pour des produits physiques dont la sécurité s'évalue au moment de la fabrication) vers des produits logiciels dont la sécurité est un processus continu. L'innovation du CRA réside dans l'obligation de gestion des vulnérabilités tout au long du cycle de vie. La question est de savoir si l'infrastructure institutionnelle nécessaire à cette gestion continue peut émerger dans le délai imparti.

Ce que le RGPD enseigne sur l'impact différencié des normes européennes

Le précédent le plus éclairant pour anticiper les effets du CRA sur l'écosystème open source est le Règlement général sur la protection des données (RGPD), entré en application en mai 2018. Huit ans de recul permettent de documenter un effet différencié structurel entre grandes et petites organisations.

Une étude publiée par le CEPR (Chen et al., 2022) montre que les entreprises exposées au RGPD ont subi en moyenne une **réduction de 8 % de leurs profits** et une baisse de 2 % de leur chiffre d'affaires. Les grandes plateformes technologiques n'ont enregistré aucun impact significatif sur ces deux indicateurs. Parmi les petites entreprises du secteur IT, l'effet négatif

sur les profits a atteint le double de la moyenne. Une étude du NBER (Demirer et al., 2024) estime les coûts de conformité entre **1,7 million de dollars pour les PME et 70 millions pour les grandes entreprises**. Le George Washington University Regulatory Studies Center documente une hausse de 17 % de la concentration du marché dans la semaine suivant l'entrée en application du RGPD : les sites web ont abandonné les fournisseurs tiers de petite taille au profit de prestataires plus importants et conformes.

Anu Bradford (*The Brussels Effect*, Oxford University Press, 2020) a théorisé ce mécanisme : les normes européennes deviennent des standards mondiaux parce que les entreprises préfèrent adopter une conformité globale plutôt que maintenir des systèmes différenciés pour 450 millions de consommateurs. Le RGPD a inspiré des législations dans plus de cent juridictions. Mais la recherche met en lumière un paradoxe : l'industrie de la « privacy tech » créée par le RGPD est majoritairement dominée par des entreprises nord-américaines, et l'initiative de simplification du RGPD lancée par la Commission en 2025 reconnaît elle-même la charge disproportionnée sur les petites structures.

La transposition au CRA appelle la prudence. Les grandes fondations et les éditeurs majeurs disposent des équipes juridiques et techniques pour absorber les obligations de diligence raisonnable, de documentation et de signalement. Les **PME intégratrices françaises**, qui constituent le cœur du marché open source national (estimé à près de 6 milliards d'euros par le CNLL, avec plus de 64 000 emplois directs en 2023), risquent de supporter un coût de conformité disproportionné. Le guide CRA publié par le CNLL et inno³ (version 2.0, décembre 2025) relève une « maturité hétérogène » parmi les acteurs et des « craintes quant à la gestion de la responsabilité » pour les produits open source.

L'obligation de signalement en 24 heures (article 14, paragraphe 2) cristallise cette asymétrie. Un éditeur comme Red Hat dispose d'une équipe de réponse aux incidents fonctionnant en continu. Une PME intégratrice de dix salariés qui découvre une vulnérabilité activement exploitée dans un composant qu'elle a intégré doit notifier simultanément le CSIRT coordinateur national (le CERT-FR en France, rattaché à l'ANSSI) et l'ENISA via la plateforme unique de signalement. Le contrat de développement de cette plateforme a été attribué par l'ENISA le 22 décembre 2025 à un consortium mené par Uni Systems, pour **11 millions d'euros sur quatre ans**. La plateforme doit être opérationnelle le 11 septembre 2026 : moins de neuf mois séparent l'attribution du contrat de l'échéance réglementaire.

La France, puissance open source sans doctrine CRA

La France occupe la première place européenne sur le marché du logiciel libre, devant le Royaume-Uni et l'Allemagne. La politique publique du logiciel libre, portée par la DINUM à travers le Socle interministériel de logiciels libres (SILL) et la plateforme code.gouv.fr, constitue un acquis rare en Europe. La circulaire du Premier ministre du 27 avril 2021, le plan

d'action logiciels libres et communs numériques, la communauté BlueHats et le Conseil logiciels libres forment un dispositif institutionnel cohérent. La politique de contribution de l'État aux logiciels libres, publiée dès 2018 par la DINSIC (devenue DINUM), encourage les agents publics à contribuer aux projets existants.

Au moment où le CRA entre dans sa phase d'application, **aucune position publique coordonnée entre la DINUM et l'ANSSI sur l'articulation entre contribution open source publique et obligations du CRA n'a pu être identifiée**. L'ANSSI a publié une page d'information sur le CRA (cyber.gouv.fr), centrée sur son rôle d'autorité de notification des organismes d'évaluation de conformité et de coordination CSIRT via le CERT-FR. Son plan stratégique 2025-2027 positionne le CRA aux côtés du NIS2 et du DORA dans une logique de convergence réglementaire, mais sans traitement spécifique de l'open source. La DINUM poursuit sa mission de promotion du logiciel libre dans l'administration. La direction générale des Entreprises (DGE) a publié un guide d'information pour les entreprises. Mais ces trois acteurs n'ont produit aucune analyse conjointe sur l'impact du CRA sur la politique française de contribution upstream, ni sur le statut des administrations comme potentiels « fabricants » au sens de l'article 13.

La question est pourtant concrète. Lorsqu'un agent public contribue à un projet open source référencé au SILL dans le cadre de sa mission, dans quel régime CRA cette contribution s'inscrit-elle ? Si l'administration française utilise et modifie un composant open source dans un téléservice, l'État devient-il fabricant au sens du règlement ? La Commission européenne a publié le 3 mars 2026 un projet de lignes directrices (sous consultation jusqu'au 31 mars) qui aborde la question des stewards et du périmètre du logiciel libre, mais ce document, non contraignant, ne tranche pas le cas des administrations publiques contributrices.

Le contraste avec l'Allemagne est instructif. Le Sovereign Tech Fund (STF), créé en octobre 2022 sous l'égide du ministère fédéral de l'Économie, a investi **23,5 millions d'euros dans plus de 60 projets** d'infrastructure open source critique. Il finance directement des mainteneurs, des audits de sécurité, des programmes de résilience. Le mainteneur d'Apache Log4j, Christian Grobmeier, a reçu 596 160 euros du STF après des années de travail bénévole sur un composant dont la vulnérabilité Log4Shell (CVE-2021-44228, décembre 2021) avait touché 93 % des environnements cloud d'entreprise. Un projet d'extension européenne (EU-STF) propose un budget de 350 millions d'euros sur sept ans. Le STF constitue précisément le type de mécanisme capable de combler l'angle mort du CRA : **financer le troisième groupe**, celui des mainteneurs individuels, que la régulation ne peut ni contraindre ni protéger.

> **L'ombre portée des incidents passés**
>
> En dix ans, quatre incidents ont exposé la fragilité structurelle des composants open source critiques. Heartbleed (CVE-2014-0160, avril 2014) a révélé qu'OpenSSL, bibliothèque utilisée par 66 % des serveurs web, reposait sur un seul développeur à temps plein et recevait environ 2 000 dollars de dons annuels. La réponse institutionnelle (Core

> Infrastructure Initiative, puis OpenSSF) n'a pas empêché la répétition du scénario. Log4Shell (CVE-2021-44228, décembre 2021) a touché des centaines de millions d'appareils via un composant maintenu par une poignée de bénévoles. Le maintainer Volkan Yazici décrivait « des journées de 22 heures sans rémunération ». La backdoor xz-utils (CVE-2024-3094, mars 2024) a démontré qu'une opération d'ingénierie sociale de trois ans pouvait compromettre un composant intégré dans presque toutes les distributions Linux. L'incident event-stream (2018) avait déjà montré le même vecteur : un mainteneur épuisé transférant le contrôle de son projet à un inconnu qui y a injecté du code malveillant ciblant des portefeuilles Bitcoin.

Un second non-dit mérite attention. L'obligation de partage upstream de l'article 13, paragraphe 6, impose aux fabricants de transmettre « le code ou la documentation pertinents » au mainteneur d'origine lorsqu'ils corrigent une vulnérabilité. L'intention est vertueuse. Le risque est celui du « patch dumping » : des contributions de qualité inégale, soumises pour satisfaire une obligation légale, qui créent du bruit dans les processus de revue de code des projets amont et **alourdissent la charge de travail des mainteneurs** que le texte cherche précisément à protéger. La crise Log4Shell a montré cette dynamique à l'œuvre : les mainteneurs bénévoles ont été submergés de sollicitations après la divulgation publique, dans un contexte où les entreprises utilisant le composant n'avaient jamais contribué à son financement.

Une hypothèse à vérifier d'ici fin 2027

L'analyse développée dans cet article repose sur un cadre d'isomorphisme institutionnel qui conduit à formuler une prédiction testable. Si la dynamique identifiée par DiMaggio et Powell (1983) opère dans le champ de la régulation logicielle européenne, le CRA devrait produire trois effets observables d'ici la date d'application complète du 11 décembre 2027.

Premier indicateur : la **composition de la liste des entités reconnues comme Open Source Stewards**. Le projet de lignes directrices de la Commission (publié le 3 mars 2026) distingue trois niveaux de capacité parmi les stewards potentiels, allant des fondations non techniques aux organisations disposant de ressources d'ingénierie. Si l'isomorphisme coercitif opère, la très grande majorité des stewards reconnus seront des fondations anglophones disposant de ressources juridiques significatives. L'hypothèse peut être testée en examinant, à l'horizon de décembre 2027, la proportion d'organisations françaises ou d'Europe continentale parmi les stewards effectivement enregistrés. L'article de Mattis van 't Schip dans JIPITEC (2025) conclut que le CRA réalise un équilibre, mais « uniquement à travers une approche législative étroitement applicable et, parfois, complexe ». Cette complexité favorise structurellement les organisations dotées de capacités d'interprétation juridique.

Deuxième indicateur : le **taux de contribution individuelle aux projets référencés au SILL**

et sur code.gouv.fr. Si l'effet inhibiteur (« chilling effect ») anticipé par le CNLL dès septembre 2023 se matérialise, les contributeurs individuels situés dans l'Union européenne réduiront leur participation à des projets susceptibles de tomber dans le champ du CRA, par crainte d'une requalification en activité commerciale. Les données des forges publiques et de code.gouv.fr permettraient de mesurer cette évolution.

Troisième indicateur : l'**opérationnalité effective de la plateforme ENISA au 11 septembre 2026**. Le contrat de développement n'a été attribué que neuf mois avant l'échéance, pour un système qui doit interagir avec les CSIRT de 27 États membres et s'articuler avec les dispositifs NIS2 et DORA. Un retard significatif constituerait un signal de « découplage » au sens de Meyer et Rowan (1977) entre l'ambition normative du CRA et sa capacité réelle de mise en œuvre. L'étude de la Linux Foundation « Unaware and Uncertain » (2025) révélait déjà des lacunes significatives dans la préparation des communautés open source.

L'administration française, consommatrice et contributrice majeure de logiciel libre, dispose d'un intérêt stratégique direct à investir ce sujet avant que les normes de conformité ne soient définies sans elle. L'Open Forum Europe et la Python Software Foundation soulignent que le concept d'Open Source Steward, « idée entièrement nouvelle dans le droit européen », reste en construction. La fenêtre d'influence se refermera avec l'adoption des actes d'exécution et la finalisation des normes harmonisées CEN/CENELEC/ETSI, dont les premiers livrables sont attendus au troisième trimestre 2026. Les choix effectués dans les dix-huit prochains mois détermineront si la France sera actrice ou spectatrice de la recomposition réglementaire de l'écosystème open source européen.

Note méthodologique

Cet article s'appuie sur le texte consolidé du règlement (UE) 2024/2847 disponible sur EUR-Lex, les publications officielles de l'ENISA, de la Commission européenne et de l'ANSSI, les rapports des principales fondations open source, les données du CNLL et les publications académiques citées. Les recherches ont été conduites en avril 2026. L'absence de position publique coordonnée DINUM/ANSSI sur l'articulation CRA et open source a été vérifiée par recherche systématique sur les sites officiels, sans pouvoir exclure l'existence de documents de travail non publiés. Les chiffres économiques du marché open source français proviennent de l'étude CNLL/Numeum/MARKESS (2022) et des déclarations CNLL (2023).

Sources

Sources primaires institutionnelles

Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024, texte complet : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847

Commission européenne, « Cyber Resilience Act and open source software » : https://digital-strategy.ec.europa.eu/en/policies/cra-open-source

Commission européenne, projet de lignes directrices CRA (3 mars 2026) : https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16959-Draft-Commission-guidance-on-the-Cyber-Resilience-Act_en

Commission européenne, FAQ de mise en œuvre du CRA (3 décembre 2025) : https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions

Commission européenne, calendrier de mise en œuvre CRA (mis à jour le 4 mars 2026) : https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation

ENISA, plateforme unique de signalement (SRP) : https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp

ENISA, appel d'offres SRP (ENISA/2025/OP/0001) : https://www.enisa.europa.eu/procurement/implementation-of-the-single-reporting-platform

ANSSI, page CRA : https://cyber.gouv.fr/reglementation/cybersecurite-des-produits/cyber-resilience-act/

DINUM, plan d'action logiciels libres et communs numériques : https://code.gouv.fr/fr/plan-action-logiciels-libres-et-communs-numeriques/

Règlement d'exécution (UE) 2025/2392 (catégories de produits) : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R2392

Rapports officiels et publications des fondations

Eclipse Foundation, Open Regulatory Compliance Working Group : https://orcwg.org/

Eclipse Foundation, projet OCCTET (outils de conformité CRA financés par la Commission) : https://occtet.eu/

OpenSSF et Linux Foundation Europe, initiative CRA (31 janvier 2025) : https://www.linuxfoundation.org/press/openssf-and-lf-europe-launch-cra-initiative

Linux Foundation, rapport « Unaware and Uncertain : The Stark Realities of CRA Readiness in Open Source » : https://www.linuxfoundation.org/research/cra-readiness

OpenSSF, page de ressources CRA : https://openssf.org/public-policy/eu-cyber-resilience-act/

OpenSSF, « OSS and the CRA : am I a Manufacturer or a Steward ? » (2 juin 2025) : https://openssf.org/blog/2025/06/02/oss-and-the-cra-am-i-a-manufacturer-or-a-steward/

ORC WG, livre blanc « Stewards and CRA » : https://github.com/orcwg/orcwg/blob/main/

cyber-resilience-sig/whitepapers/stewards-and-cra.md

CNLL, déclaration sur le CRA (septembre 2023) : https://cnll.fr/news/declaration-cra-cyber-resilience-act/

CNLL/inno³, guide de conformité au CRA, version 2.0 (décembre 2025) : https://cnll.fr/news/guide-de-conformité-au-cyber-resilience-act-version-20/

Sovereign Tech Fund : https://www.sovereign.tech/

Open Forum Europe, « EU Cyber Resilience Act Takes a Leap Forward » : https://openforumeurope.org/eu-cyber-resilience-act-takes-a-leap-forward/

Cadres théoriques

DiMaggio, P. et Powell, W. (1983), « The Iron Cage Revisited : Institutional Isomorphism and Collective Rationality in Organizational Fields », *American Sociological Review*, 48(2), p. 147-160

Meyer, J. et Rowan, B. (1977), « Institutionalized Organizations : Formal Structure as Myth and Ceremony », *American Journal of Sociology*, 83(2), p. 340-363

Ostrom, E. (1990), *Governing the Commons : The Evolution of Institutions for Collective Action* , Cambridge University Press

Benkler, Y. (2006), *The Wealth of Networks : How Social Production Transforms Markets and Freedom*, Yale University Press

Bradford, A. (2020), *The Brussels Effect : How the European Union Rules the World*, Oxford University Press

Broca, S. et Coriat, B. (2015), « Le logiciel libre et les communs », HAL hal-01174746 : https://hal.science/hal-01174746

Publications académiques sur le CRA

van 't Schip, M. (2025), « The Cyber Resilience Act and Open-Source Software : A Fine Balancing Act », *JIPITEC*, 16(1) : https://www.jipitec.eu/jipitec/article/view/421

« The end of open source ? Regulating open source under the Cyber Resilience Act and the new Product Liability Directive » (2024), *Computer Law and Security Review* : https://www.sciencedirect.com/science/article/pii/S0267364924001705

Torres Ponce, M. E. (2025), « Open Source Under the Cyber Resilience Act : Compliance automation and governance models for sustainable security », SSRN : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5552760

Parallèles historiques et données empiriques

Chen, Z. et al. (2022), « The GDPR Effect : How Data Privacy Regulation Shaped Firm Performance Globally », CEPR/VoxEU

Demirer, M. et al. (2024), Working Paper, NBER/MIT Sloan

FOSDEM 2026, DevRoom « CRA in Practice » (31 janvier 2026) : https://fosdem.org/2026/schedule/track/cra-in-practice/

Presse spécialisée

GitHub, « What the EU's new software legislation means for developers » : https://github.blog/open-source/maintainers/what-the-eus-new-software-legislation-means-for-developers/

Python Software Foundation, « The EU's Proposed CRA Law May Have Unintended Consequences for the Python Ecosystem » (avril 2023) : https://pyfound.blogspot.com/2023/04/the-eus-proposed-cra-law-may-have.html

Python Software Foundation, mise à jour CRA (janvier 2024) : https://pyfound.blogspot.com/2024/01/CRA-update.html