Logiciel privateur de liberté… jusqu'à la prison ?

Dans le mode du logiciel libre, et contrairement à ce que le nom laisse suggérer, ce n'est pas le logiciel qui est libre, mais bien l'utilisateur du logiciel.

Le logiciel propriétaire, c'est-à-dire l'opposé du logiciel libre, est alors parfois appelé « logiciel privateur », car il prive l'utilisateur de certaines libertés fondamentales (étudier, exécuter, etc. le code source du programme).

Rebecca Wexler, étudiante dans l'école de droit de Yale (Yale Law School) nous montre ici qu'en plus ne nous priver de ces libertés qui peuvent parfois sembler bien futiles pour tout un chacun, ces logiciels peuvent compromettre le système judiciaire et nous priver ainsi de nos libertés fondamentales.

Condamnés par le code

par Rebecca Wexler

Source : Convicted by code (Slate)

Traduction :Vincent, McGregor, roptat, oS,Diane, CLC, touriste, teromene, Piup, Obny et anonymes.

Le code « secret » est partout : dans les ascenseurs, les avions, les appareils médicaux.

En refusant de publier le code source de leurs logiciels, les entreprises rendent impossible son inspection par des tiers, et ce même si le code a un impact énorme sur la société et la politique. Verrouiller l'accès au code empêche de connaître les failles de sécurité qui peuvent nous rendre vulnérables au piratage et à la fuite de données. Cela peut menacer notre vie privée en accumulant de l'information sur

nous à notre insu. Cela peut interférer avec le principe d'égalité devant la loi si le gouvernement s'en sert pour vérifier notre éligibilité à une allocation, ou nous inscrire sur une liste d'interdiction de vol. De plus, le code gardé secret permet le trucage des données et occulte les erreurs, comme dans l'affaire Volkswagen : l'entreprise a récemment avoué avoir utilisé un logiciel caché pour truquer les tests d'émission menés sur 11 millions de voitures, qui rejetaient l'équivalent de 40 fois la limite légale.

Mais aussi choquante que la fraude de Volkswagen puisse être, elle ne fait qu'en annoncer bien d'autres du même genre. Il est temps de s'occuper de l'un des problèmes de transparence technologique les plus urgents et les plus négligés : les programmes secrets dans le système judiciaire. Aujourd'hui, des logiciels fermés, propriétaires, peuvent vous envoyer en prison et même dans le couloir de la mort. Et dans la plupart des juridictions des États-Unis, vous n'avez pourtant pas le droit de les inspecter. Pour faire court, les procureurs ont le même problème que Volkswagen.

Prenons la Californie. Martell Chubbs est actuellement accusé de meurtre pour des faits remontant à 1977, dans lesquels la seule preuve contre lui est une analyse ADN effectuée par un logiciel propriétaire. Chubbs, qui dirigeait une petite entreprise de dépannage à domicile à l'époque de son arrestation, a demandé à inspecter le code source du logiciel afin de pouvoir contester la précision de ses résultats. Il cherchait à déterminer si le code implémente correctement les procédures scientifiques établies pour l'analyse ADN et s'il fonctionne comme son fabriquant le prétend. Mais ce dernier a affirmé que l'avocat de la défense pourrait voler ou dupliquer le code et causer des pertes financières à l'entreprise. Le tribunal a rejeté la requête de Chubbs, lui autorisant l'examen du rapport de l'expert de l'état, mais pas l'outil qu'il a utilisé. Des tribunaux de Pennsylvanie, Caroline du Nord, Floride et d'autres ont rendu des décisions similaires.

Nous devons faire confiance aux nouvelles technologies pour nous aider à trouver et condamner les criminels, mais aussi pour disculper les innocents. Les logiciels propriétaires interfèrent avec cette confiance dans de plus en plus d'outils d'investigation, des tests ADN aux logiciels de reconnaissance faciale et aux algorithmes qui indiquent à la police où chercher les futurs crimes. Inspecter les logiciels n'est cependant pas seulement bon pour les accusés : divulguer le code à des experts de la défense a permis à la Cour suprême du New Jersey de confirmer

la fiabilité scientifique d'un éthylotest.

Non seulement il est injuste de court-circuiter la possibilité pour la défense de contre-expertiser les preuves médico-légales, mais cela ouvre la voie à de mauvaises pratiques scientifiques. Les experts décrivent la contre-expertise comme « le meilleur instrument légal jamais inventé pour la recherche de la vérité ». Mais des révélations récentes ont révélé une épidémie de mauvaises pratiques scientifiques qui sapent la justice criminelle. Des études ont contesté la validité scientifique des recherche de similitudes sur les marques de morsure, les cheveux et les fibres, des diagnostics du syndrome du bébé secoué, de techniques balistiques, des séances d'identifications olfactives par des chiens, des preuves issues de l'interprétation de taches de sang, et des correspondances d'empreintes digitales. Le Massachusetts se démène pour gérer les retombées des falsifications de résultats par un technicien d'un laboratoire criminel qui a contaminé les preuves de dizaines de milliers d'affaires criminelles. Et le Projet Innocence rapporte que de mauvaises analyses légales ont contribué à l'incrimination injustifiée de 47% des prévenus. L'Académie Nationale des Sciences (National Academy of Sciences) accuse entre autres le manque de processus d'évaluation par les pairs dans les disciplines liées à l'analyse légale d'être responsable de cette crise.

Les logiciels ne sont pas non plus infaillibles. On a découvert des erreurs de programmation qui changent les ratios de probabilité des tests ADN d'un facteur 10, amenant des procureurs australiens à remplacer 24 avis d'experts dans des affaires criminelles. Quand les experts de la défense ont identifié une erreur dans le logiciel de l'éthylotest, la Cour suprême du Minnesota a invalidé le test en tant que preuve pour tous les futurs jugements. Trois des plus hautes cours de l'état (américain, NdT) ont encouragé à accepter davantage de preuves de failles dans des programmes, de manière à ce que les accusés puissent mettre en cause la crédibilité de futurs tests.

La contre-expertise peut aider à protéger contre les erreurs – et même les fraudes – dans la science et la technique de l'analyse légale. Mais pour que cet appareil judiciaire puisse fonctionner, l'accusé doit connaître les fondements des accusations de l'état. En effet, lorsque le juge fédéral de Manhattan, Jed S. Rakoff, a démissionné en signe de protestation contre la commission sur les sciences légales du président Obama, il a prévenu que si l'accusé n'a pas accès à toutes les informations pour effectuer une contre-expertise, alors le témoignage

d’un expert judiciaire n’est « rien d’autre qu’un procès par embuscade » (c.-à-d. sans accès préalable aux éléments de preuve, NdT).

La mise en garde de Rakoff est particulièrement pertinente pour les logiciels des outils d’analyse légale. Puisque éliminer les erreurs d’un code est très difficile, les experts ont adopté l’ouverture à l’analyse publique comme le moyen le plus sûr de garder un logiciel sécurisé. De manière identique, demander au gouvernement d’utiliser exclusivement des outils d’analyse légale ouverts permettrait leur contre-expertise participative. Les fabricants d’outils d’analyse légale, qui vendent exclusivement aux laboratoires d’expertise criminelle du gouvernement, peuvent manquer de motivations pour conduire les tests de qualité minutieux requis.

Pour en être certains, les régulateurs du gouvernement conduisent actuellement des tests de validation pour au moins quelques outils d’analyse légale numériques. Mais même les régulateurs peuvent être incapables d’auditer le code des appareils qu’ils testent, se contentant à la place d’évaluer comment ces technologies se comportent dans un environnement contrôlé en laboratoire. De tels tests « en boite noire » n’ont pas été suffisants à l’Agence de Protection de l’Environnement (*Environmental Protection Agency*) pour repérer la fraude de Volkswagen et ce ne sera pas non plus assez pour garantir la qualité des technologies numériques d’analyse légale.

La Cour suprême a depuis longtemps reconnu que rendre les procès transparents aide à s’assurer de la confiance du public dans leur équité et leur légitimité. Le secret de ce qu’il y a sous le capot des appareils d’informatique légale jette un doute sur ce processus. Les accusés qui risquent l’incarcération ou la peine de mort devraient avoir le droit d’inspecter les codes secrets des appareils utilisés pour les condamner.