Aaron Swartz et la criminalisation de la dissidence numérique par Jeremy Hammond

La mort tragique du combattant pour la liberté sur Internet Aaron Swartz révèle la stratégie ratée de « cyber sécurité » du gouvernement, ainsi que sa corruption systématique à travers ses enquêtes sur la criminalité informatique, la loi sur la propriété intellectuelle, et la transparence des corporations/gouvernements. Dans une société prétendument fondée sur les principes de démocratie et une « procédure légale régulière », les efforts d'Aaron pour libérer l'Internet, y compris la distribution gratuite d'essais JSTOR universitaires, l'accès aux archives judiciaires publiques sur PACER, l'arrêt du passage de la loi SOPA / PIPA, et le développement de la licence Creative Commons font de lui un héros, et non un criminel. Ce ne sont pas les « crimes » qu'Aaron aurait soi-disant commis qui ont fait de lui une cible de poursuites fédérales, mais ses idées – élaboré dans son manifeste « Guerrilla Open Access Manifesto » – que le gouvernement a trouvé tellement dangereux. La poursuite agressive du procureur général des États Unis, truffée d'abus et de mauvaise conduite, est ce qui a conduit à la mort ce héros. Ce chapitre triste et enrageant devrait servir de signal d'alarme nous éveillant tous sur le danger inhérent à notre système de justice pénale.

Le cas d'Aaron est une partie de la récente expansion agressive, politiquement motivée du droit criminel informatique où hackers et activistes sont de plus en plus criminalisés en raison de prétendues « cyber-menaces terroristes ». Le procureur général des États-Unis pour le district sud de New York, Preet Bharara, dont le bureau est en poursuite contre moi et mes co-accusés dans l'affaire du procès contre Lulzsec, a tenu un discours alarmiste, comme la menace d'une imminente « cyber-attaque à la Pearl Harbor » pour justifier ces poursuites. En même temps, le gouvernement forme et déploie régulièrement leurs propres pirates informatiques pour lancer des cyber-attaques sophistiquées contre les infrastructures des pays étrangers, tels que le virus Stuxnet et Flame, sans la connaissance, la consultation du public, ni déclaration de guerre officielle, ni le consentement des autorités internationales.

DARPA, US Cyber Command, la NSA et de nombreux contractants privés du gouvernement fédéral recrutent ouvertement les pirates pour développer les capacités défensives et offensives et construire des réseaux de surveillance numérique orwelliens, non conçus pour accroître la sécurité nationale, mais pour faire avancer l'impérialisme américain. Ils vont même jusqu'à assister et prendre la parole lors des conférences de pirates informatiques, comme DEFCON, tentent de soudoyer les hackerspaces pour leurs recherches, et ont créé l'insulte de la « Journée nationale du hacker civique » - efforts qui devraient être boycottés ou confrontés à chaque étape de leur parcours.

Aaron est un héros parce qu'il a refusé de suivre le programme du gouvernement, au lieu de cela il a utilisé son intelligence et sa passion pour créer une société transparente. Dans le cadre du mouvement du logiciel libre, la publication libre de droits, le partage de fichiers ouvert, et le développement de la cryptographie et de la technologie d'anonymat, les cyber-activistes ont révélé la pauvreté du néo-libéralisme et de la propriété intellectuelle. Aaron s'est opposé à réduire tout à une marchandise pouvant être achetée ou vendue pour un profit.

L'accroissement de l'efficacité du soutien du public pour des mouvements comme Anonymous et Wikileaks ont conduit à une expansion des enquêtes sur les crimes informatiques – surtout des améliorations à 18 USC § 1030, le *Computer Fraud and Abuse Act* (CFAA). Au fil des années, le CFAA a été modifié à cinq reprises et a subi un certain nombre de décisions judiciaires qui ont considérablement élargi ce que la loi couvre concernant « l'accès à un ordinateur protégé sans autorisation. » Il est désormais difficile de déterminer exactement quel comportement serait considéré comme juridique. La définition d'un «ordinateur protégé » a été progressivement élargie pour inclure tout gouvernement ou entreprise à l'intérieur ou

extérieur des États-Unis. « Autorisation », pas explicitement défini par le CFAA, a également été élargi pour être si équivoque que toute utilisation d'un site Web, réseau, ou un PC qui est en dehors des intérêts, de l'agenda, ou des obligations contractuelles d'une entité privée ou publique pourrait être criminalisée.

Dans le cas d'Aaron et d'autres, le gouvernement a défini la violation d'une Politique d'utilisation acceptable (PUA), de Conditions de Service (TOS), ou du Contrat de Licence Utilisateur Final (CLUF) comme illégale. Chaque fois que vous vous inscrivez à un service comme Gmail, Hotmail ou Facebook et cliquez sur le bouton « J'accepte » qui fait suite au long contrat d'utilisation que personne ne lit jamais, vous pourriez être poursuivi en vertu de la CAFA, si vous ne respectez pas les termes.

Le nombre massif d'usagers réguliers d'ordinateurs pouvant être considérés comme des criminels en vertu de ces définitions larges et ambigües permet des poursuites politiquement motivées de toute personne qui exprime sa dissidence. La CFAA devrait être jugée inconstitutionnelle en vertu de la doctrine vide et vague de la clause de procédure légale régulière. Au lieu de cela, le Congrès a proposé l'an dernier une loi qui permettrait de doubler les peines maximales légales et d'introduire des peines minimales obligatoires, semblables à des peines excessives imposées dans les affaires de drogue qui ont été largement imposées par de nombreux juges fédéraux et d'État.

Le cas de l'opération « Payback » à San José, en Californie, est un autre déni de justice, où 16 membres présumés d'Anonymous (dont un garçon de 16 ans) aurait participé à une action de déni de service contre PayPal pour protester contre le blocus financier de Wikileaks. Un déni de service (DOS ou DDOS) ne peut pas « dépasser accès autorisé», comme il est pratiquement impossible de le distinguer des requêtes Web standard. Il s'apparente plus à un sit-in de protestation électronique, la surcharge des serveurs du site Web le rendant incapable de servir le trafic légitime, à un acte criminel impliquant le vol d'informations privées ou la destruction de serveurs. Le site de PayPal est seulement devenu lent ou indisponible pour quelques heures, alors que ces activistes numériques font face à une peine de prison de plus que 10 ans, 250 000 dollars d'amende et les condamnations criminelles parce que le gouvernement veut criminaliser cette forme de protestation sur Internet et envoyer un avertissement à quiconque voudrait supporter Wikileaks.

Un autre cas récent est celui d'Andrew « Weev » Auernheimer, qui a été reconnu coupable en novembre dernier par l'entremise du CFAA. Andrew avait découvert que AT&T publiait les noms et adresses emails de clients sur son site web destiné au public, sans aucun mot de passe, cryptage, ou pare-feux. Au lieu de reconnaître leur propre erreur à violer la vie privée des clients, AT&T a poursuivi une peine de prison pour Andrew. Andrew a défendu ses actions en disant: « Nous n'avons pas seulement un droit, en tant qu'Américains d'analyser les choses que les sociétés publient et les rendre accessibles au public mais probablement aussi une obligation morale d'informer les gens à ce sujet. »

Je suis actuellement confronté à de multiples accusations de complot par piratage informatique à cause de mon implication présumée avec Anonymous, LulzSec et AntiSec, les groupes qui ont ciblés et dénoncé la corruption dans les institutions gouvernementales et les sociétés telles que Stratfor, le Ministère de la Sécurité publique d'Arizona, et HB Gary Federal. Ma peine encourue s'est vue abruptement alourdie à cause de l'élargissement par le Patriot Act de la définition du CFAA de « perte ». Ça a permis à Stratfor de réclamer plus de 5 millions de dollars en dommages et intérêts, y compris le coût exorbitant de l'embauche qui dépasse les limites de couverture des sociétés de crédit et des corporations « infosec », l'achat de nouveaux serveurs, 1,6 millions de dollars en « revenus potentiels perdus » pour le temps que leur site Web était hors fonction, et même le coût d'un arrangement financier de 1,3 millions de dollars pour un recours collectif déjà déposé contre eux. Couplé avec l'utilisation de « moyens sophistiqués » et « infrastructures essentielles » en tant qu'alourdisseurs de sentence, si reconnu coupable au procès, je fais face à une peine de 30 ans, allant jusqu'à vie.

Les sales tours judiciaires et des phrases longues ne sont pas des anomalies mais font partie du système fondamentalement corrompu et vicieux à deux vitesses de la « justice », qui vise à récolter des profits de l'incarcération de masse de millions de gens, et en particulier les personnes de couleur et les pauvres. L'utilisation d'agents doubles qui coopèrent en échange de peines plus légères n'est pas seulement utilisé

dans le cadre des poursuites répressives de mouvements de protestation et aux chasses aux sorcières « terroristes » islamophobes fabriquées, mais aussi dans la plupart des affaires de drogue, où les accusés font face à certaines des peines les plus sévères au monde .

Pour Aaron Swartz, qui faisait face lui-même à 13 chefs d'accusation sous la CFAA, il est fort probable que c'est cette pression intense de la part des procureurs implacables et sans compromis qui, tout en étant conscient de la fragilité psychologique d'Aaron, ont continué à réclamer une peine d'emprisonnement, ce qui a conduit à sa mort prématurée.

En raison de l'indignation généralisée du public, il y a maintenant des rumeurs d'enquêtes du Congrès dans le CFAA. Mais étant donné que ce même Congrès avait proposé des sanctions accrues il y a moins d'un an, les efforts de réforme ont peu de chances d'être plus que symboliques. Ce qu'il faut, ce n'est pas une réforme, mais une totale transformation; pas des amendements, mais une abolition. Aaron est un héros pour moi, parce qu'il n'a pas attendu que ceux au pouvoir réalisent sa vision et changent leur jeu, il a cherché à changer le jeu lui-même, et il l'a fait sans crainte d'être étiqueté comme criminel et emprisonné par un système judiciaire arriéré.

Nous, le peuple, exigeons un accès libre et équitable à l'information et à la technologie. Nous exigeons la transparence et la responsabilité de la part des gouvernements et des grandes entreprises, et que la vie privée des masses soit protégée des réseaux de surveillance envahissants.

Le gouvernement ne sera jamais pardonné. Aaron Swartz ne sera jamais oublié.

Source

freehammond.com

Pour écrire à Jeremy:

Jeremy Hammond 18729-424
Metropolitan Correctional Center
150 Park Row
New York, New York, 10007