La cryptographie et l'autoritarisme (Blog do Mauro Santayana)

Mauro SANTAYANA

8 mai 2015

Les États-Unis, qui se présentent, comme toujours, comme le paladin de la défense de la liberté et de la démocratie, viennent de demander à la communauté scientifique de mettre fin à la cryptographie, un processus qui permet aux utilisateurs d'ordinateurs de défendre leurs données des pirates, et de les protéger des États abusifs et autoritaires qui espionnent leurs propres citoyens comme les étrangers, ce qui est le cas des États-Unis.

Lors de la dernière conférence RSA, sur les systèmes de sécurité cybernétique, le Secrétaire pour la Sécurité Intérieure des EU, Jen Johnson, a lancé un appel aux techniciens et aux scientifiques présents, afin qu'ils développent une forme définitive pour « contourner et rendre caduque la cryptographie », afin de renforcer le pouvoir des organes de sécurité.

Le chemin le plus simple dans ce but est déjà tracé. L'avance rapide de l'informatique quantique rendra possible un nouveau type d'ordinateur, contre lequel la majorité des logiciels de cryptographie ne seront d'aucune utilité.

Il y a pourtant des pays et des organisations, anticipant la menace que ce type de machine pourrait occasionner aux libertés individuelles, qui s'organisent pour inciter au développent de nouveaux types de cryptographie capables de protéger les données dans l'univers futur de l'informatique quantique, avant même que les ordinateurs quantiques ne soient développés.

Échaudée par l'espionnage pratiqué contre certains de ses dirigeants, comme la chancelière Angela Merkel, l'Union Européenne ne semble pas être disposée à rester les bras croisés contre un immense Big Brother planétaire fomenté par le gouvernement étasunien, non pas dans le style de son homonyme imbécile (le *reality show* du même nom *NdT*), mais dans celui décrit par le roman prophétique de George Orwell *1984*.

La Commission Européenne vient de libérer des millions d'euros pour que soient développés des systèmes cryptographiques immunisés contre les ordinateurs quantiques, dans ce qui est déjà appelé la cryptographie « post-quantique ». N'importe quelle donnée qui devrait être protégée à un horizon de plus de dix ans nécessiterait déjà la garantie de ce système, puisque c'est le délai prévu pour l'entrée en service de l'informatique quantique par les gouvernements les plus avancés dans ce domaine.

Le Brésil, dont le gouvernement a été également la victime de l'espionnage étasunien, devrait se joindre à cet effort, en collaboration avec l'Union Européenne, ou en finançant de telles études au sein d'universités comme l'USP (Université de São Paulo).

Les EU allèguent qu'il est nécessaire d'éliminer la cryptographie pour se défendre des « terroristes » et des criminels.

La question est de savoir qui, dans le futur, déterminera qui est « terroriste » et qui est un combattant qui lutte, éventuellement, contre des états fascistes disposant de technologie de localisation des personnes, de reconnaissance faciale, de données biométriques, d'espionnage en masse des télécommunications et de l'internet.

Au nom de la liberté, il est primordial que cette prérogative appartienne à l'individu, et non au système.

Traduit par Lucien pour Si le Brésil m'était traduit...

»» http://www.maurosantayana.com/2015/04/a-criptografia-e-o-autoritarismo.html