HDD 3-Derecho y Política MARIA ROSA AVILA- UBA-

Democracia, Estado y Ciudadanía del siglo XXI. El Estado hackeado.

En el siglo XX ya nos alertaba Norberto Bobbio**4**, sobre los riesgos de la tecnocracia en relación con la Democracia, que consideraba antitéticas. Si el experto, es el protagonista no puede serlo un ciudadano o ciudadana común y corriente. Y si la democracia se basa en la hipótesis de que todos pueden tomar decisiones sobre todo; en sentido contrario, la tecnocracia pretende que los que tomen las decisiones sean los pocos que entienden de tales asuntos. En este sentido, en la actualidad dentro del proceso electoral, se pueden realizar controles, y se cuenta con indicadores de confiabilidad en su funcionamiento. Sin embargo, se instaura un posible cambio por un sistema de voto electrónico, en la necesidad aparente de adecuar y "actualizar" el sistema.

¿Es necesario pasar a un sistema de voto electrónico, en un país con un porcentaje de población como el nuestro? ¿Es necesario alejar del control del proceso eleccionario a cualquier ciudadano/a?. Es necesario modificar un sistema y proceso que cuenta con la confianza y credibilidad de parte de la ciudadanía? ¿Y si definimos cambiar utilizando una boleta única de papel? ¿Podría ser esta boleta una alternativa acertada e incluso de bajo costo? Ya hay experiencias de Estados donde se encuentra legalmente prohibido o paralizado como el caso de Alemania[1], Finlandia, Holanda, Irlanda, Kazajistán, Noruega y el Reino Unido. La Corte Suprema de Alemania en 2009 declaró inconstitucional la utilización de urnas electrónicas por no permitir el sistema de votación electrónica la fiscalización del proceso electoral por personas sin conocimientos técnicos. Del mismo modo, entre 2002 y 2007, el Reino Unido ha llevado a cabo más de treinta pruebas pilotos con diferentes sistemas de votación electrónica. Y una Comisión Electoral en 2008, ha declarado en base a las pruebas realizadas que la seguridad y garantías adoptadas eran insuficientes y determina no continuar con el voto electrónico.

Si los expertos afirman que una computadora construida específicamente para el sufragio es intrínsecamente insegura y no se puede garantizar que no pueda ser afectada por ciberataques o manipulaciones en momentos cruciales como el de emitir el voto (secreto), ni en el conteo de los mismos. Si el Estado puede ser víctima, y diversos Estados han sido hackeados en sus páginas web, agencias y recientemente hasta en hospitales como el caso de Inglaterra por Ransomware,[2]-malware- "gusano"-. Si las guerras pueden tener también escenarios dentro del mundo digital en el cual estamos inmersos. Y si la delincuencia puede tener como protagonistas, a individuos sin demasiados conocimientos técnicos que en la Internet profunda compran con moneda digital "bitcoin", un paquete con la gestión y servicios para realizar un ciberataque.

Es decir que si el mundo digital deja de ser un lugar próximo a Rousseau en tanto paradigma de Libertad; Igualdad y Fraternidad, para aproximarse al modelo de Hobbes, al brindar la posibilidad de convertirnos meramente en lobos y lobas. Si el mundo digital le brinda al Estado datos e información inédita sobre cada habitante. Si todo esto es posible, entonces el Estado de Derecho en el Mundo Digital se enfrenta a la tensión y dilema de la necesidad de garantizar la transparencia en la elección de sus gobernantes, gestionar y asegurar el universo de información privilegiada que posee de sus ciudadanos como nunca antes y a la vez conjurar su vulnerabilidad manifiesta a los ciberataques[3] y hackeos.

---

[1] http://www.euskadi.eus/botoelek/otros_paises/ve_mundo_paralizado_c.htm

[2] http://www.milenio.com/internacional/inglaterra-hospitales-ciberataque-ransomware-computadora-milenio-noticias_0_955104584.html

[3] http://www.excelsior.com.mx/global/2017/05/12/1163129