

La vigilancia masiva de personas en la lucha contra el COVID19. Enfoque político

Dr. **Francisco Bariffi**

Grupo de Investigación VIAR-DDHH

Vigilancia por Inteligencia Artificial, Robótica y Derechos
Humanos, Universidad Nacional de Mar del Plata, Argentina

bariffi@mdp.edu.ar

*“there are a number of impersonal
forces pushing in the direction of less
and less freedom”*

Aldous Huxley 1958

Edward Snowden



- Ley de Vigilancia de la Inteligencia Extranjera (FISA)



- El programa se ejecuta en forma conjunta con otros organismos internacionales de Australia y Nueva Zelanda, Canadá y Reino Unido.

- Ex consultor tecnológico de la CIA y NSA (USA)
- En junio de 2013, a través de los periódicos The Guardian y The Washington Post, Snowden hizo públicos documentos clasificados como alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM y Xkeyscore;
- Por ejemplo, los documentos liberados por Snowden muestran cómo el gobierno estadounidense espió a la canciller alemana Angela Merkel, o como en España, además de espiar al presidente del gobierno, también se espionaron más de 60 millones de llamadas entre ciudadanos españoles en menos de un mes.

Vigilancia Permanente (2019)



- Cambio de la vigilancia selectiva de individuos a la vigilancia masiva de poblaciones enteras;
- En secreto EEUU asumió el poder de la vigilancia masiva, una autoridad que, por definición, aflige mucho más la inocente que al culpable;
- “La libertad de un país solo puede calibrarse según el respeto que tiene por los derechos de sus ciudadanos, y estoy convencido de que esos derechos son en realidad limitaciones al poder estatal que definen exactamente dónde y cuándo un gobierno no debe invadir el terreno de libertades personales o individuales, que durante la revolución estadounidense se denominó “libertad” y en la revolución de internet se llama “privacidad”.



Snowden (Entrevista para Business Insider, Mar 27, 2020)

- <https://www.businessinsider.com/edward-snowden-coronavirus-surveillance-new-powers-2020-3>
- Los países han estado aumentando rápidamente su vigilancia de los ciudadanos para estudiar y frenar la propagación del virus, a través del mapeo de datos de ubicación de teléfonos anónimos a poderes altamente invasivos, como permitir que los servicios de seguridad rastreen los teléfonos de las personas sin una orden judicial;
- "Ya saben lo que estás viendo en Internet, ya saben dónde está y cómo se mueve tu teléfono, ahora saben cuál es tu frecuencia cardíaca. ¿Qué sucederá cuando comiencen a combinar estos datos y aplicarles inteligencia artificial?";
- Estos nuevos poderes cedidos a los Estados podrían permanecer vigentes una vez que finalice la pandemia.

Yuval Noah Harari



Cap. 3 Libertad
Los macrodatos
están
observándose

- Cambio de paradigma de la autoridad divina a la autoridad de los algoritmos de macrodatos;
- Confluencia de dos revoluciones inmensas. La biológica (neurociencia y biogenética). La informática con un poder de procesamiento de datos sin precedentes;
- La invención clave es el sensor biométrico que convierte procesos biológicos en información electrónica que los ordenadores pueden almacenar y analizar;
- El Riesgo: un régimen de vigilancia global que haga el seguimiento no solo de todas nuestras actividades y nuestras manifestaciones externas, sino también logre incluso metérsenos bajo la piel para conocer nuestras experiencias internas.

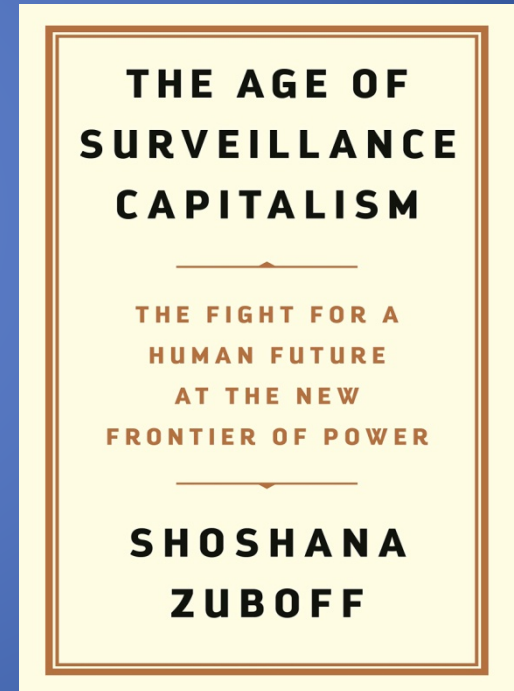
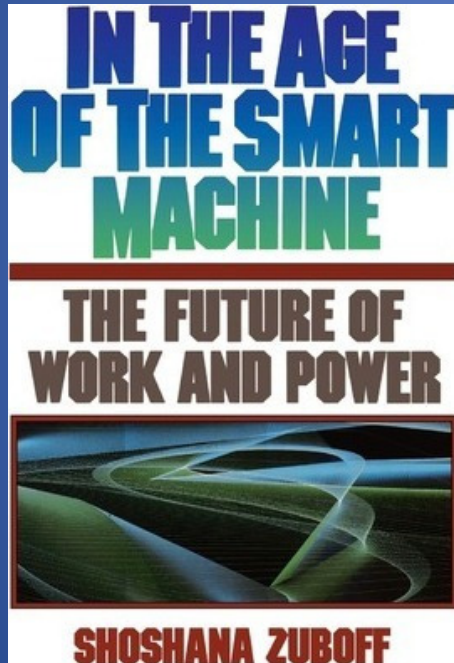
Yuval Harari “The world after coronavirus”, March 20, 2020. The Financial Times

Vigilancia bajo la piel

- Hoy, por primera vez en la historia humana, la tecnología hace posible monitorear a todos todo el tiempo;
- En su batalla contra la epidemia de coronavirus, varios gobiernos ya han implementado las nuevas herramientas de vigilancia;
- Las decisiones que en tiempos normales podrían llevar años de deliberación se aprueban en cuestión de horas. Se ponen en servicio tecnologías inmaduras e incluso peligrosas, porque los riesgos de no hacer nada son mayores;
- Sin embargo, si no tenemos cuidado, la epidemia podría marcar un hito importante en la historia de la vigilancia. No solo porque podría normalizar el despliegue de herramientas de vigilancia masiva en países que hasta ahora las han rechazado, sino aún más porque significa una transición dramática de la vigilancia “sobre la piel” a “bajo la piel”;
- La misma tecnología que identifica la tos también podría identificar risas;
- Pedirle a la gente que elija entre privacidad y salud es, de hecho, la raíz del problema. Porque esta es una elección falsa. Podemos y debemos disfrutar tanto de la privacidad como de la salud. Necesitamos un plan global

Shoshana Zuboff

- Prof. Escuela de Negocio de Harvard



Capitalismo de Vigilancia (2019)

- En el capitalismo de vigilancia, todos los aspectos de la experiencia humana se convierten en datos y se venden a una variedad de empresas por una variedad de razones (**Macrodatos tiene un gran Valor**);
- Después de 11 de septiembre de 2001, los esfuerzos para sancionar normas regulatorias de privacidad online fueron rechazados. Actualmente, hay muy pocas normas para proteger que los datos personales sean recopilados y vendidos, o utilizados para hacer dispositivos inteligentes predictivos más potentes (**Falta de normas**);
- El capitalismo de vigilancia se está volviendo más granular en su recopilación de datos (**Los sistemas se están haciendo cada vez mas precisos y efectivos**);
- Los capitalistas de vigilancia esperan momentos clave de sensibilidad social para aumentar las posibilidades de compra y modificación del comportamiento (**behaviorism**).
- Un futuro invasivo y de control absoluto del capitalismo de vigilancia no tiene que ser visto como inevitable.

Virtual Private Networks

(<https://www.top10vpn.com>)

- **COVID-19 Digital Rights Tracker (Datos al 12/05)**

In response to the outbreak of COVID-19:

- **Contact Tracing Apps** are being used in 28 countries
- **Alternative digital tracking measures** are active in 32 countries
- **Physical surveillance technologies** are in use in 10 countries
- **COVID-19-related censorship** has been imposed by 16 governments
- **Internet shutdowns** continue in 3 countries despite the outbreak

Contact Tracing Apps

- **Key Findings:**
- There are currently 47 contact tracing apps available globally
- India's Aarogya Setu is the most popular, with 50 million downloads
- 53% use GPS, 15% use Bluetooth & 28% use both GPS and Bluetooth
- 24 apps (51%) contain Google and Facebook tracking
- 11 apps (23%) have no privacy policy
- 25 apps (53%) do not disclose how long they will store users' data for
- 28 apps (60%) have no publicly stated anonymity measures

Conclusiones

Riesgos

- Que estados de emergencia y de restricción de derechos se conviertan en estados permanentes;
- Que los datos colectados de los Estados se filtren o se vendan a empresas u otros Estados;
- Que los mapeos de contagio generen etiquetamientos de grupos sociales según niveles de riesgo (Semaforo), y por ende se generen nuevas formas de discriminación masiva.