javierderivera.net

Privacidad y nuevo orden mundial

javier de rivera

Artículo publicado en el número 02 de la Revista Ajoblanco (Noviembre 2017)
https://www.ajoblanco.org/revistas/n-2-invierno-2018
Referencia:
Rivera, Javier de (2017). Privacidad y nuevo orden mundial. *Revista Ajoblanco, 2* Noviembre 2017.

En el año 2037, Google E-Government ha conseguido acabar con los movimientos sociales, criminalizar el activismo y eliminar cualquier expresión de pensamiento subversivo.

Google E-Government es la inteligencia artificial que gestiona todos los sistemas sociales: la sanidad, la justicia, la educación, la economía, la seguridad, el tráfico, etc. … Todos los datos están centralizados y son analizados para optimizar la gestión de la sociedad de acuerdo con los principios de maximización del beneficio. La privacidad es una utopía

Así empieza el manifiesto del Hackmeeting 2017 que se celebró en octubre en el centro social La Ingobernable de Madrid. El texto recrea una distopía del futuro desde la que una Inteligencia Artificial envía un mensaje a "las hackers del pasado", a quienes llama a construir la resistencia contra la deriva totalitaria que se esconde detrás de los sistemas de la gestión centralizada de la información digital.

Registrar información es mucho más que describir la realidad, supone crearla y darle forma. Ser ciudadano es aparecer como tal en las bases de datos de un Estado y tener dinero consiste en un apunte contable a nuestro favor en las listas del sistema bancario. Quien produce y gestiona todos estos registros controla la sociedad. Quizás por eso Jacques Derrida dice que las instituciones, públicas y privadas, tienen "mal de archivo" (1997), un obsesión por acumular información y poder sobre el mundo.

En este contexto, la tecnología digital ha cambiado radicalmente el modo en que se producen y gestionan los archivos de la sociedad. Internet nos provee de enormes bases de datos interconectadas en las que se crean y acumulan datos a medida que el público interactúa con ellas. El volumen global de información aumenta, y con ella el potencial de poder. La aparente libertad de que cualquiera pueda producir información online se contrarresta con la acumulación de poder por parte de las corporaciones que crean y gestionan la infraestructura que hace posible la Red.

A través de las tecnologías digitales se están abriendo nuevos espacios de existencia, en los que convivimos y nos relacionamos, y poco a poco su influencia se extiende como una "malla de inteligibilidad" sobre el mundo. Por fuera, el espacio físico ha sido ya mapeado en su totalidad con satélites y cámaras sobre el terreno, y los sujetos que lo habitamos aparecemos como puntos en movimiento, registrados por nuestros dispositivos móviles. Por dentro, el espacio de nuestras emociones, pensamientos y relaciones también es mapeado con el registro de nuestras comunicaciones y del movimiento de nuestra atención cuando navegamos en Internet.

El ciberespacio que se ha convertido en una segunda naturaleza para nuestras conciencias que se mueven por él dibujando patrones estadísticos. En la "Posdata a la sociedad del control", Gilles Deleuze (1991) denunciaba la división interna de las personas, convertidas en seres *dividuales*, es decir, incompletos, fragmentados en múltiples realidades a medida que los datos que dan sentido a su vida se distribuyen en registros cruzados sobre los que se ha perdido toda capacidad de actuar. Así, al mismo tiempo que disfrutamos de estas múltiples dimensiones de existencia nos partimos, incapaces de reconocernos como seres unitarios. Mapear el territorio y dividir al adversario son

actividades previas a la conquista. Al individuo así fragmentado se le ofrece un mundo regulado en el que puede triunfar creando una *marca personal*, ese espectro de unidad desprovisto de cualquier esencialidad real.

La digitalización de la sociedad niega la importancia del contexto social y cultural en la generación de vínculos personales, todo lo que no puede ser procesado para mejorar la gobernabilidad de la sociedad es desechado como ruido comunicativo. Sin embargo, tal como se preguntaba Ronald Day (2001), ¿cómo podemos saber que no es precisamente el ruido lo que produce el sentido de la comunidad. El ruido de una sala llena de gente nos enmarca como miembros de una comunidad que se reúne en el espacio, obligados a aguantarse y convivir, a ser en conjunto.

El pragmatismo de gestión que acompaña a la fiebre de archivar y registrar de las instituciones digitales atenta directamente contra la existencia en común, desechada como ruido y confusión. Para ello, su *modus vivendi* tiene que ser también inculcado a los usuarios de nuevas tecnologías: “Elígelo todo”. “El mundo al alcance de tu mano”. La mentalidad del consumidor de experiencias se extiende sobre todas las áreas de la vida. Los otros se convierten en productos de información—perfiles, marcas—que pueden ser consumidos individualmente, y uno mismo es invitado a “venderse” en las redes sociales para triunfar y ser admirado.

La comunidad existencial ruidosa se sustituye por una comunidad digital etérea y funcional. Ya no nos molesta la vigilancia de la vecina chismosa, y cada vez nos importa menos que otros accedan a los detalles de nuestra vida. Las redes digitales han ayudado a superar el miedo a ser diferente y nos liberan de muchas opresiones cercanas. Pero esto es a costa de la sumisión total a estructuras de control casi invisibles, que pasamos por alto, considerándolas como recursos públicos o como espacios neutrales. Sin embargo, están lejos de ser gestores desinteresados de nuestra vida digital: son las instituciones más hambrientas de datos y de poder que ha habido en la historia.

El Big Data

El análisis de datos masivos permite explorar, controlar e influir en este nivel de realidad social, tanto en el nivel agregado de las tendencias generales como en el nivel pormenorizado de cada individuo concreto. La matriz de datos es extensa y profunda. Su uso más conocido es el de la segmentación social para identificar *targets* comerciales para productos o servicios. Registrar los gustos de la población implica darles forma, y también influir sobre ellos por medio del diseño de nuevos servicios. Algunos consumidores agradecen que las máquinas entiendan mejor sus preferencias sin entender la naturaleza performativa del sistema: los gustos son automáticamente reforzados y perdemos la posibilidad de cambiar; o peor, cambiamos según las inversiones de las marcas patrocinadoras, ya sean comerciales o políticas.

En el aspecto individual, la red de datos también permite aislar casos concretos para obtener su perfil social, político y psicológico. William Gibson (1984), el novelista visionario que imaginó el ciberespacio antes de que existiera, describía un futuro en el que todas las personas contaban con un perfil que les definía al detalle, anticipando incluso sus deseos y motivaciones. Antes de hacer tratos con un desconocido, las empresas se aseguraban de acceder a su fichero. Hoy día este mercado de perfiles psicológicos es cada vez más viable, y probablemente sea ya una realidad para los servicios de inteligencia que analizan a individuos “conflictivos”.

Los malos de la película

Según la lógica de la economía de mercado, las empresas son organizaciones dedicadas a la persecución legítima del lucro. En el capitalismo la codicia es una pasión socialmente aceptada que se canaliza hacia la producción y movilización de recursos. La gran mayoría de las empresas—grandes, medianas y pequeñas—responden a este patrón, adaptándose a las *leyes* del mercado. Sin embargo, a partir de cierto nivel de acumulación la naturaleza del juego cambia. La ambición de las corporaciones que controlan los flujos de capital e información no se limita a la obtención de beneficios económicos. Para ellas, el beneficio es solo un recurso más para establecerse como los centros de poder desde los que influir en la sociedad, en toda su profundidad y textura.

Además, las corporaciones tecnológicas de Silicon Valley han puesto de moda el modelo dual de acciones, un sistema que permite vender acciones de la empresa sin perder el control de la misma. Las acciones normales (tipo A) conviven con acciones tipo B, que gozan de 10 veces más poder de voto y están reservadas para los fundadores. De este modo, el 5,1% de la propiedad controla el 51% del poder de decisión. En la práctica, esto significa que el mercado digital está dominado por unos pocos individuos que se han convertido en los nuevos señores de la red. Comúnmente se les presenta como los genios que hacen posible el desarrollo tecnológico, pero lo cierto es que acumulan inimaginables cotas de poder.

Junto a estos señores de la red, los otros "malos de la película" de la privacidad son las agencias de inteligencia que, al tiempo que invierten en masivos sistemas de espionaje y almacenaje de información, se reservan el derecho de acceso a las bases de datos privadas. Las revelaciones de Edward Snowden en 2013 demostraron que los servicios digitales ofrecen puertas traseras para que la Agencia de Seguridad Nacional de EEUU pueda acceder a los datos de los usuarios: imágenes, correos electrónicos, conversaciones, etc. Y lo que parece menos peligroso, a los metadatos, es decir, al archivo de quien se comunica con quien. Cuando estos datos son masivamente analizados, permiten extraer la composición de la estructura social y el lugar que cada persona ocupa en ella.

Imaginemos por un momento que esta información se aplica contra organizaciones civiles y movimientos sociales: se pueden identificar a las personas centrales y conocer en detalles sus vulnerabilidades. La privacidad de las comunicaciones literalmente ha dejado de existir desde el momento en el que todas nuestras conversaciones e interacciones quedan archivadas en sistemas informáticos privativos. Frente al escándalo de las puertas traseras, las empresas tecnológicas prometieron públicamente protegerse y proteger a sus usuarios contra el espionaje gubernamental, pero lo cierto es que puede ser más peligroso que sean ellos quienes poseen esos datos. En realidad, tanto en un caso como en otro no existen controles democráticos sobre el uso que se hace de los datos privados, y técnicamente resulta casi imposible auditar el uso que una empresa hace de sus servidores.

Por otro lado, a estas revelación se le suman todo tipo de informes técnicos sobre la capacidad de registrar y enviar información de los dispositivos que usamos a diario. En 2013, un informático inglés descubrió que su televisor inteligente estaba enviando información de sus vídeos caseros a Korea del Sur[1], y posiblemente también audio y vídeo de la actividad en su sala de estar. Lejos de ser la excepción, esta es una práctica generalizada. Básicamente, todos los fabricantes de dispositivos y proveedores de servicios se reservan la posibilidad de acceder a nuestra información a través puertas traseras. Según las hackers, *por norma general somos hackeadas tres veces: primero por el fabricante, luego por el proveedor de servicios y después por el diseñador de aplicaciones privativas*.

1 https://www.cnet.com/news/fbi-taps-cell-phone-mic-as-eavesdropping-tool/

La mayoría de los dispositivos cuentan con la posibilidad de grabar y enviar el audio, de forma que, técnicamente, todos los teléfonos móviles son micrófonos que pueden ser activados a distancia. Esta característica de los teléfonos se hizo público en 2006, cuando un auto judicial desveló cómo el FBI la usó en una operación contra la mafia. Snowden también la otorga mucha importancia, tanta que en sus reuniones con periodistas los teléfonos eran sistemáticamente guardados en la nevera para evitar posibles escuchas.

Mal de archivo

La reacción más común a esta información es desestimar el riesgo que supone la vulneración masiva de la privacidad. Después de todo, ¿para qué iban a querer nuestros datos, nuestras fotos y nuestras conversaciones? El motivo declarado es para la mejora de los servicios publicitarios, como si la excusa del beneficio económico fuera suficiente. Sin embargo, la cantidad de recursos que se invierten en registrar y almacenar información aparentemente inútil es tan elevada que parece que la realidad no es tan sencilla.

Por ejemplo, el Data Center de la NSA en Utah es un complejo de 100.000 m^2, con cerca de 10.000 m^2 dedicados directamente a almacenamiento, con un coste aproximado de 4.000 millones (entre equipos y construcción) y un consumo de agua de 6.000 m^3 al día. Según las revelaciones de Snowden, este tipo de centros sirven para almacenar masivamente todo los datos que se interceptan pinchando directamente los cables de Internet.

Y bien, ¿deberíamos preocuparnos, sino hacemos nada malo? Si, porque más allá de la búsqueda de beneficio, estos agentes actúan movidos por el *mal de archivo*: una ambición de poder que lleva a la compulsión inevitable por registrar toda información potencialmente útil. Aunque no sea para nada en particular, registrar datos personales otorga un poder omnímodo sobre los demás. Después de todo, ¿quién sabe si eventualmente esa persona y sus datos podrán ser útiles para lograr algún objetivo de la organización? Es un recurso a su disposición.

Otra forma de interpretar la utilidad de estas inversiones es el efecto panóptico: la idea estar siendo vigilados hace que nos autocensuremos. Si pensamos que todos nuestros datos se almacenen y de que potencialmente pueden escuchar todas nuestras conversaciones privadas—porque siempre hay un teléfono cerca—, consciente o inconscientemente empezaremos a limitarnos, especialmente si somos críticos con cómo está organizado el mundo… De este modo, el efecto del poder asociado a la vigilancia se hace sentir incluso sin necesidad de que los datos sean analizados y usados.

Así lo demostró un investigador del Oxford Internet Institute[2] en 2016. Jon Penney analizó el uso de Wikipedia antes y después de las revelaciones de 2013 y descubrió que las visitas a páginas conflictivas, relacionadas con el terrorismo como “Al-qaeda”, “Coche-bomba” o “Taliban”, habían descendido un 20%. Además, en términos generales, el estudio muestra un cambio de tendencia en el comportamiento online de los usuarios. Este es un efecto de la vigilancia que surge como un efecto no intencionado de la denuncia social, que se instala creando la vaga sensación de que existe un poder desconocido capaz de espiar cada rincón de nuestra conciencia.

2 https://www.washingtonpost.com/news/wonk/wp/2016/04/27/new-study-snowdens-disclosures-about-nsa-spying-had-a-scary-effect-on-free-speech/

La toma de conciencia:

Entre la paranoia paralizante y la sumisión despreocupada a los mecanismos de vigilancia debe existir un modo de recuperar la cordura y la autonomía sobre nuestras vidas.

Psicológicamente, la paranoia se asocia con una especie de narcisismo que nos hace pensar que todo gira a nuestro al rededor, que hablan de nosotros, que somos una pieza importante en el puzzle de la vida. Sin embargo, en la hipertrofia de vigilancia digital en la que vivimos no parece descabellado pensar que alguien puede estar observándonos, por el motivo que sea. Para protegernos de la paranoia, el miedo y la ansiedad que esto produce, el impulso es evolucionar hacia la hipernormalidad: dejar de visitar páginas conflictivas, disminuir nuestra inquietud política y, sobre todo, renunciar a cualquier expectativa de realizar algún cambio social significativo, no vaya a ser que atraigamos la atención sobre nosotros. Ahí, ya hemos perdido.

Según Snowden, “no preocuparse por la privacidad porque no tienes nada que ocultar es como no preocuparse por la libertad de expresión porque no tienes nada que decir”. Pero la situación es incluso peor: pensar que no tienes nada que ocultar a los poderosos—los señores de Silicon Valley y los servicios de inteligencia extranjeros—es ya una declaración de rendición incondicional ante ellos y sus intereses, cualesquiera que estos sean (porque los desconocemos). La privacidad de las comunicaciones es un bien común que a todas nos interesa proteger, no porque algunas personas sean relevantes, sino porque cada persona es relevante a su manera.

La hipernormalidad implica la sumisión total de la conciencia a un poder abstracto. Esta actitud llega al extremo de agradecer las facilidades comerciales que nos indican qué consumir, qué pensar y qué hacer. Culturalmente se está desarrollando una especie de “indefensión aprendida” con respecto al poder tecnológico que nos lleva a aceptar su dominio con naturalidad. La pasividad mental de las actitudes adaptativas nos aleja cada vez más del “atrévete a pensar” de la filosofía latina. Pensar por uno mismo requiere estar dispuesto a romper con las reglas y convicciones sociales para llegar a conclusiones que nos rompen los esquemas. Si ya es difícil sin que nos observen, ¿cómo atreverse a hacerlo cuando sentimos que toda acción comunicativa (hablar, leer, mirar...) queda registrada?

En física cuántica se dice que el hecho de observar modifica lo observado, como si la conciencia tuviera algún efecto sobre el comportamiento de las partículas. En la sociedad este efecto es evidente e incuestionable: ser mirados cambia radicalmente el sentido de nuestras acciones y pensamientos. Esto tiene una dimensión política, fácil de identificar como autocensura, y una dimensión cultural, más sutil e inconsciente, por la que el pensamiento colectivo se orienta hacia cuestiones inocuas y superficiales.

¡Acción!

Lo primero que hay que contrarrestar es el miedo a pensar, hablar y actuar, que afecta especialmente a las personas con más sentido crítico. Es necesario inspirar el valor de seguir adelante. La amenaza es real, pues se ha demostrado la existencia de múltiples programas para la identificación, seguimiento y represión de activistas—como Occupy o el 15M—; pero ese es el coste que hay que asumir para construir la primera barrera de resistencia cognitiva. Sin ella, todos los pasos subsiguientes son imposibles. Además, sobre el peligro real, la amenaza del abuso de poder se alza como un espectro cuya verdadera naturaleza y extensión desconocemos: no le demos la fuerza de

proyectar nuestros miedos particulares sobre él. Aunque, *es difícil no temer lo que otros temen, porque desconocemos el poder del mal.*

Lo segundo es concienciar socialmente de la importancia de la privacidad a través de una alfabetización digital crítica. La gente en general tiene que ser capaz de entender cómo funciona el mundo digital, y el modo en que las corporaciones tecnológicas están acumulando un poder omnímodo sobre la sociedad, a través de la gestión de datos sobre nosotros. Hay que atacar la idea de que los servicios comerciales son bienes públicos, y desvelar la estrategia de dominación que se oculta detrás de sus diseño. El desarrollo tecnológico es algo demasiado importante como para dejarlo en manos de instituciones ávidas de poder, enfermas de archivo.

Lo tercero es construir y apoyar las iniciativas de autonomía tecnológica. Aunque la seguridad total no exista, de lo que se trata es de aumentar el coste de registrarlo todo para abrir agujeros en la malla que mapea nuestras acciones y comunicaciones, para dotar a nuestro pensamiento—individual y colectivo—de más espacios de intimidad. Una vez que hemos logrado poner socialmente en valor la importancia de la privacidad, hay que desarrollar las alternativas. Esto requiere mejorar la pedagogía tecnológica, así como destinar esfuerzos y recursos a mantener sistemas que rompan con la lógica comercial de la venta de datos, y la sustituyan por la lógica de funcionamiento de las instituciones del común.

Referencias:

Day, R. E. (2001). *The Modern Invention of Information: Discourse, History, and Power.* Southern Illinois University, Chigcago.

Deleuze, G. (1991) Posdata sobre las sociedades de control. En Christian Ferrer (Comp.) *El lenguaje literario*, Ed. Nordan, Montevideo.

Derrida, J. (1997) *Mal de Archivo*. *Una impresión freudiana.* ed. Trotta, Madrid.

Gibson, W. (1984). Neuromancer. Ed. Ace, New York.

Penney, Jon, Chilling Effects: Online Surveillance and Wikipedia Use (2016). Berkeley Technology Law Journal, Vol. 31, No. 1, p. 117, 2016. Available at SSRN: https://ssrn.com/abstract=2769645