Módulo 3: Vigilancia corporativa

3.1. La recolección masiva de datos por parte de las corporaciones y la vigilancia corporativa

En 2012, Andy Morar, un ciudadano del estado de Georgia (EE.UU), buscó online acerca del auto que pensaba comprar, un BMW deportivo. Dejó su nombre y datos de contacto en el sitio de un vendedor y, apenas lo hubo hecho, todo fue a parar a Dataium, una empresa de Nashville que se dedica a procesar información personal. Dataium podía crear un perfil de todos los sitios que Morar había visitado sin haber dejado sus datos, además de un montón de otra información de utilidad comercial sobre otros aspectos de su perfil como consumidor. Así que cuando fue a comprar, el vendedor ya lo sabía todo sobre él.

Según informaba el sitio de Dataium cuando se conoció este caso, la empresa observaba rutinariamente a más de 20 millones de posibles compradores de autos, que visitaban en conjunto diez mil websites sobre coches por mes. Luego compilaba, indexaba y resumía esa información para sus clientes. Si entre sitio y sitio a uno le daba por ir a ver uno sobre perros labradores, eso también era útil para que el vendedor pudiera intentar establecer una comercialmente útil empatía hablando primero sobre mascotas, por ejemplo.

Ocurre que, con cada click, búsqueda y sesión de visita o de compras en un sitio damos mucha información sobre nuestros hábitos, intereses y hasta comportamientos futuros. También contribuimos a que las empresas midan la eficacia de sus promociones y diseños web. No importa si solo pusiste tu dirección de correo electrónico en el sitio de un vendedor y no tu nombre, igual pueden rastrearte sin que lo sepas y conocer muchos datos que te sorprenderían. Nunca sabrás si usaron esta información ni cómo lo hicieron.

Casos como el de Morar, aunque no extraordinariamente dañinos, ilustran el conflicto inherente a Internet entre privacidad y negocios. Porque las empresas ganan ventajas competitivas cuando tienen la mayor cantidad posible de información sobre posibles consumidores. Por eso existen otras empresas como la mencionada Dataium, así como Experian o Axciom, dedicadas a recolectarla, sistematizarla y analizarla para vender esos *dossiers* a sus clientes. A esos mayoristas se los conoce como *data brokers*. Ellos conocen lo que compras y lo que quieres comprar, tu etnia, tu estado financiero, tu salud, tu actividad en redes sociales online y tus hábitos de navegación.

Otras empresas ofrecen rankings de consumidores. Es decir, deciden cuáles son valiosos (y a ellos les ofrecen mejores descuentos, ofertas, tarjetas de crédito y otros “regalos”) y cuáles son una pérdida de tiempo.

También hay *data brokers*, por así decirlo, “especializados”. Se dedican a armar archivos de personas que han cometido algún crimen, o de divorcios, afiliaciones políticas o religiosas en

particular, consumo de entretenimiento adulto o problemas con el juego. Otros juntan información sobre víctimas de abuso, personas con enfermedades de transmisión sexual, demencia, SIDA o Alzheimer o depresión.

Finalmente están las redes publicitarias (*ad networks*), que hacen un perfilado de usuarios y venden a sus clientes acceso online a ellos para mostrarles anuncios segmentados.

Todas estas empresas entienden que el rastreo online de consumidores es algo que los beneficia, porque los pone en contacto con productos que realmente les interesan y les permiten tener una experiencia más personalizada en Internet. También suelen resaltar que lo que hacen no es perjudicial porque supuestamente la información recolectada es anónima.

Por otra parte, uno podría preguntarse si alguien tiene derecho a reclamar privacidad cuando es posible que haya brindado cada pieza de información voluntariamente.

El problema es que, a diferencia de lo que ocurre con la información que está en papel, la que está online típicamente termina en la computadora de otra persona o empresa. Un mensaje de correo electrónico necesariamente pasa por nuestro proveedor de Internet, por ejemplo. Una búsqueda en la web la hacemos desde un navegador y con un buscador en particular (se podría usar TOR y DuckDuckGo, por ejemplo, para dejar menos huellas, pero no es la práctica usual de los internautas). Si pensamos en esto, deja de estar muy claro qué es privado y qué es público.

3.1.1. ¿Cómo llegamos a esta situación?

Mucho antes de que existiera Internet, las tiendas, bancos y otras empresas ya recolectaban información sobre los clientes, con fines de marketing o para analizar riesgo crediticio, por ejemplo. Para solicitar una tarjeta de crédito se requiere brindar nombre, dirección, datos laborales y de ingresos, información bancaria y otras informaciones bastante personales. Cuando no había computadoras, este tipo de datos se guardaban en papeles que formaban parte del expediente de cliente. Aun así, surgieron empresas de verificación de créditos que intentaban centralizar este tipo de datos, incluso buscando en anuncios personales de los diarios para registrar, por ejemplo, casamientos, divorcios, arrestos, promociones y fallecimientos. Simplemente recortaban las noticias de los diarios y las adjuntaban al archivo en papel de cada cliente.

Cuando llegaron las computadoras, se crearon los primeros centros de procesamiento de datos que recolectaban, almacenaban y distribuían información personal de interés para fines crediticios y vendían esos informes a bancos y entidades financieras. Estamos hablando de tan atrás en el tiempo como fines de los ’60 y principios de los ’70. Por cierto, esta industria tendió a la concentración, y las empresas de análisis crediticio más pequeñas fueron vendidas a otras mayores.

La situación comenzó a preocupar a algunos sectores, concretamente en Estados Unidos a fines de los ’60. Así, una comisión del Senado de ese país comenzó a investigar el negocio del crédito. En la

investigación surgió que se estaba recolectando información tan personal como asuntos extramatrimoniales, excesos con la bebida y preferencias sexuales. Muchos testigos declararon que se les había denegado un crédito debido a información incorrecta o prejuiciosa. También se demostró que los archivos generados estaban al alcance de cualquiera que quisiera comprarlos, como revendedores, empleadores potenciales e investigadores privados. Incluso agencias gubernamentales como el FBI, el Departamento de Estado y la agencia de recaudación de impuestos podía accederlos. La única persona que no tenía idea de lo que había en su archivo era justamente el sujeto de los datos.

Debido a esta investigación, el Congreso de Estados Unidos aprobó en 1970 la *Fair Credit Reporting Act*, que promovía la exactitud, corrección y privacidad de la información sobre consumidores en manos de las empresas crediticias. Se les restringió a estas últimas compartirla con cualquiera y, además, los sujetos de los datos adquirieron derecho a revisar sus archivos y exigir enmiendas sobre los datos erróneos. También se les otorgó a los consumidores el derecho a recibir una lista de todos los receptores de lo recopilado por las empresas de información crediticia.

Pero, con la llegada de la Web en 1990, comenzó a hacerse complicado el cumplimiento efectivo de esta ley. Por no mencionar que en la mayoría de los países con acceso a Internet no existía siquiera un intento de límite legal como la *Fair Credit Reporting Act*.

En efecto, con la explosión del comercio electrónico que sobrevino con la Web a mediados de los ’90, la Internet se convirtió en un factor muy fuerte en la experiencia de compras. La usamos hasta para encargar comida a domicilio, además de para buscar productos, comparar precios, o estudiar qué opinaron otros consumidores sobre algo que nos interesa. El problema es que, al hacerlo, podemos tener una falsa sensación de anonimato, podemos creer que nadie se entera de cómo vamos de sitio comercial en sitio comercial, cuánto tiempo nos detenemos en cada lado, qué productos comparamos o en cuáles nos fijamos más. Y, lo que es más riesgoso, podemos creer que nadie registra cuando investigamos online sobre una condición médica o participamos en discusiones políticas.

También podemos pensar que, en todo caso, solo el sitio que visitamos registra nuestra actividad. Sin embargo, lo que hacemos puede ser compartido con otras empresas sin que lo sepamos. Y como los datos obtenidos cada vez se suman y se cruzan con los de otras fuentes, es posible deducir información muy detallada, como cuestiones financieras, creencias religiosas, afiliación política, raza, problemas de salud y hasta preferencias sexuales. Ninguno de estos datos tan personales es superfluo desde el punto de vista comercial porque, mediante el uso de ciertas herramientas estadísticas, es posible por ejemplo determinar si las personas de ascendencia asiática que sufren de alergia al polen tienen mayor probabilidad de adquirir tablets de 10 pulgadas. Variables aparentemente inconexas pueden dar lugar a hallazgos muy útiles para dirigir publicidad exactamente al público con mayor probabilidad de concretar una compra. Claro está, con los mismos métodos puede concluirse que quienes compran mochilas y ollas a presión tienen mayor probabilidad de estar tramando un plan terrorista, como lo muestra este tristemente célebre ejemplo.

La verdad es que cada cosa que hacemos con computadoras, teléfonos inteligentes y tablets, entre

otros equipos, almacena bases de datos de muchas compañías. Así vamos generando una huella imborrable de datos que puede ser usada de modos diversos por empleadores potenciales, departamentos de marketing y entidades gubernamentales. Y no se necesita realmente ser un *data broker* para comprobarlo. En 2009, por ejemplo, un profesor de leyes de la universidad Fordham ganó cierta notoriedad cuando asignó a su clase crear un archivo sobre el juez de la corte suprema de Estados Unidos Antonin Scaglia usando solo información que pudieran encontrar online. El resultado fueron quince páginas de cosas que incluían la dirección postal de Su Señoría, su número de teléfono personal, la dirección electrónica de su esposa y los programas de televisión que prefería.

Por otra parte, todas las empresas de Internet podrían ser blanco de ataques informáticos, y los datos personales recolectados pasar así a disposición de delincuentes de todo tipo. Por ejemplo, en 2013 un ataque informático a las tiendas Target comprometió nombres, números de tarjeta de crédito, direcciones de correo electrónico, números de teléfono y dirección postal de al menos 70 millones de personas en Estados Unidos. Aquí podrás ver muchos otros ejemplos.

3.1.2. ¿Cómo lo hacen?

- Una de las formas más sencillas de rastrear usuarios es mediante su dirección IP. La dirección IP es un número asignado a cada suscriptor por el proveedor de Internet en cada sesión de trabajo.
- Para obtener aún más información, la mayoría de los sitios web utilizan c*ookies*. Una *cookie* es un pequeño archivo de texto que los servidores web almacenan en el disco rígido del usuario. Como son solo texto, no pueden leer información guardada en el equipo ni infectarlo con virus ni ejecutar ningún software. Sí permiten a un sitio (y solo ese sitio) rastrear los movimientos del usuario dentro suyo y cualquier información voluntariamente provista allí. Cuando esa *cookie* queda en el rígido, el sitio recuerda las preferencias del usuario y va creándose un perfil que puede usarse para interacciones de marketing, para mejorar la eficacia del sitio o detectar áreas de mejora comercial. Sin embargo, es posible configurar el navegador para limitar las *cookies* y también borrarlas una vez almacenadas en el disco.
- También está creciendo el uso de otra herramienta de rastreo, los *web beacons*. Estos son pequeños gráficos embebidos en una página web que recolectan información como direcciones IP, cantidad de veces que el gráfico fue visto, y datos acerca de las *cookies* relacionadas almacenadas en el disco del usuario. Efectivamente, los *web beacons* suelen usarse en combinación con las *cookies*, pero ellos son capaces de rastrear al usuario a medida que va de sitio en sitio. Además, a diferencia de las *cookies*, pocos los notan y, aunque los encontraran, no son borrables del mismo modo ni uno puede elegir si aceptarlos o no. A lo sumo, si uno configura el navegador para declinar cookies, un *web beacon* no

podrá rastrear esa información en particular.

- Otro método usual son las *cookies* de terceros para exhibir avisos publicitarios. Muchos sitios, en lugar de buscar sus propios anunciantes para sostener sus operaciones, lo que hacen es contratar redes de colocación de anuncios. Estos terceros son quienes reclutan anunciantes y colocan sus avisos en el sitio contratante. Muchos de los anuncios que uno ve al visitar un sitio no están albergados en éste, sino que vienen de una empresa desconocida para el visitante. Por supuesto, esos terceros utilizan *cookies* para monitorear el comportamiento de los usuarios, por ejemplo cuántas veces vimos determinado anuncio y si hicimos click sobre él. Cuando aceptamos una de ellas, esa compañía accede a nuestra información y va construyendo un perfil que incluye dirección IP, ubicación, preferencias de compra y métodos de pago disponibles, entre otros datos. Luego ese perfil, a su vez, se usa para personalizar los anuncios que cada uno ve al navegar online. Esos anuncios pueden ser exhibidos a cada persona en un orden particular, según su perfil, con el fin de optimizar la eficacia comercial. Lo importante es que, cuando visitamos un sitio, no solamente podemos recibir *cookies* suyas, sino de esos terceros desconocidos que pudo haber contratado para optimizar la segmentación publicitaria.
- Las *cookies* tienen dos problemas para el mercado publicitario. Uno, que cada vez más usuarios configuran sus navegadores para rechazarlas, o bien las eliminan. Otro, que los teléfonos móviles son cada vez más utilizados para usar Internet, pero no usan *cookies*. Entonces, algunos anunciantes online desarrollaron métodos de rastreo más difíciles de deshabilitar. De hecho, para evitarlos haría falta descartar el equipo utilizado, dejar de usar por completo una red social o borrar un archivo completo de mensajes de correo electrónico. Estoy hablando de la autenticación. Sitios como Facebook, Apple iCloud, Google Gmail y el navegador Chrome requieren loguearse, así que las compañías en cuestión pueden saber fácilmente quiénes son los usuarios y qué están haciendo. Esto es muy importante para ellas, ya que hoy todos nos manejamos con múltiples equipos y quieren seguirnos en todos ellos. De hecho, cada vez menos sitios de la Web permiten entrar sin registrarse primero con un usuario y contraseña que se obtienen luego de dejar muchos datos personales. Es posible no hacerlo, claro, o poner datos falsos, pero ciertamente las plataformas no facilitan la elusión de este “pago” que debe hacer el internauta a cambio de unos deliciosos servicios “gratuitos”. Además, hay sitios que directamente impiden poner nombres no reales. Entre los riesgos, mira por ejemplo cómo la política de nombre real de Facebook puso en peligro la vida de una mujer.
- En el caso de los sitios de medios sociales online, como Facebook, cada vez que uno se loguea la empresa chequea nombre, dirección electrónica, amigos e historial de actividad pasada. Además, inserta *cookies* en el disco duro. Y cada vez que visitamos un sitio de terceros que tenga el botón “me gusta” o el *plugin* de Facebook, éste actúa junto con la *cookie* para decirle a Facebook la fecha, hora y dirección web de ese otro sitio visitado. También registra características distintivas de la computadora y el navegador utilizados, como la dirección IP, el sistema operativo y la versión. Con tanta información, los sitios de medios sociales online pueden crear perfiles detallados de un usuario, incluyendo ideas

políticas, creencias religiosas, orientación sexual y problemas de salud. Cualquier cosa de estos temas que hayas comentado, aun en mensajes privados con otros usuarios, también puede figurar en tu perfil.

- Otro método de rastreo se basa en examinar las características de una computadora o equipo que cuando se visita un sitio. Por ejemplo, qué *plugins* están instalados, qué software, el tamaño de la pantalla, la zona horaria, las fuentes utilizadas, etc. En conjunto, todo esto conforma una especie de "huella digital" que singulariza unívocamente al usuario. Por cierto, cada cambio que el usuario hace en la configuración de su equipo no hace más que facilitar su identificación.

3.1.3. ¿Cuál es el problema?

Las empresas alegan que la recolección de datos de navegación con fines publicitarios es el único modo que tienen de ofrecer servicios atractivos en forma gratuita y que, si uno quiere algo, debe dar algo. Sin embargo, para esta línea argumental hay un claro contraejemplo: el servicio de *streaming* de películas y series Netflix utiliza profusamente técnicas de Big Data para analizar cada cosa que sus clientes hacen con el servicio y, sin embargo, no es gratuito. Como dice en esta nota Elena Neira, profesora de marketing cinematográfico y distribución audiovisual de la UOC:

Netflix monitoriza el número de reproducciones (en marcha, adelante, atrás, pausa, abandono), las valoraciones de cada película, el soporte con que se visiona, la ubicación geográfica, el día y la hora del visionado, la huella digital que vamos dejando con nuestros comentarios» e incluso «los retrasos que hay en la visualización de un producto debido al buffering o al bitrate (parámetro que indica el flujo de datos con el que se puede reproducir un archivo de vídeo en un ordenador y que puede afectar a la calidad de la imagen.

Así que, aunque es cierto que "si un producto es gratis es porque el producto eres tú", también puedes ser el producto cuando éste NO es gratis. Y, aunque estés dando voluntariamente tus datos y te dejes rastrear por la empresa online de tu elección, debés saber que otras que no conocés pueden acceder a lo que generas, ya sea por acuerdos comerciales o simplemente por accesos indebidos. Entre quienes accedan a tus movimientos pueden estar empleadores, aseguradoras, bancos y hasta agencias de inteligencia. Las leyes de protección de datos que puedan regir en tu país no te protegerán mucho, porque la información lo más probable es que trascienda tus fronteras. Nunca nos enteraremos cuánto se han pasado de la raya, porque gran parte de los métodos de rastreo o, incluso, de manipulación de los sitios web sobre sus usuarios son en gran medida invisibles.

Tampoco es fácil que nos demos cuenta si estamos siendo discriminados. En efecto, cuando algunos sitios despliegan versiones personalizadas para cada usuario según su perfil le muestran un conjunto diferente de productos, y hasta el mismo producto pero a diferente precio. Y se puede perfectamente pensar que es una forma de discriminación que nos cobren más caro algo solo por nuestros hábitos de compra o nuestras singularidades personales, de acuerdo a lo que considere un algoritmo.

Además, la información personal, como hemos visto, puede caer en malas manos. Aún peor, podemos ser víctimas de suplantaciones de identidad en transacciones, o de acosadores y depredadores diversos, incluso en los sitios más respetables. Por ejemplo, en 2010 Google despidió a un ingeniero porque se dedicaba a utilizar las bases de datos de correos, chats y otros datos de usuarios para localizar y acechar adolescentes. Lo cual destierra el habitual argumento de las empresas de que los datos recolectados son anónimos y que no los ceden a cualquiera. Aunque esa sea su política, entre sus mismos empleados puede haber quienes los usen en provecho propio. Pero incluso si todos los empleados con acceso a tus datos son gente honesta y seria y se hayan tomado medidas excelentes para proteger la información contra intrusiones por parte de *crackers*, siempre existirán los errores humanos o de sistemas que generan fugas de datos no intencionales, errores lógicos o transferencias hacia sitios inseguros.

Por cierto, lo de los datos anónimos debemos entenderlo de acuerdo a una reformulación de su definición. Hacia el 2000 se decía que una navegación era anónima si no había acceso a información personalmente identificable. Hoy muchas compañías sostienen que el rastreo rutinario es anónimo aunque tengan el nombre real y la dirección de correo del usuario, porque luego separan, protegen o eliminan la identidad de la persona de su historial de navegación. Pero algunos expertos sostienen que los procedimientos técnicos empleados para hacer esta separación e igual mostrar publicidad personalizada no permiten una completa anonimización de los datos. También se ha reportado que ciertos sitios que supuestamente anonimizan los datos igual venden nombres y direcciones a terceros.

3.1.4. Políticas de privacidad

La mayoría de los sitios tienen una sección con sus políticas de privacidad, donde te explican qué datos recolectan, si usan cookies o con quién pueden compartir la información. Por ejemplo, la de Yahoo dice que la empresa puede compartir tu información personal con socios en los que confíe, con los cuales mantiene acuerdos de confidencialidad (el equivalente online a “esto no lo sabe nadie, solo nuestros amigos y, por supuesto, sus amigos, los amigos de sus amigos, etc.”).

Simon Smelt, un economista que dirige la empresa de encuestas SimplyQuick.com, comparó las políticas de privacidad de varios sitios entre junio y noviembre de 2013. En la encuesta de junio encontró que la mayoría de los sitios decía que no iba a compartir información personal con terceros. En la de noviembre, muchos habían ya cambiado de opinión y ya se reservaban el derecho de vender los datos a otras empresas. Quien no aceptara eso, era libre de darse de baja. Solo 30 por ciento de los 90 sitios investigados garantizaba que no vendería la información a otros.

La verdad es que la mayor parte de esas políticas de privacidad son más una necesidad legal y de relaciones públicas que una verdadera protección. La mayor parte de ellas son difíciles de entender para el usuario promedio, están en letra muy chica, en algún enlace bien oculto en la parte más imperceptible de la página e, incluso, pueden contener información contradictoria. Por ejemplo,

pueden decir que no comparten datos con terceros y, al mismo tiempo, resulta que permiten a terceros poner en el sitio *web beacons* para rastrear a los usuarios. Además, hay sitios –Facebook el más paradigmático– que cambian constantemente sus políticas de privacidad, de modo que es casi imposible estar al tanto y hacer las opciones que la plataforma permita. También son una excusa de "culpar a la víctima" porque, si aceptaste todo lo que la empresa hace y, además, ella te explicó en un texto a tal efecto cómo usaría tus datos, se lava las manos si desde la CIA hasta el último ratero de la calle luego se enteran de los pormenores de tu vida.

Pero no es tu culpa. Si lo fuera, habría que culparte de no emplear 250 horas al año (unos 30 días hábiles) en leer y entender las políticas de privacidad de los sitios más populares que seguramente visitas regularmente.

De todos modos, te recomendamos tener algunas precauciones, como las que se sugieren aquí y aquí. Pero aun así no te confíes porque, hagas lo que hagas, lo mejor al usar Internet es asumir que todo lo que uno hace y dice es público.

3.1.5. El efecto de la ley

Muchos países tienen leyes de protección de datos, algunas muy buenas. El problema es que lo que habría que proteger es a la persona, no a los datos. Porque casi todas las legislaciones justamente enfatizan la protección según el carácter del dato, por ejemplo, creencias religiosas. Sin embargo, si se cruza por ejemplo la lista de lo que compró para leer alguien en Amazon con su lista del supermercado, no sería raro que pudiera conjeturar con bastante exactitud ciertas creencias religiosas en particular, sin necesidad de que nadie lo haya preguntado expresamente. Es lo que se llama "triangulación violatoria de la privacidad". Implica que uno puede deducir gran parte de los datos médicos, financieros, impositivos u otros de carácter protegido a partir de aquellos de apariencia inocente que no gozan de ningún privilegio legal. Por ejemplo, si alguien compra una peluca y además falta mucho al trabajo, probablemente tenga cierta condición médica.

Un informático llamado Tom Owad escribió una simple pieza de software que le permitía descargar las listas de deseos que los clientes de Amazon arman online sobre los productos que les gustaría tener. Descargó unas 250 mil y luego usó el buscador de personas de Yahoo para identificar las direcciones físicas y números telefónicos de quienes las habían confeccionado. A continuación, publicó un mapa detallado que mostraba las ubicaciones geográficas de dichas personas, clasificándolas por libros o temáticas. Como luego explicó Owad: "Solía hacer falta una orden judicial para monitorear una persona o grupo de personas. Hoy es crecientemente fácil monitorear ideas y luego rastrearlas hacia personas". Muchos de los que ponen datos muy simples e insignificantes en sus perfiles de Facebook no se dan cuenta de que eso puede permitir adivinar rasgos concretos de su personalidad con un 90 por ciento de exactitud, más que si les hicieran un test psicológico.

Se puede pensar que las empresas privadas usan toda la información que recolectan, más la que deducen mediante técnicas de Big Data, solo con fines comerciales no particularmente perjudiciales, mientras que el gobierno cuando hace lo mismo es para tratar de encarcelarnos, controlarnos, cobrarnos impuestos o censurarnos. Sin embargo, la violación de la privacidad por parte de compañías tiene el mismo efecto atemorizador y causa la misma discriminación del disenso que la cometida por los estados. Si un banco le deniega un crédito a alguien porque parezca tener cáncer, o los posibles empleadores no lo contratan debido a su orientación sexual o ideas políticas, las consecuencias de esa violación de la privacidad son tan dañinas como cuando es el estado quien viola derechos humanos. Además, como ya hemos mencionado, la información que las corporaciones amasan también está a disposición de los estados. De hecho, los estados podrían estar entre sus clientes y, cuando las empresas acumulan datos, quizá lo hagan teniendo en mente que están construyendo un activo útil a la hora de negociar lo que en algún momento necesiten negociar con los gobiernos.

3.2. La vigilancia como modelo de negocio

En este apartado sostendremos que la vigilancia es una cualidad inherente al modo de generar ganancias propio del capitalismo informacional contemporáneo.

Recordemos que en el capitalismo no hay una coordinación a priori entre oferta y demanda. En el mercado es donde se decide si determinada producción es útil o no. Por eso es que se necesita el marketing: para minimizar esa incertidumbre estructural en la competencia entre distintas inversiones posibles de capital.

En este contexto, la informatización facilita enlazar y modelar todos los pasos necesarios para producir mercaderías. Por ejemplo, la información sobre los compradores potenciales y previos influye en cómo un bien se produce o se distribuye. Esta es la base del marketing de datos, un factor esencial del capitalismo informacional.

Shoshana Zuboff se refiere a este fenómeno como capitalismo de la vigilancia. Y cita cuatro de sus características en base a declaraciones del economista jefe de Google, Hal Varian. Éstas son:

- El impulso de extraer y analizar más y más datos
- El desarrollo de nuevas formas contractuales que utilizan monitoreo informático y automatización
- El deseo de personalizar los servicios ofrecidos a los usuarios de plataformas digitales
- El uso de la infraestructura tecnológica para llevar a cabo experimentos con los usuarios y consumidores.

Detallemos de qué se trata cada una.

- ## Extracción y análisis

Es lo que suele hoy denominarse ampliamente como Big Data. Y en este fenómeno interesa la multiplicidad de fuentes que hay para dichos datos. Cada intercambio, cada transacción, puede alimentar para siempre esa enorme acumulación. Y el análisis de los datos permite obtener información que puede ser más sensible que la de los datos originales.

A esto debemos sumar lo que se llama “Internet de las Cosas”. En efecto, hoy tienen conectividad los autos, las cortadoras de césped, las heladeras, los relojes, las lavadoras de ropa y más objetos. Cada uno de ellos nutre de más datos el mundo del capitalismo de la vigilancia. La ubicuidad del monitoreo a menudo está oculta, o bien “oculta a plena vista”.

Por otra parte, Zuboff señala tres características entre las compañías que extraen datos y los usuarios de sus servicios:

1. **Relación asimétrica**: los datos muchas veces se obtienen y procesan en ausencia de un consentimiento o diálogo formal. En general, la política es extraer primero, preguntar después. Incluso cuando hay consentimiento, este no es precisamente informado. En general, solo se conoce la magnitud del abuso luego de algún escándalo, como el asunto de los datos personales de redes wi-fi que Google Street View recolectaba sin conocimiento de los dueños de dichas redes.
2. **Indiferencia formal**: esto se refiere a la actitud de sitios como Google frente al contenido de los datos que extrae. Recolecta todo y luego ve para qué le sirve.
3. **Independencia funcional**: las empresas de Internet en general no extraen dinero de los usuarios. Más bien, usan la información extraída como una mercancía que venden a los anunciantes. En esto las corporaciones informacionales se distinguen de las del siglo XX. Por ejemplo, las automotrices del siglo XX se apoyaban en grandes y estables redes de empleados y consumidores (que, a veces, coincidían en las mismas personas). Así que les interesaba establecer carreras durables para sus empleados y relaciones a largo plazo con los clientes. Pero no parece ser éste el modelo de empresas como Google. No extraen el dinero directamente del usuario y sus procesos centrales tampoco requieren personal que haga expresamente tareas, hay mucho de automático. Por eso Zuboff señala que estas empresas, basadas en el capitalismo de la vigilancia, son mucho más rentables que lo que las automotrices fueron nunca y, además, emplean mucha menos gente.

- ## Nuevas formas contractuales

Las tecnologías que acompañan el capitalismo de la vigilancia permiten monitorear y hacer cumplir ciertas relaciones contractuales. Por ejemplo, si alguien deja de pagar la cuota mensual por la compra de su auto, los acreedores podrían instruir a un sistema de monitoreo vehicular inserto en el rodado para que no le permita arrancar y para que transmita su ubicación y poderlo ir a incautar. Las compañías de seguros podrían usar similares sistemas para comprobar que los conductores estén manejando con prudencia y subirles o bajarles concordantemente el precio que pagan. Por qué no,

los servicios de salud podrían monitorear el reloj inteligente de alguien para verificar si camina al menos 10 mil pasos al día.

Zuboff observa que si este tipo de monitoreo contractual se convierte en la norma habrá una reestructuración radical del actual orden político y legal. De hecho, sostiene, estaremos ante una organización social "a-contractual". Porque, clásicamente, un contrato es una institución social basada en la confianza, la solidaridad y la ley. En principio, como no podemos monitorear todo el tiempo lo que hacen los otros, en la práctica confiamos en que cumplirán sus promesas con respecto a los bienes y servicios que prestan. Si no lo hacen, podemos recurrir a la ley. Pero este recurso a la ley implica reconocer implícitamente que no hay control perfecto. En el mundo que imagina Zuboff en base a las reflexiones de Varian, en cambio, ya no hay necesidad de solidaridad social ni de confianza, porque existe monitoreo contractual perpetuo y perfecto control.

En esta distopía, el Estado tampoco sería un mediador central ni árbitro de las promesas de cumplimiento de los contratos civiles. De hecho, ya no habría más necesidad de prometer: o bien uno cumple con lo impuesto, o bien automáticamente deja de tener acceso al producto o servicio en cuestión. El compromiso de cumplir un contrato sería irrelevante. Se pasa de un mundo de conformidad por anticipado con los términos de un contrato a otro de conformidad automática. La gente ya no elegirá cumplir o no cumplir, lo hará automáticamente o simplemente dejará de acceder.

- ## Personalización de servicios

Este rasgo del capitalismo de la vigilancia es bien conocido. Es lo que hace Google cuando nos muestra anuncios según nuestro perfil, o cuando Amazon nos recomienda lecturas de acuerdo a lo que nos ha interesado en el pasado, o cuando Netflix recolecta información sobre lo que vemos para hacernos sugerencias. Está claro que cuando nos vinculamos con este tipo de servicios trocamos información personal por una experiencia a la que probablemente damos valor y disfrutamos.

Puede no parecer nada especialmente siniestro. Pero hay que considerar que, a diferencia de otras transacciones de información por comodidad que podamos hacer en algunos ámbitos (como en la relación con nuestro doctor o con nuestro abogado), las comunicaciones que hacemos no son confidenciales y pueden trascender la plataforma en particular a la que las hemos confiado. Además, no hay límites intrínsecos al alcance de la información extraída, ni en su volumen, ni en el uso que se le dará ni en cómo se la analizará para obtener más información.

La realidad es que los usuarios en general no tienen ni idea de lo que están dando a cambio. Así, resalta Zuboff, el capitalismo de la vigilancia da lugar a una redistribución masiva de los derechos relativos a la privacidad desde los ciudadanos privados hacia compañías con modelos de negocios basados en la vigilancia. Porque el derecho a la privacidad es, antes que nada, un derecho a decidir. Es el derecho de elegir qué queremos compartir, en qué contexto y con qué personas físicas o jurídicas, en un amplio espectro que va desde la privacidad completa hasta la transparencia total. El capitalismo de la vigilancia permitió a ciertas grandes compañías ejercer más y más control sobre ese tipo de decisiones. Son ellas quienes deciden qué datos recolectar y qué hacer con ellos, no

nosotros.

- **Experimentación continua**

El último rasgo del capitalismo de la vigilancia consiste en el hecho de que la infraestructura tecnológica permite una experimentación y una intervención continua sobre la vida de los usuarios. Es fácil testear diferentes servicios digitales usando grupos de control basados en los perfiles de los usuarios. El famoso ejemplo de cómo Facebook intentó manipular el estado de ánimo (Links to an external site.) de sus suscriptores es paradigmático. Según Zuboff, este tipo de intervención implica ir de la "minería de datos" a la "minería de la realidad". Porque con esta experimentación continua la infraestructura tecnológica contribuye a capturar y alterar los objetos, personas y eventos del mundo real con el fin de incrementar el beneficio económico y de ejercer el control (si viste Viaje a las Estrellas, sería algo así como la Colectiva Borg).

Finalmente, digamos que sería un error acusar solamente a las empresas de llevar a cabo modelos de negocios basados en la vigilancia. Porque los estados también se aprovechan de dichos modelos de negocios cuando se apropian de los datos recolectados por corporaciones privadas. Y porque, por otra parte, indirectamente apoyan esta forma de hacer dinero mediante leyes, normativas fiscales o incluso incentivos para que la población utilice plataformas cuyo negocio se basa en la vigilancia. Ningún negocio privado puede existir si no es en el marco de una regulación estatal explícita o implícita.

3.3. Plataformas privativas, cerradas y centralizadas vs. protocolos públicos descentralizados: la disputa política alrededor del software y cómo gestionarlo

No voy a mentirte, es perfectamente factible un modelo de negocios vigilantista basado en software libre. No por nada una de las herramientas más populares para hacer analítica de Big Data es Hadoop, que es libre y abierta. Sin embargo, es bastante más difícil encontrar ecosistemas informáticos basados en plataformas cerradas que no compartan los rasgos arriba mencionados del capitalismo de la vigilancia. Justamente, el vigilantismo ha sido uno de los elementos cuestionables que el movimiento del software libre ha venido denunciando por décadas con respecto a compañías como Microsoft y Apple, entre otras. Hoy esta tendencia ya excede a la industria del software, sino que abarca varias industrias, incluso aquellas que se enfocan más al hardware.

Así reflexionaba Richard Stallman en el artículo "¿Cuánta vigilancia puede soportar la democracia?":

Usar software libre, como he defendido desde hace 30 años, es el primer paso para tomar el control de nuestra vida digital, y eso incluye la prevención de la vigilancia. No podemos confiar en

*el software que no es libre. La NSA (Agencia de Seguridad Nacional) usa e incluso crea vulnerabilidades de seguridad en el software que no es libre para poder invadir nuestros ordenadores y r*outers. *El software libre nos permite ejercer el control sobre nuestras propias computadoras, pero eso no protegerá nuestra privacidad una vez que pongamos los pies en Internet.*

Por si no estás tan en tema, te recuerdo que un software es libre si permite:

1. La libertad de ejecutar el programa con cualquier propósito.
2. La libertad de estudiar cómo funciona el programa y adaptarlo a las necesidades propias.
3. La libertad de redistribuir copias del programa y de ese modo ayudar a otros.
4. La libertad de mejorar el programa y liberar esas mejoras al público beneficiando así a toda la comunidad.

Y un software es privativo si nos priva de ejercer alguna de las libertades antes expuestas. Esto puede ser porque sus términos de licencia lo prohíban o porque su fabricante no pone a disposición de la comunidad el código fuente necesario para poder ejercer fácticamente las libertades 1 y 3.

Un software privativo, por lo tanto, puede contener funcionalidades orientadas a la vigilancia sin que nadie pueda saberlo. También podría no tenerlas pero, justamente porque es privativo, tampoco lo sabremos. Sí se sabe, por ejemplo, que la NSA colaboró en el desarrollo de Microsoft Windows 7. No se me ocurren muchos motivos por los cuales una agencia de espionaje pueda intervenir en el desarrollo de un sistema operativo de uso masivo, excepto espiar, claro.

Un software libre también podría tener funcionalidades orientadas a la vigilancia pero, como su código fuente estaría a disposición del público, en algún momento alguien con conocimientos de programación podría descubrirlo y denunciarlo. Y, como también podría modificarlo y compartir las modificaciones, también estaría en condiciones de distribuir otra versión que no contuviera dichas funcionalidades cuestionables.

A continuación, para que tengas un listado de software privativo de uso común y cómo vigila al usuario, te paso una parte de este artículo de la Free Software Foundation. Me gustaría traducirlo entero pero es un poco largo.

Spyware en sistemas operativos

Spyware en Windows

- *Windows 10 viene con configuraciones por defecto que no tienen ningún cuidado por la privacidad de los usuarios, lo que da a Microsoft el "derecho" de espiar los archivos de éstos, el ingreso de texto y de voz, información de ubicación, contactos, registros de la agenda e historial de navegación, y también conecta automáticamente las máquinas a hotspots abiertos y muestra anuncios personalizados.*
- *Windows 10 envía a Microsoft información identificable, incluso si el usuario desconecta el buscador Bing y la función Cortana, y activa la configuración de protección de la*

privacidad.

- *Microsoft Windows 10 usa una "política de privacidad" que abiertamente se reserva el derecho de mirar los archivos de los usuarios en cualquier momento. La encriptación completa del disco de Windows 10 le da a Microsoft una clave.*
- *Entonces, Windows es malware al descubierto con respecto a la vigilancia, como lo es en otros respectos.*
- *Podemos suponer que Microsoft mira los archivos de los usuarios a pedido del gobierno de Estados Unidos, aunque la "política de privacidad" no lo dice explícitamente. ¿Miraría también los archivos de los usuarios a pedido del gobierno chino?*
- *La "ID publicitaria" única para cada usuario permite a otras compañías rastrear la navegación de cada usuario específico.*
- *Es como si Microsoft hubiera elegido deliberadamente hacer Windows 10 máximamente malvado en cada dimensión, para obtener poder total sobre cualquiera que todavía no haya abandonado Windows.*
- *Se pone peor con el tiempo.Windows 10 requiere a los usuarios dar permiso para el espionaje total, incluyendo sus archivos, sus comandos, sus ingresos de texto y de voz.*
- *Windows 8.1 espía las búsquedas locales.*
- *Y hay una clave secreta de la NSA en Windows, cuyas funciones no conocemos.*

El espionaje de Microsoft sobre los usuarios no comenzó con Windows 10. Hay mucho más malware de Microsoft.

Spyware en MacOS

- *MacOS envía automáticamente a los servidores de Apple los documentos sin guardar que están siendo editados. Las cosas que uno no decidió guardar son aún más delicadas que las almacenadas en archivos.*
- *Apple hizo diversos programas para MacOS que envían archivos a los servidores de Apple sin pedir permiso. Esto expone a los archivos al Hermano Mayor y quizá a otros espías.*

También demuestra que uno no puede confiar en el software propietario, porque incluso si la versión actual no tiene una funcionalidad maliciosa, la de mañana sí podría añadirla. El desarrollador no eliminará la funcionalidad mala a menos que muchos usuarios presionen fuertemente, y los usuarios no podrán eliminarla por sí mismos.

- *Diversas operaciones en el último MacOS envían informes a servidores Apple.*
- *Apple admite que espía mediante un servicio de búsqueda, pero hay mucho más espionaje del que Apple no ha hablado.*
- *Las búsquedas con Spotlight envían los términos de búsqueda a Apple.*

Hay mucho más iThing spyware y malware Apple.

Spyware en Android

- *Las aplicaciones gratuitas Android (que no son software libre) se conectan en promedio a*

100 URLs de rastreo y publicidad.

- *Hay spyware presente en algunos dispositivos Android desde que se venden. Algunos teléfonos Motorola modifican Android para enviar datos personales a Motorola.*
- *Algunos fabricantes añaden un paquete general de vigilancia, como Carrier IQ.*
- *Las puertas traseras de Samsung brindan acceso a cualquier archivo del Sistema.*

Spyware en móviles

Spyware en iThings

- *Las iThings* [cosas que empiezan con "i", los productos típicos de Apple] *suben automáticamente a los servidores de Apple todas las fotos y videos que hacen. "La iCloud Photo Library almacena cada foto y video que sacas y los mantiene actualizados en todos tus dispositivos. Cualquier edición que hagas se actualiza automáticamente en todas partes [...] (de la información de Apple iCloud, accedida el 24 de septiembre de 2015). La función iCloud se activa al arranque de iOS. La palabra "nube" significa "por favor no preguntes dónde".*
- *Hay una manera de desactivar iCloud, pero está activo por defecto, así que igual cuenta como funcionalidad para la vigilancia. Aparentemente, desconocidos aprovecharon esto para conseguir fotos de muchas celebridades desnudas. Ellos necesitan romper la seguridad de Apple para accederlas, pero la NSA puede hacerlo mediante PRISM.*
- *Spyware en iThings: el iBeacon permite a las tiendas determinar exactamente dónde está la iThing, y también conseguir otra información.*
- *Hay otra funcionalidad para que los sitios rastreen a usuarios que está activa por defecto. (el artículo habla sobre iOS 6, pero también es válido para iOS 7).*
- *La iThing por defecto le dice a Apple su geolocalización, aunque eso puede desactivarse.*
- *Apple puede extraer a distancia, y regularmente lo hace, algunos datos de iPhones para el estado.*
- *O bien Apple ayuda a la NSA a espiar todos los datos de la iThing, o es completamente incompetente.*
- *Algunas "funciones" de iOS no parecen servir a otro propósito más que la vigilancia. He aquí la presentación técnica.*

3.4. La privacidad de las comunicaciones en el marco de los dispositivos "inteligentes" (o de inteligencia)

Una forma muy efectiva de rastrear a alguien es por medio de su teléfono móvil, usando un dispositivo llamado *IMSI catcher*, que funciona a una distancia de unos cientos de metros. Un

international mobile subscriber identity (IMSI) es el identificador de la tarjeta SIM del teléfono y, por lo tanto, de su dueño. Los diseñadores de celulares querían prevenir accesos no autorizados a las señales inalámbricas de modo que pudiera leerse el IMSI y, por lo tanto, crearon identificadores temporarios llamados TMSIs, que cambian frecuentemente. Lamentablemente, el diseño de los protocolos es defectuoso y hay maneras de chequear los IMSIs y rastrear la presencia de teléfonos

Por otra parte, algunas compañías telefónicas ofrecen servicios para que amantes, esposas, abogados o cualquiera encuentre dónde está alguien o rastree sus movimientos mediante la capacidad GPS de su teléfono móvil. Un político alemán que solicitó información sobre su ubicación en un período de seis meses descubrió que en ese lapso la longitud y latitud donde se encontraba fue almacenada 35 mil veces.

Muchos aparatos móviles y aplicaciones de las que nos descargamos de las tiendas online de los fabricantes pueden rastrearnos por donde vayamos también. Un tercio al menos de esas aplicaciones pide otros datos personales excesivos. La información en riesgo no es solo la relativa a la propia intimidad, sino también la relacionada con datos confidenciales de nuestros respectivos trabajos. Muchas empresas obligan a sus empleados a emplear ciertas medidas de protección para los dispositivos móviles propios que se usen también para fines laborales. Pero, aunque dichas medidas puedan brindar algo más de protección contra intrusiones externas, lo hacen al precio de someter a la persona a una especial vigilancia adicional por parte de sus empleadores.

Otro factor de riesgo en el que incurrimos frecuentemente tiene que ver con el uso de redes wi-fi públicas. Cualquiera podría interceptar los datos en ese tipo de redes. El robo o pérdida de los equipos móviles también expone la información. Existen modos de acotar estos riesgos, pero pocos los conocen o los usan.

Finalmente, las cámaras incorporadas en los teléfonos móviles también podrían usarse para transmitir información de situaciones que deberían permanecer privadas. Si estas capturas de imágenes luego se combinan con sistemas de reconocimiento facial basados en la nube, el relativo anonimato que uno siente al caminar despreocupadamente por la calle deja de existir, ya que alguien podría no solo estarnos filmando, sino estar obteniendo una mini biografía nuestra en cualquier momento y lugar. Dispositivos como Google Glass también despiertan este tipo de preocupación.