Módulo 2: El nuevo paradigma de la vigilancia

2.1. Reflexiones fuera de programa

No es fácil continuar con un curso donde tratamos de cuestionar el vigilantismo contemporáneo luego de los recientes atentados en Francia. Son cosas que hacen decir a muchos “déjense de fastidiar con la privacidad y esas cosas, mejor que nos investiguen a todos y se prevenga el terrorismo a que pasen cosas tan horrendas como esa”.

Por cierto, Francia ya tenía desde mayo piedra libre para emprender ese camino, ya que aprobó una ley que le permite:

- Controlar y monitorizar comunicaciones personales como correos electrónicos o llamadas de teléfono sin necesidad de una orden judicial.
- instalar en áreas específicas del país unos dispositivos conocidos como ISMI, que permiten rastrear todas las comunicaciones móviles producidas dentro de una zona determinada, e incluso seguir los movimientos de quienes estén usando dispositivos móviles.
- Implementar “cajas negras” que registren y analicen la actividad de millones de ciudadanos en Internet.

Por eso quería comenzar el nuevo módulo refiriéndome a un asunto que no estaba planeado inicialmente para el programa del curso, aunque claramente hubiera podido estar: la minería de datos.

Hasta ahora, hemos hablado de la recolección masiva de datos personales. Pero tener una enorme cantidad de datos no equivale a obtener información significativa y útil para fines comerciales o para prevención de delitos. Para apuntar a ese tipo de objetivos es necesario utilizar técnicas de “minería de datos” o “data mining”. Es decir, usar métodos de la inteligencia artificial, aprendizaje automático, estadística y sistemas de bases de datos para encontrar patrones en grandes volúmenes de datos de un modo automático o semi automático. La minería de datos se usa rutinariamente para detectar y prevenir fraudes financieros, identificar clientes que podrían abandonar servicios de telecomunicaciones, u ofrecer otros productos a quienes ya han comprado algo en un sitio web, entre otras aplicaciones.

Parece tener mucho sentido, entonces, la idea de recolectar todo tipo de datos de la mayor cantidad posible de la población mundial, analizarlos con técnicas de minería de datos y así poder prevenir el terrorismo. Sin embargo, no es así y, para mostrártelo, voy a transcribirte la traducción de este blog del experto en seguridad informática Bruce Schneier:

Por qué la minería de datos no detendrá el terror

9 de marzo de 2005

En el mundo después del 9/11 hay mucho foco en conectar puntos. Muchos creen que la minería de datos es la bola de cristal que nos permitirá descubrir futuros planes terroristas. Pero aún en las proyecciones más salvajemente optimistas la minería de datos no es sostenible para dicho propósito. No estamos cambiando privacidad por seguridad: estamos abandonando la privacidad sin obtener ninguna seguridad a cambio.

La mayoría de la gente supo de la minería de datos en noviembre de 2002, con las noticias sobre el programa gubernamental masivo de minería de datos llamado Total Information Awareness. La idea básica era tan audaz como repelente: absorber todos los datos posibles sobre todo el mundo, tamizarlos con computadoras masivas, e investigar patrones que puedan indicar planes terroristas.

Estadounidenses de todo el espectro político denunciaron el programa y, en septiembre de 2003, el Congreso eliminó sus fondos y cerró sus oficinas.

Pero TIA no murió. Según The National Journal, solo cambió de nombre y se mudó al Departamento de Defensa.

Esto no debería ser una sorpresa. En mayo de 2004, la Oficina General de Contaduría publicó un reporte que listaba 122 programas federales diferentes gubernamentales de minería de datos que usaban información personal de la gente. Esta lista no incluía programas clasificados, como el esfuerzo de escuchas de la NSA o programas ejecutados por el estado como MATRIX.

La promesa de la minería de datos es atractiva y convence a muchos. Pero está equivocada. No vamos a averiguar planes terroristas mediante sistemas como éste y vamos a desperdiciar recursos valiosos cazando falsas alarmas. Para entender por qué, debemos mirar la economía del sistema.

La seguridad siempre es un compromiso y, para que un sistema valga la pena, las ventajas deben ser mayores que las desventajas. Un programa nacional de seguridad basado en minería de datos encontrará cierto porcentaje de ataques reales y cierto porcentaje de falsas alarmas. Si los beneficios de encontrar y detener esos ataques superan el costo en dinero, en libertades, etc., entonces es un buen sistema. Si no, es mejor invertir el capital de otro modo.

La minería de datos funciona mejor cuando uno está buscando un perfil bien definido, hay una cantidad razonable de ataques al año y las falsas alarmas generan bajos costos. El fraude con tarjetas de crédito es una de las historias de éxito de la minería de datos: todas las compañías de tarjetas de crédito minan sus bases de datos de transacciones para buscar datos que muestren patrones de gasto que indiquen una tarjeta robada.

Muchos ladrones de tarjetas de crédito comparten un patrón: compras de bienes de lujo costosos, compras de cosas fácilmente revendibles, etc. Y los sistemas de minería de datos pueden minimizar las pérdidas en muchos casos dando de baja la tarjeta. Además, el costo de las falsas alarmas es solo una llamada de teléfono al usuario para pedirle que verifique un par de compras. Los usuarios ni siquiera se molestan por dichas llamadas, siempre que sean infrecuentes, así que el

costo es solo unos pocos minutos del tiempo de un operador.

Los planes terroristas son diferentes. No hay perfiles bien definidos y los ataques son muy raros. En conjunto, estos hechos significan que los sistemas de minería de datos no descubrirán ningún plan terrorista hasta lograr ser muy exactos, y aun los sistemas muy exactos estarán tan inundados de falsas alarmas que serán inútiles.

Todos los sistemas de minería de datos fallan de dos maneras diferentes: falsos positivos y falsos negativos. Un falso positivo es cuando el sistema identifica un plan terrorista cuando en realidad no lo hay. Un falso negativo es cuando el sistema no advierte un plan terrorista real. Según cómo uno ajuste sus algoritmos de detección, puede errar de uno u otro modo: puede incrementar la cantidad de falsos positivos para garantizar que es menos probable omitir un plan terrorista real, o puede reducir la cantidad de falsos positivos a expensas de omitir planes terroristas.

Para reducir ambos números, se necesita tener un perfil bien definido. Y ése es el problema cuando se trata de terrorismo. En retrospectiva, era realmente fácil conectar los puntos relativos al 9/11 y apuntar a los signos de alarma, pero es mucho más difícil hacerlo antes del hecho. Cuanto mejor uno defina lo que está buscando, mejores resultados obtendrá. La minería de datos para planes terroristas puede ser chapucera y será difícil que encuentre nada útil.

La minería de datos es como buscar una aguja en un pajar. Hay 900 millones de tarjetas de crédito en circulación en Estados Unidos. Según el Informe de la Encuesta de Robo de Identidad de la FTC de septiembre de 2003, cerca del 1 por ciento (10 millones) de las tarjetas son robadas y usadas fraudulentamente cada año.

Cuando se trata de terrorismo, sin embargo, existen billones de conexiones entre las personas y los eventos, cosas a las cuales los sistemas de minería de datos tendrán que "mirar", y muy pocos planes terroristas en comparación. Esta rareza hace que aún los sistemas más exactos sean inútiles.

Veamos unas cifras. Seremos optimistas, asumiremos que el sistema solo tiene uno en cien falsos positivos (99 por ciento de exactitud), y uno en mil falsos negativos (99,9 de exactitud). Supongamos que hay un billón de posibles indicadores para tamizar: esto es alrededor de 10 eventos por persona –mensajes de correo electrónico, llamadas de teléfono, destinos en la Web, cualquier cosa- en los Estados Unidos, por día. También supongamos que diez de ellos realmente están tramando un plan terrorista.

Este irrealmente exacto sistema generaría mil millones de falsas alarmas por cada plan terrorista real que descubriera. Cada día de cada año, la policía tendría que investigar 27 millones de planes potenciales para encontrar el único plan terrorista real mensual. Elevemos la exactitud de falsos positivos a un absurdo 99,9999 por ciento y estaremos cazando 2.750 falsas alarmas por día. Pero eso inevitablemente elevaría los falsos negativos y estaríamos omitiendo algunos de los 10 planes reales.

Esto no es nuevo, se llama la "falacia de la tasa base", y aplica a otros dominios también. Por ejemplo, incluso las pruebas médicas más exactas son inútiles como herramientas diagnósticas si

la incidencia de la enfermedad es rara en la población general.

Los ataques terroristas son también raros y cualquier "prueba" resultará en una corriente sin fin de falsas alarmas.

Esta es exactamente la clase de cosa que hemos visto con el programa de escuchas de la NSA: el New York Times informó que las computadoras escupieron miles de pistas por mes. Cada una de ellas resultó ser una falsa alarma.

Y el costo fue enorme, no solo para los agentes del FBI corriendo para cazar pistas que no llevaban a ningún lado en vez de hacer cosas que realmente podría ponernos más a salvo, sino también en el costo en libertades civiles. Las libertades fundamentales que hacen de nuestro país la envidia del mundo son valiosas, no algo que debiéramos descartar a la ligera.

La minería de datos puede funcionar. Visa mantiene así bajos sus costos de fraude, así como Amazon me alerta de libros que podría querer comprar y Google me muestra anuncios en los cuales probablemente estaré interesado. Pero estos son todos ejemplos donde el costo de los falsos positivos es bajo (una llamada telefónica de un operador de Visa o un anuncio poco interesante) en sistemas que tienen valor aun si hay una alta cantidad de falsos negativos.

Encontrar planes terroristas no es un problema que se preste a la minería de datos. Es un problema de encontrar una aguja en un pajar, y tirar más heno en la pila no hace el problema más fácil. Haríamos mucho mejor poniendo gente a cargo de investigar planes potenciales y dejando que ellos dirijan a las computadoras, en lugar de poner a las computadoras a cargo y dejarlas decidir quién debería ser investigado.

2.2. De la doctrina de la seguridad nacional a la vigilancia masiva: cambios en el paradigma. La cooperación entre el sector privado y el sector público en la recolección y análisis masivo de datos

Probablemente ya habrás oído o leído que vivimos en una sociedad de la vigilancia. Esta noción, acuñada por Gary Marx en 1985, preanunciaba el advenimiento del «control social total», de la mano de la informática, Y no es solamente porque seamos muy descuidados con la información que compartimos en Internet (yo suelo llamar a esa línea de argumentación "culpar a la víctima": si alguien o algo registra tus movimientos las 24 horas del día, algo habrás hecho para merecerlo. Es una coartada habitual de personas físicas y jurídicas que suponen que cada individuo debe poner los medios para no ser vigilado, en lugar de ser ellas quienes operen en un marco de respeto por los derechos humanos). Más bien, vivimos en una sociedad de la vigilancia porque la recolección y procesamiento constantes de información personal son vitales para el modo de vida contemporáneo. He aquí algunos ejemplos:

- Una huella digitalizada se genera y se almacena automáticamente sobre todo lo que hacemos

o decimos cuando estamos online.
- La policía y otras agencias de cumplimiento de la ley usan rutinariamente los datos de ubicación de los teléfonos móviles para saber dónde han estado individuos de interés.
- También es posible usar los teléfonos móviles como micrófono para grabar conversaciones, aunque estén apagados.
- Los vehículos que utilizan sistemas de localización satelital GPS pueden ser ubicados sin necesidad de una orden judicial.
- Los sistemas de identificación biométrica son de uso creciente en el mundo y se usan tanto para transacciones con el estado como con entidades privadas.
- Se insertan chips RFID en cada vez más productos de consumo, incluso se ha propuesto implantarlos en humanos.
- Hay sistemas de reconocimiento facial integrados en cámaras de vigilancia.
- Las cámaras de vigilancia no solo registran imágenes, sino también pueden registrar sonidos y conversaciones.
- Se impulsa la creación de bases masivas de datos genéticos, que no solo revelan información sobre un individuo sino que también podrían involucrar a personas de su familia.
- Las empresas no solo retienen grandes cantidades de datos personales sobre sus clientes, sino que también les dan acceso a los mismos a los gobiernos.
- Se combinan datos personales de diferentes orígenes y tipos.
- La minería de datos, las técnicas de Big Data y el monitoreo de la actividad online de las personas pueden producir perfiles muy precisos con información excesivamente personal.
- La existencia de vigilancia por parte de gobiernos y empresas, muchas veces ilegal, de las comunicaciones privadas es cada vez más común.
- Muchos aeropuertos someten a los pasajeros en tránsito a escaneos de cuerpo completo mediante equipos que generan imágenes semejantes a las de la persona sin ropas.
- Están en desarrollo y quizá en uso dispositivos capaces de ver los movimientos de alguien a través de paredes, de modo que deje de ser necesario obtener una orden judicial para ver lo que ocurre en un domicilio privado.
- Vehículos no tripulados, también llamados drones, que portan cámaras, son desplegados cada vez más con fines de vigilancia doméstica.
- Hay investigaciones en curso en neurotecnologías capaces de, prácticamente, leer los pensamientos.
- La llamada “Internet de las cosas” produce un entorno total donde todo el mundo pueda estar siendo registrado todo el tiempo, aún en el interior de su hogar.
- En los ámbitos laborales, las personas hoy están todo el tiempo bajo la mirada de las cámaras, se registra cada tecla que oprimen en sus computadoras y hasta se graban sus conversaciones telefónicas.

Para ver muchos casos concretos de estas y otras formas de usar la tecnología al servicio del vigilantismo, haz click aquí.

Es importante hacer notar que la vigilancia siempre ha existido y no necesariamente implica una práctica abusiva. Como dice David Lyon en *El Ojo Electrónico*, hay registros de que ya en la antigüedad se ha vigilado a otros para comprobar qué tramaban, para controlar su progreso, para organizarlos o para cuidarlos. Los antiguos egipcios, por ejemplo, llevaban registros de población con fines fiscales, inmigratorios y militares. Y el libro de los Números, de la Biblia, registra que el pueblo nómada de Israel emprendió varios censos de población en el siglo XV A. C. En épocas más recientes, año 1086, un libro catastral inglés llamado *Domesday Book* registraba hechos específicos sobre personas y propiedades. Por cierto, es interesante observar que, para que pudieran existir estos registros antiguos hizo falta disponer de la técnica de la escritura. Hoy las técnicas son otras.

El cambio que hoy experimentamos en forma tan aguda hacia un mayor vigilantismo en realidad comenzó hace unos 400 años, con la paulatina "racionalización" o "burocratización" de las prácticas organizacionales, que tendió a remplazar las redes sociales informales y controles cotidianos en los que se basaban previamente en general las transacciones. Quien mejor analizó este proceso fue Max Weber en 1947, en su influyente obra "Economía y Sociedad". Allí el sociólogo define administración burocrática como:

…el ejercicio del control sobre la base del conocimiento. [...]. Esto consiste, por un lado, en el conocimiento técnico que, por sí mismo, es suficiente para asegurar una posición de extraordinario poder. Pero, además, las organizaciones burocráticas, o quienes detentan el poder de usarlas, tienden a incrementar más aún su poder por el crecimiento del conocimiento que deviene de su experiencia en el servicio.

Se suele citar como un logro de la modernidad que las personas hayan pasado a ser reconocidas como identidades únicas e iguales ante la ley. El problema es que justamente eso hizo al mismo tiempo mucho más sencillo su control. El ejercicio del control requiere garantizar la previsibilidad. Y la previsibilidad sólo se obtiene en el marco de la construcción de sistemas formales. El peligro es que, como auguró Weber para la burocratización, el ejercicio del control sobre la base del conocimiento convierta a la sociedad en una jaula de hierro. Por ejemplo, las tarjetas inteligentes que permiten a un médico acceder rápidamente a la historia clínica completa de un paciente pueden, por un lado, permitir salvarle la vida en caso de accidente pero, por otro, la difusión de los datos que contiene podría ser usada para discriminarlo en contextos laborales o crediticios.

El análisis de Weber, aplicado a la problemática de la nueva vigilancia, abre el tema de la multiplicidad de poderes asociados con su ejercicio, más las desigualdades informacionales que paralelamente genera. Por un lado, se puede decir que toda una generación de administradores de bases de datos, altamente especializados y de formación principalmente técnica, tiene acceso privilegiado a la recolección y análisis de los datos personales de mucha gente y participan en las decisiones sobre su ulterior uso. Constituyen quienes, en términos de Weber, detentan el poder de hacer valer el poder de su experiencia en las instituciones burocráticas o las corporaciones donde trabajan. Por otra parte, dichas instituciones o empresas participan de la acumulación capitalista en el actual mundo globalizado, y constituyen un poder opaco que conoce todo sobre todos, sin que nadie sepa demasiado sobre su conformación, intereses y fines concretos.

En el mismo sentido Giddens (*El Estado-Nación y la Violencia*, 1985) dice que las sociedades modernas tienen varias dimensiones institucionales de fundamental importancia, ninguna de las cuales es reducible a otra. Se trata del capitalismo, el industrialismo, el poder militar y la vigilancia. Para este autor el totalitarismo es, ante todo, una atención extrema a la vigilancia.

Panopticismo y más allá

El concepto de «sociedad de la vigilancia» tiene un importante antecedente en el de «sociedades disciplinarias», de Michel Foucault (*Vigilar y Castigar*, 1976). En ellas, el individuo nunca cesa de pasar de un ambiente cerrado a otro, donde la estructura física es de carácter panóptico. Es decir que, desde un centro, puede observarse cada rincón del edificio. La prisión es el modelo analógico de dichos lugares. Aunque Foucault ubica el origen de las sociedades disciplinarias en los siglos XVIII y XIX, éstas habrían alcanzado su cúspide en el XX.

Otro concepto afín con el propuesto por Gary Marx para englobar las actuales tendencias sociales pertenece a Gilles Deleuze (*Postcriptum a las sociedades de control*, 1992). Según este autor, ya no estamos en sociedades disciplinarias, sino en sociedades de control. Entre otras razones, porque los ambientes o "interiores" que eran el centro del ejercicio de la disciplina (la familia, el ejército, la escuela, el hospital y la prisión) hoy están en crisis. El control social asociado a dichas instituciones ya no está espacialmente marcado, asociado a un determinado ambiente cerrado, sino que puede seguirlo a uno a todas partes. Como glosa Lyon, "El trabajador podía en tiempos dejar la empresa capitalista tras las puertas de la fábrica. Ahora, ésta le sigue hasta su casa como consumidor". Como consecuencia, dice Deleuze, "ya no lidiamos con el par masa/individuo. Los individuos se han convertido en dividuos, y son masas, muestras, datos, mercados o bancos".

El filósofo explica que las antiguas sociedades de la soberanía (que precedieron a las disciplinarias y se orientaban a gravar, más que a organizar la producción y a regular la muerte, antes que a administrar la vida) usaban máquinas simples: palancas, poleas, relojes. Sin embargo, "las sociedades de control operan con máquinas de tercer tipo, computadoras, cuyo peligro pasivo es que se atasquen y su peligro activo es la piratería y los virus".

David Lyon (1995) realiza una crítica a los análisis demasiado "foucaultianos" de la moderna vigilancia, cuando dice que "por mucho que estas prácticas de la vigilancia del consumidor recuerden a métodos tayloristas o panopticistas, es preciso reconocer que el principio guía del orden del consumo es el placer, no el dolor ni la coerción".

Otra característica de la sociedad de la vigilancia que ciertas conceptualizaciones no atienden lo suficiente es su carácter global, acorde con la actual etapa del capitalismo. Como dice Lyon (op. cit):

En la actualidad, es cierto que los «centros» gubernamentales y comerciales de los estados contemporáneos siguen teniendo acceso a archivos sobre poblaciones de gran volumen, pero la extensión de las redes de ordenadores también descentraliza las operaciones.

En general, las características de la nueva vigilancia, que la distinguen de formas previas de control social, son las que enumera Gary Marx, en su libro *Undercover* (p. 208.):

1. Trasciende la distancia, la oscuridad y las barreras físicas.
2. Trasciende el tiempo, lo que puede observarse especialmente en la capacidad de almacenamiento y recuperación de la información de los ordenadores;
3. la información personal puede «liofilizarse», o convertirse en un "extracto" como el de las conservas de alimento.
4. Es escasamente visible, o directamente invisible: los sujetos de los datos son cada vez menos conscientes de ella.
5. Es frecuentemente involuntaria.
6. La prevención es uno de sus objetivos fundamentales: piénsese en los libros dotados con códigos de barras en las bibliotecas o en las cámaras de video en las tiendas, instaladas para prevenir las pérdidas y no la inmoralidad del robo.
7. Hace uso intensivo del capital, y no del trabajo, lo que hace su atractivo económico cada vez mayor.
8. Implica un autocontrol policial centralizado: participamos en nuestra propia vigilancia.
9. Desencadena un cambio desde la identificación de sospechosos específicos hacia la sospecha categorial.
10. Es, simultáneamente, más intensiva y más extensiva.

La importancia de un enfoque social, no técnico, sobre la vigilancia

Entender la sociedad de la vigilancia como un subproducto de la modernidad es útil para evitar pensar la vigilancia en términos conspirativos, como si fuera un simple fruto de algún complot deliberadamente maligno, y también permite ubicarla en un contexto social, en lugar de suponer que es un simple efecto del desarrollo técnico (es decir, permite estudiarla sin caer en el determinismo tecnológico). Como dice Lyon:

Existe diversidad de opiniones respecto a la interacción entre «tecnología» y «sociedad». Pero incluso el plantear las cuestiones de este modo es caer en la trampa de suponer que ambas pueden existir separadamente de algún modo [...]. Tiene mucho sentido concebir la tecnología como una actividad con dimensiones sociales, políticas, económicas y culturales.

Por ejemplo, uno podría caer en la tentación de haber definido privacidad como "aquello que puede perderse bajo excesiva vigilancia". Pero los análisis de corte más sociológico permiten resaltar el hecho de que la excesiva vigilancia no solamente hace perder privacidad, sino también dignidad, igualdad de oportunidades, libertad de expresión, justicia social y respeto por las minorías, entre otros valores.

Por otra parte, el vigilantismo justamente pone en cuestión la esencia misma de lo privado. Porque, por ejemplo, el hogar solía ser un ámbito privado por excelencia, donde nadie podía entrometerse, salvo causas graves y con orden judicial. Pero ahora tenemos televisores inteligentes que registran lo que vemos, teléfonos celulares que hasta pueden revelar hacia afuera si acaso estamos en el baño dentro de nuestro domicilio, computadoras que, por más hogareñas que sean, revelan hacia el exterior consumos, lecturas, gustos, costumbres. Paralelamente, en la calle, tradicionalmente considerada un lugar público, también podemos tener expectativa de no ser sometidos a un exceso

de vigilancia. Hoy lo privado o lo público ya no puede pensarse solamente en relación con espacios fijos.

Lo privado y lo público se cruzan también por simple filtración de datos entre ambos ámbitos. Por ejemplo, por medio de las compañías de seguros, de las agencias de seguridad privadas (cuyos hallazgos son utilizados por los cuerpos policiales) y del control de los trabajadores; éste último ha generado datos que se utilizan extensamente dentro y fuera de la administración gubernamental para vetar candidaturas a puestos de trabajo o promociones. Además, en la actualidad, el ser aceptado como un miembro de la sociedad plenamente participativo depende cada vez más de la capacidad de consumo del individuo, y gran parte de la vigilancia contemporánea es de hecho comercial. Si el gobierno parece operar cada vez más por criterios comerciales, parece también que ciertas corporaciones actúan de forma casi gubernamental.

2.3. La concentración de la infraestructura de las telecomunicaciones y su impacto sobre la privacidad

No todas las tecnologías que favorecen el vigilantismo son parte de Internet pero, ciertamente, las de Internet se encuentran entre las más utilizadas por gobiernos y empresas para este fin. La infraestructura de la Red facilita la vigilancia porque el tráfico de datos pasa en algún momento por routers que están en países donde es legal interceptar comunicaciones extranjeras, como Estados Unidos. En efecto, históricamente, los proveedores de Internet de regiones como Latinoamérica y África vieron elevados sus costos porque deben hacer pasar el tráfico a través de routers de Estados Unidos o Europa, incluso si dicho tráfico se origina en su mismo continente. Esto no solo genera ese problema de costos, sino que también facilita la vigilancia de las comunicaciones de los países periféricos por parte de los países centrales.

La solución no es “balcanizar” la red, o hacer silos aislados donde cada país tenga como si fuera su propia Internet, más bien habría que favorecer la multiplicación de la conectividad a través de una mayor diversificación de la infraestructura y, sobre todo, de sus propietarios. Pensemos que en América Latina el tráfico de Internet pasa, en un 98%, por cables, servidores y empresas de Estados Unidos, donde puede ser interceptado por los servicios de inteligencia de ese país.

El espionaje entre países es algo que siempre existió y todos hemos disfrutado de las populares películas sobre espías ambientadas en la época de la Guerra Fría. Pero ahora ya no se trata de infiltrarse en blancos políticos específicos. Ahora el objetivo es recolectar absolutamente todos los datos posibles de todos, y luego intentar analizarlos para encontrar la famosa “aguja en el pajar”.

La centralización de Internet también tiene lugar en lo que hace a almacenamiento y poder de cómputo. Supuestamente los datos que están en la “nube” están a salvo de intrusos mientras usen encriptación tanto en su almacenamiento como en su transmisión. Sin embargo, sería buena idea no confiar ciegamente en la “nube”, porque ésta no son más que sistemas concretos, no precisamente

"etéreos", que siempre pertenecen a alguien concreto y potencialmente pueden ser interceptados.

El ámbito del contenido en Internet también está muy centralizado. No el contenido en sí, que es producido por múltiples individuos, sino las plataformas que éstos usan para canalizarlo. En el mundo, solo cuatro empresas se reparten el 67 por ciento de los ingresos económicos generados: Amazon, Alphabet (nuevo nombre corporativo de Google), EBay y Facebook. Por otra parte, en la mayoría de los países latinoamericanos, los sitios de origen internacional (Google, Facebook, Microsoft, y Yahoo) ocupan las primeras cuatro posiciones en términos de visitantes únicos. Es decir, empresas cuyos servidores centrales están en Estados Unidos, donde incluso el tráfico configurado como privado puede ser interceptado.

La concentración del tráfico y los ingresos en pocas manos hace muy complicado para las grandes empresas de Internet resistan la tentación de abusar del poder que les otorga el ser depositarias de una enorme cantidad de datos de sus usuarios. En paralelo, los gobiernos tienen en dichas plataformas puntos únicos obvios para ir a buscar rastros de todos los ciudadanos, sin necesidad de causa probable previa para investigarlos, sin orden judicial y sin que nadie tenga por qué enterarse nunca de si lo hacen en forma cuestionable o no. Y, si en algún momento se denuncia una práctica abusiva, en general no es difícil justificarla en la lucha contra el terrorismo, la defensa de la seguridad nacional, la protección de los niños o incluso la prevención del crimen común.

2.4. El rol de los Estados Unidos y de las corporaciones norteamericanas

Es importante resaltar que el vigilantismo no es exclusivo de Estados Unidos. Sin embargo, dado que como mencionamos en el punto anterior ese país es tan central en la infraestructura mundial de comunicaciones, se hace necesario reseñar el origen de su rol en el desarrollo de las actuales tendencias hacia la vigilancia masiva global.

- Entre los antecedentes del vigilantismo actual conviene mencionar primero la historia de Bletchley Park (también conocido como "Estación X"), donde Winston Churchill ubicó su centro de control de inteligencia en Gran Bretaña durante la Segunda Guerra Mundial. La historia se mezcla con la trayectoria personal del gran matemático Alan Turing, que diseño las máquinas automáticas que descifraban cosas como el Código Enigma, utilizado por los nazis. En 1942, Turing viajó a Estados Unidos para supervisar la producción masiva de esas máquinas al otro lado del Atlántico, así como para trabajar en un sistema telefónico encriptado con Bell Laboratories, para que lo usaran los altos funcionarios gubernamentales. Pero Turing no portaba cartas de referencia de las autoridades británicas, así que fue detenido como sospechoso por el servicio de inmigración norteamericano, hasta ser rescatado por funcionarios del Reino Unido en Nueva York. Esto se conoció como el "affair" Turing.

- Este fue el origen de la alianza secreta de inteligencia surgida en la posguerra entre Estados Unidos y Reino Unido como miembros principales, secundados por Canadá, Australia y Nueva Zelanda y otras naciones con menor injerencia. Esto es lo que se denominó Tratado UKUSA. Su propósito era definir áreas de cooperación técnica y evitar conflictos de seguridad.
- Desde la fundación de la National Security Agency en Estados Unidos, los miembros del tratado UKUSA incrementaron sus capacidades de hacer inteligencia de señales (SIGINT), recolectando las que pasaban por cables submarinos en los puntos de llegada a tierra, las de satélites y antenas como las que se ubicaban en bases militares y embajadas. La evolución y la naturaleza de estas actividades fueron documentadas en informes de instituciones europeas sobre la red “ECHELON”, el nombre código de un sistema particular de vigilancia que suele usarse por extensión para referirse al nodo completo de vigilancia de comunicaciones del UKUSA.
- También hay que mencionar un hito en la historia del vigilantismo producido luego del escándalo Watergate, que culminó en la renuncia del presidente de Estados Unidos Richard Nixon en 1974. Por esa época el senador Frank Church encabezó una comisión legislativa para investigar los abusos de poder por parte de las agencias de seguridad y de inteligencia que habían llevado a cabo escuchas domésticas ilegales contra líderes políticos y cívicos. La pregunta era si se había violado la cuarta enmienda constitucional de ese país, que protege contra intromisiones ilegales, debido a que se había descubierto que había habido monitoreos masivos e intercepciones de comunicaciones internacionales desde 1940. La investigación, no obstante, concluyó que era tolerable la recolección inadvertida de datos de norteamericanos si se habían llevado a cabo procedimientos para minimizar el acceso erróneo sin orden judicial.
- Este proceso condujo a la *Foreign Intelligence Surveillance Act* de 1978 (FISA), que estructuró la intercepción de “inteligencia de información extranjera” junto con las operadoras de telecomunicaciones. La recolección de datos por parte de cualquier nación, por fuera de su territorio, no está restringida por ningún tratado explícito internacional. No sería de esperar otra cosa porque a ningún país le convendría comprometerse a no espiar a otros. Pero, ciertamente, un país con tantos recursos de todo tipo como Estados Unidos tiene muchas más posibilidades de recolectar datos de otros que los países menos poderosos.
- Luego de los ataques a las torres gemelas el 11 de septiembre de 2001, la privacidad y la protección de los datos se vieron profundamente afectadas por medidas supuestamente excepcionales tomadas en nombre de la seguridad y de la lucha contra el terrorismo.
- La ley llamada *USA Patriot Act* fue aprobada por el congreso de Estados Unidos el 26 de octubre de 2001, y su efecto principal fue incrementar enormemente el poder de las agencias de seguridad e inteligencia de recolectar información dentro del país. Pero otra ley llamada Foreign Intelligence Surveillance Amendment Act, de 2008, blanqueó la vigilancia masiva específicamente orientada a recolectar datos de personas que no vivían en el país ni eran nacionales de éste.
- La mayoría de los programas de vigilancia masiva global de Estados Unidos y sus aliados

era secreta incluso para miembros del Congreso de aquel país, hasta que en junio de 2013 el diario británico *The Guardian* reveló que la NSA, junto con sus contrapartes como el British Government Communications Headquarters (GCHQ), habían estado durante por lo menos una década registrando números telefónicos, horarios de llamadas y, en algunos casos, los contenidos de miles de millones de llamadas telefónicas, así como mensajes de correo electrónico, mensajes instantáneos, búsquedas en la Web e incluso chats de video. La fuente de estas informaciones era el excontratista de la NSA Edward Snowden.

- La primera revelación de Snowden se publicó el 6 de junio de 2013 y decía que la NSA había exigido mediante una orden secreta al gigante de las comunicaciones Verizon la entrega a la NSA y al FBI de los metadatos de millones de llamadas telefónicas de estadounidenses. Como la orden era secreta, Verizon no podía revelar públicamente dicha solicitud.
- Al día siguiente, salieron artículos en el *Washington Post* y en *The Guardian* detallando cómo un programa llamado PRISM daba a la NSA acceso directo a los servidores de algunas de las mayores compañías de tecnología, incluyendo Apple, Facebook, Google, Microsoft, Skype, Yahoo y YouTube. Según los documentos de Snowden, los controles que estas empresas estaban implementando para proteger la privacidad mediante encriptación estaban siendo inutilizados con ayuda de las mismas empresas. En el Reino Unido, un programa llamado Tempora se constituyó en una red de vigilancia masiva que daba al GCHQ (General Communications Headquarters, el equivalente a la NSA en ese país) acceso a toda clase de tráfico de Internet.

Las prácticas de vigilancia reveladas por Snowden mostraron claramente que varios gobiernos, encabezados por el de Estados Unidos y secundados por los de los Cinco Ojos y posiblemente otros más estaban embarcados en un monitoreo asombrosamente masivo, detallado y a gran escala de poblaciones completas. Y que la NSA y sus socios mundiales subcontratan empresas para recolectar y minar los datos provenientes de compañías telefónicas y de Internet, entre otras. Por ejemplo, cada vez que uno se loguea en un sitio de Internet, esa información va a las agencias de inteligencia. Y los datos de geolocalización que generan los teléfonos celulares y los sitios de redes sociales, entre otros, también terminan en bases de datos de las agencias de inteligencia.

Aquí hay unas buenas infografías que ilustran y resumen el contenido de las revelaciones de Snowden. Es digno de subrayar que nueve de cada diez personas, tanto estadounidenses como de otros países, a los que la NSA espió sus comunicaciones eran simples usuarios de Internet y no personas que supusieran algún tipo de riesgo de seguridad.

Como explican Bigo, Bauman *et al.* en el artículo que ya hemos citado en el módulo 1:

Hay entonces al menos tres actores significativos en este drama: las agencias gubernamentales, las corporaciones privadas y, aunque sin siempre darse cuenta, los usuarios comunes. Lo que de cierto modo une a estos grupos es el software, los algoritmos, los códigos que permiten que los datos de los usuarios sean sistemáticamente extraídos o revelados, analizados y convertidos en lo que los recolectores de datos, y otros, como la NSA, esperan que sean datos aprovechables.

Entre los datos recolectados sistemáticamente por la NSA y sus aliados se encuentran los llamados "metadatos". Se trata de "datos acerca de los datos", como direcciones IP, identidad de cada contacto, ubicación de la comunicación y duración de la misma. Cuando Snowden reveló lo que las agencias hacían con estos metadatos, los voceros y representantes de relaciones públicas de éstas salieron rápidamente a decir que no se trataba de información privada y que, de todos modos, no era muy relevante porque no se refería al contenido mismo de los mensajes. Sin embargo, los metadatos pueden ayudar a saber cuándo alguien en particular entra a determinado lugar del mundo, por ejemplo. Y también se pueden entrecruzar datos de allegados a una persona en particular para analizar relaciones o encuentros. Esto, ciertamente, puede ser útil para detener criminales, pero no hay que forzar mucho la imaginación para pensar cómo también podría usarse en forma abusiva.

Lo que demuestra el ejemplo de los metadatos, entonces, es que no es tanto qué tipo de datos son recolectados, sino qué se hace para analizarlos, y con qué fin. Porque lo que se ve como tendencia es que los principios de presunción de inocencia o el derecho de no declarar contra uno mismo ni contra parientes cercanos, entre otros, están siendo sistemáticamente socavados por las actuales prácticas de vigilantismo.

Si hay que vigilar, que sea respetando derechos

A esta altura habrá quedado bastante claro que nuestra postura con respecto al vigilantismo es bastante crítica. Sin embargo, coincidimos con lo que dice Richard Stallman en su texto "¿Cuánta vigilancia puede soportar la democracia?", cuando dice que:

Para que el Estado pueda encontrar a los delincuentes tiene que tener la posibilidad de investigar delitos específicos, o sospechas de presuntos delitos específicos, por orden judicial. Con Internet, el poder de pinchar conversaciones telefónicas se extendería de forma natural al poder de pinchar las conexiones a Internet. Es fácil abusar de este poder por razones políticas, pero también es necesario. Afortunadamente, esto no haría posible encontrar a los denunciantes a posteriori si, como recomiendo, impedimos que los sistemas digitales acumulen información masiva a priori.

Entonces, para que las políticas de seguridad no se conviertan en abusivas, lo que hace falta es que se respeten determinados principios para garantizar todos los derechos humanos. Específicamente, en Vía Libre suscribimos los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, apoyados por 260 organizaciones de 77 países de todos los continentes, encabezadas por la Electronic Frontier Foundation. Entre los 13 principios, vale destacar:

- **Necesidad**: La vigilancia por parte del Estado debe estar limitada a la persecución de un fin legítimo.
- **Proporcionalidad**: La vigilancia en las comunicaciones debe ser vista como un acto fuertemente intrusivo y sopesada con el daño que puede causar a los derechos individuales.
- **Transparencia**: Los Estados deben ser transparentes sobre el uso y alcance de la vigilancia en comunicaciones.
- **Auditoría Pública**: Las políticas de vigilancia por parte de los Estados deben contar con mecanismos de auditoría independientes.

- **Autoridad judicial competente**: Las decisiones relacionadas con la Vigilancia de las Comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente.