Comienza la saga de Snowden

GLENN GREENWALD :: 16/05/2014

"He estado en los rincones más oscuros del Gobierno y lo que temen es la luz" :: Historia de cómo el ex-analista del régimen de EEUU se puso en contacto con periodistas

[Este artículo es una versión abreviada y adaptada del Capítulo 1 del nuevo libro de Grenn Greenwald 'No Place to Hide: Edward Snowden, the NSA, and the U.S. Security State']

El 1 de diciembre de 2012 recibí mi primera comunicación de Edward Snowden, aunque entonces no tenía la menor idea de que provenía de su persona.

El contacto llegó en forma de un correo electrónico de alguien que se llamaba Cincinato, una referencia a Lucio Quincio Cincinato, el agricultor romano que en el Siglo V a.C. fue nombrado dictador de Roma para defender la ciudad. Se le recuerda más por lo que hizo después de vencer a los enemigos de Roma: inmediata y voluntariamente renunció al poder político y volvió a la vida agrícola. Saludado como un "modelo de virtud cívica", Cincinato se ha convertido en un símbolo del uso del poder político en función del interés público y el valor de limitar o incluso renunciar al poder individual por el bien público.

El correo comenzaba diciendo: "La seguridad de las comunicaciones de la gente me resulta muy importante" y su propósito declarado era instarme a comenzar a utilizar encriptación PGP para que "Cincinato" pudiera comunicar cosas en las cuales, decía, estaba seguro de que yo estaría interesado. Inventado en 1991, PGP significa "bastante buena privacidad". Ha llegado a ser un instrumento sofisticado para proteger correos electrónicos y otras formas de comunicación en línea contra vigilancia y hackeo.

En su correo, "Cincinato" dijo que había buscado por doquier mi "clave pública" PGP, un código único que permite que la gente reciba correos electrónicos encriptados, pero no pudo encontrarla. Por ello, concluyó que yo no estaba usando el programa y me escribió, "Es poner en riesgo a cualquiera que se comunique con usted. No estoy argumentando a favor de que cada comunicación en la que esté involucrado sea encriptada, pero por lo menos debería ofrecer esa opción a los que se comunican con usted."

"Cincinato" luego se refirió al escándalo sexual del general David Petraeus, cuyo affaire extramarital con la periodista Paula Broadwell, que terminó con su carrera, fue descubierto cuando investigadores encontraron emails de Google entre los dos. Si Petraeus hubiera encriptado sus mensajes antes de entregarlos a Gmail o de almacenarlos en su archivo de borradores, escribió, los investigadores no habrían podido leerlos. "La encriptación importa, y no es solo para espías y donjuanes".

"Estarías encantado de tener noticias de gente que hay por ahí", agregó, "pero nunca podrá tomar contacto contigo sin saber que sus mensajes no pueden ser leídos en tránsito". Luego me ofreció a ayudarme a instalar el programa. Firmó: "Gracias. C."

Hace tiempo que me había propuesto utilizar software de encriptación. Había estado

escribiendo durante años sobre WikiLeaks, denunciantes, el colectivo de hackeadores conocido como Anonymous, y también me había comunicado con gente dentro del establishment de seguridad nacional de EEUU La mayoría estaba preocupada por la seguridad de sus comunicaciones e impedir monitoreo indeseado. Pero el programa es complicado, especialmente para alguien con poca pericia en programación y ordenadores, como yo. Por lo tanto era una de esas cosas que nunca había encontrado el tiempo para hacer.

El correo de C. no me llevó a la acción. Como tenía la reputación de cubrir historias que el resto de los medios pasan por alto a menudo, recibo frecuentemente mensajes de todo tipo de personas que me ofrecen una "inmensa historia", y usualmente resultan ser nada. Y todo el tiempo trabajo usualmente en más casos de los que puedo manejar. Por lo tanto necesito algo concreto para abandonar lo que estoy haciendo a fin de dedicarme a un nuevo caso.

Tres días después, volví a tener noticias de C., pidiéndome que confirmara el recibo del primer email. Esta vez respondí rápidamente. "Lo recibí y voy a ocuparme del asunto. No tengo un código PGP, y no sé cómo hacerlo, pero trataré de encontrar a alguien que pueda ayudarme".

C. respondió más tarde ese día con una guía clara, paso a paso para PGP: Encriptación para tontos, en esencia. Y al final de las instrucciones, dijo que eran solo "lo más básico". Si no podía encontrar a alguien que me ayudara a operar el sistema, agregó, "házmelo saber. Yo puedo facilitar contacto con gente que entiende criptografía en casi cualquier parte del mundo."

Ese correo terminaba con una firma más directa: "Criptográficamente suyo, Cincinato."

A pesar de mis intenciones, no hice nada, por estar consumido con otras historias, y sin estar todavía convencido de que C. tuviera algo que valiera la pena decir.

En vista de mi inacción, C. aumentó sus esfuerzos. Produjo un vídeo de 10 minutos de duración titulado PGP para Periodistas.

En ese momento C., como me dijo más adelante, se sintió frustrado. "Aquí estoy", pensó, "listo para arriesgar mi libertad, tal vez incluso mi vida, por entregar a este tipo miles de documentos de Máximo Secreto de la agencia más secreta de la nación – una filtración que producirá docenas si no cientos de inmensas sensaciones periodísticas. Y ni siquiera se molesta por instalar un programa de encriptación."

Así estuve a punto de abandonar una de las mayores y más importantes filtraciones de seguridad nacional de la historia de EEUU

"Es real"

Lo siguiente que supe del asunto fue 10 semanas más tarde. El 18 de abril, volé desde mi casa en Rio de Janeiro a Nueva York, y vi al llegar al Aeropuerto JFK que tenía un email de Laura Poitras, la documentalista. "¿Hay alguna posibilidad de que estés en EEUU la próxima semana?" escribió. "Me gustaría ponerme en contacto sobre algo, aunque lo mejor es

hacerlo en persona".

Tomo en serio cualquier mensaje de Laura Poitras. Respondí de inmediato: "En realidad, acabo de llegar a EEUU esta mañana… ¿Dónde estás?" Organizamos una reunión para el día siguiente en el lobby de mi hotel y encontramos asientos en el restaurante. Por insistencia de Laura, nos cambiamos dos veces de mesa antes de iniciar nuestra conversación para estar seguros de que nadie pudiera oírnos. Laura pasó a lo sustancial. Tenía "un asuntos extremadamente importante y delicado" que discutir, dijo, y la seguridad era esencial.

En primer lugar, sin embargo, Laura pidió que sacara la batería de mi teléfono celular o lo dejara en mi habitación en el h0otel. "Suena paranoico", dijo, pero el gobierno tiene la capacidad de activar teléfonos celulares y laptops remotamente como dispositivos de escucha. Yo había oído eso de activistas por la transparencia y hackeadores pero tendía a considerarlo como una precaución exagerada. Después de descubrir que era imposible sacar la batería de mi teléfono celular, lo llevé de vuelta a mi habitación, luego volví al restaurante.

Laura comenzó a hablar. Había recibido una serie de correos electrónicos anónimos de alguien que parecía honesto y serio. Afirmaba que tenía acceso a algunos documentos extremadamente secretos e incriminadores sobre espionaje del gobierno de EEUU contra sus propios ciudadanos y el resto del mundo. Estaba determinado a filtrar esos documentos a ella y había solicitado específicamente que trabajara conmigo en la publicación e información sobre ellos.

A continuación Laura sacó varias páginas de su cartera provenientes de dos de los correos enviados por el filtrador anónimo, y los leí en la mesa de principio a fin. En el segundo correo, el filtrador llegó al punto crucial de lo que consideraba como su misión:

El choque de este período inicial [después de las primeras revelaciones] proveerá el apoyo necesario para construir un Internet más equitativo, pero esto no resultará ventajoso para la persona promedio a menos que la ciencia sobrepase a la ley. Al comprender los mecanismos mediante los cuales nuestra privacidad es violada, podemos triunfar en este caso. Podemos garantizar a todos igual protección contra una búsqueda irracional mediante leyes universales, pero solo si la comunidad técnica está dispuesta a enfrentar la amenaza y a comprometerse a implementar soluciones demasiado complejas. Finalmente, debemos imponer un principio mediante el cual la única manera cómo los poderosos pueden gozar a de privacidad sea cuando sea de la misma clase compartida por los de a pie: una privacidad impuesta por las leyes de la naturaleza, en lugar de las políticas del hombre.

"Es real", dije cuando terminé de leer. "No puedo explicar exactamente por qué, pero siento intuitivamente que esto es serio, que es exactamente quien dice que es".

"Lo mismo siento yo", respondió Laura. "Tengo muy pocas dudas".

Instintivamente reconocí la pasión política del autor. Sentí una afinidad con nuestro corresponsal, con su visión del mundo, y con el sentido de urgencia que evidentemente lo consumía.

En uno de los últimos pasajes, el corresponsal de Laura escribió que estaba completando los últimos pasos necesarios para suministrarnos los documentos. Necesitaba otras cuatro o seis semanas, y debíamos esperar noticias suyas.

Tres días después, Laura y yo volvimos a reunirnos, y con otro correo del filtrador anónimo, en el cual explicaba por qué estaba dispuesto a arriesgar su libertad, a someterse a la gran probabilidad de una condena a prisión muy prolongada, a fin de revelar esos documentos. Ahora yo estaba aún más convencido: nuestra fuente era real, pero como dije a mi asociado, David Miranda, en el vuelo a casa a Brasil, estaba determinado a olvidar todo el asunto. "Podría no suceder. Podría cambiar de opinión. Podría ser atrapado." David es una persona de poderosa intuición, y estaba extrañamente seguro. "Es real. Es real. Va a suceder", declaró. "Y va a ser inmenso".

"Tengo solo un temor"

Un mensaje de Laura me dijo que teníamos que hablar urgentemente, pero solo mediante chat OTR (off-the-record), un instrumento encriptado para hablar con seguridad en línea.

Su noticia fue asombrosa: podríamos tener que viajar de inmediato a Hong Kong para encontrar a nuestra fuente. Yo había supuesto que nuestra fuente anónima se encontraba en Maryland o el norte de Virginia. ¿Qué hacía en Hong Kong alguien con acceso a documentos de máximo secreto del gobierno de EEUU? ¿Qué tenía que ver Hong Kong con todo esto?

Las respuestas solo podían provenir de la propia fuente. Estaba molesto por el ritmo de las cosas hasta entonces, y era crítico que hablara con él directamente, que lo tranquilizara y aquietara sus crecientes preocupaciones. Dentro de una hora, recibí un correo de Verax@******. Verax significa "quien dice la verdad" en latín. El asunto decía, "Necesito hablar".

"He estado trabajando en un proyecto importante con un amigo mutuo nuestro" comenzaba el correo. "Usted tuvo que negarse a viajar a corto plazo para encontrarse conmigo. Tiene que involucrarse en esta historia", escribí. "¿Hay alguna manera para que podamos hablar dentro de poco? Comprendo que usted no tiene gran cosa como infraestructura segura, pero me las arreglaré con lo que tenga." Sugirió que habláramos vía OTR y suministró su nombre de usuario.

Mi ordenador repicaba como una campana, indicando que la fuente había contestado. Ligeramente nervioso, hice clic en su nombre y escribí "hola". Respondí y me vi hablando directamente con alguien que yo asumía que, en ese momento, había revelado una serie de documentos secretos sobre programas de vigilancia de EEUU y que quería revelar más.

"Estoy dispuesto a hacer lo necesario para informar sobre esto", dije. La fuente –cuyo nombre, sitio de empleo, edad, y todos los demás atributos me seguían siendo desconocidos– preguntó si iría a Hong Kong a encontrarlo. No pregunté por qué estaba allí; no quería parecer que estuviera en pesca de información y supuse que su situación era delicada. Cualquier cosa que fuera verdad, sabía que esa persona había resuelto realizar lo que el gobierno de EEUU consideraría un crimen muy serio.

“Desde luego iré a Hong Kong”, dije.

Hablamos en línea ese día durante dos horas, discutiendo en detalle su objetivo. Yo sabía por los correos que Laura me había mostrado que se sentía obligado a revelar al mundo el masivo aparato de espionaje que el gobierno de EEUU estaba construyendo en secreto. ¿Pero qué esperaba lograr?

“Quiero provocar un debate mundial sobre la privacidad, la libertad en Internet, y los peligros de la vigilancia estatal”, dijo. “No temo lo que me pueda suceder. He aceptado que probablemente mi vida se acabará por hacer esto. En ese sentido estoy tranquilo. Sé que estoy haciendo lo correcto.” Luego dijo algo sorprendente: “Quiero identificarme como la persona detrás de estas revelaciones. Creo que tengo la obligación de explicar porqué estoy haciendo esto y lo que espero lograr.” Me dijo que había escrito un documento que quería colocar en Internet cuando se revelara como la fuente, un manifiesto pro privacidad, contra la vigilancia para que la gente en todo el mundo lo firmara, mostrando que existe apoyo global para la protección de la privacidad.

“Solo tengo un temor al hacer todo esto”, dijo, que es “que la gente vea estos documentos, y se encoja de hombros, que diga, ‘Suponíamos que esto estaba ocurriendo y no nos importa’. Lo único que me preocupa es que hago todo esto a mi vida para nada.”

“Dudo seriamente que eso suceda”, le aseguré, pero no estaba convencido de que realmente yo lo creyera. Sabía por mis años de escribir sobre abusos de la NSA que puede ser difícil generar una preocupación seria por la vigilancia secreta del Estado.

Esto parecía diferente, pero antes de partir a Hong Kong, yo quería ver algunos documentos para comprender el tipo de revelaciones que la fuente estaba dispuesta a hacer.

Entonces pasé un par de días en línea mientras la fuente me mostraba, paso a paso, cómo instalar y utilizar los programas que necesitaría para ver los documentos.

Pedía disculpas continuamente por mi falta de habilidad técnica, por tener que ocupar horas de su tiempo para enseñarme los aspectos más básicos de comunicación segura. “No te preocupes”, dijo, “la mayor parte de esto tiene poco sentido. Y ahora mismo dispongo de mucho tiempo libre.”

Una vez que los programas estuvieron todos instalados, recibí un archivo que contenía aproximadamente veinticinco documentos: “Solo una pequeña prueba: la punta de la punta del iceberg”, explicó tentadoramente.

Descomprimí el archivo, vi la lista de documentos, e hice clic al azar en uno de ellos. En la parte superior de la página apareció en letras rojas, un código: “TOP SECRET/COMINT/NO FORN/.”

Esto significaba que el documento había sido legalmente calificado de máximo secreto, que pertenecía a inteligencia de comunicaciones (COMINT), y que no estaba destinado a distribución a nacionales extranjeros, incluyendo organizaciones internacionales o socios de una coalición (NO FORN). Ahí estaba con claridad incontrovertible: una comunicación

altamente confidencial de la NSA, una de las agencias más secretas del gobierno más poderoso del mundo. Nunca algo de significación semejante había sido filtrado de la NSA, no en la historia de seis décadas de la agencia. Ahora tenía en mi poder un par de docenas de ítems semejantes. Y la persona con la que había pasado horas chateando durante los últimos dos días tenía muchos, muchos más para darme.

Cuando Laura y yo llegábamos al Aeropuerto JFK para tomar un vuelo de Cathay Pacific a Hong Kong, Laura sacó un dispositivo USB de su mochila. "¿Adivina lo que es esto?" preguntó con una mirada de intensa seriedad.

"¿Qué?"

"Los documentos" dijo. "Todos".

"Léeme primero"

Durante las siguientes 16 horas, a pesar de mi agotamiento, no hice nada fuera de leer, tomando febrilmente notas de un documento tras el otro. Uno de los primeros que leí era una orden del tribunal secreto de la Ley de Vigilancia de Inteligencia Extranjera (FISA, por su sigla en inglés), que había sido creado por el Congreso en 1978, después que el Comité Church descubrió décadas de escuchas telefónicas abusivas del gobierno. La idea tras su formación era que el gobierno podía seguirse involucrando en vigilancia electrónica, pero para impedir abusos semejantes, tenía que obtener permiso del tribunal FISA antes de hacerlo. Yo nunca antes había visto una orden judicial FISA. Casi nadie había visto alguna. El tribunal es una de las instituciones más secretas del gobierno. Y todos sus dictámenes son automáticamente designados como máximo secreto, y solo un pequeño grupo de personas tiene autorización para acceder a sus decisiones.

El dictamen que leí en el avión a Hong Kong era fascinante por diversas razones. Ordenaba a Verizon Business que entregara a la NSA "todos los registros en detalle" de comunicaciones (i) entre EEUU y el exterior; y (ii) enteramente dentro de EEUU, incluyendo llamados telefónicos locales. Eso significaba que la NSA estaba recolectando secreta e indiscriminadamente los registros telefónicos de decenas de millones de estadounidenses, por lo menos. Virtualmente nadie tenía la menor idea de que la administración de Obama estuviera haciendo algo semejante. Ahora, con este dictamen, yo no solo sabía del asunto sino tenía la orden del tribunal secreto como prueba.

Solo entonces sentí que estaba comenzando a procesar la verdadera magnitud de la filtración. Había estado escribiendo durante años sobre la amenaza planteada por la vigilancia interior ilimitada; mi primer libro, publicado en 2006, advertía de la ilegalidad y radicalismo de la NSA. Pero yo había luchado contra el gran muro de secreto que protegía el espionaje gubernamental: ¿Cómo se documentan las acciones de una agencia tan completamente oculta en múltiples capas de secreto oficial? En ese momento, el muro había sido roto. Tenía en mi posesión documentos que el gobierno había tratado desesperadamente de ocultar. Tenía evidencia que probaría indisputablemente todo lo que el gobierno había hecho para destruir la privacidad de estadounidenses y de gente en todo el mundo.

En 16 horas de lectura apenas interrumpida, logré revisar solo una pequeña fracción del archivo. Pero cuando el avión aterrizó en Hong Kong, sabía dos cosas con seguridad. Primero, la fuente era altamente sofisticada y políticamente astuta, evidente en su reconocimiento de la significación de la mayoría de los documentos. También era altamente racional. La manera cómo escogió, analizó y describió los miles de documentos que ahora tenía en mi posesión lo probaba. Segundo, sería muy difícil negar su condición como denunciante clásico. Si la revelación de pruebas de que funcionarios de máximo nivel de la seguridad nacional mintieron de manera absoluta al Congreso sobre programas internos de espionaje no convierte a alguien indisputablemente en denunciante, ¿qué lo convierte?

Poco antes del aterrizaje, leí un último archivo. Aunque estaba titulado "LÉAME PRIMERO", lo vi por primera vez solo al final del vuelo. Este mensaje era una explicación de la fuente de porqué había decidido hacer lo que hizo y qué esperaba que sucediera como resultado – e incluía un hecho que los otros no mencionaban: el nombre de la fuente.

"Comprendo, que se me hará sufrir por mis acciones, y que la entrega de esta información al público marca mi fin. Estaré satisfecho si la federación de ley secreta, perdón desigual, e irresistibles poderes ejecutivos que rigen el mundo que amo son revelados aunque sea por un instante. Si queréis ayudar, uníos a la comunidad de la fuente abierta y luchad por mantener vivo el espíritu de la prensa y el Internet libre. He estado en los rincones más oscuros del gobierno, y lo que temen es la luz.

Edward Joseph Snowden, SSN: *****

CIA Alias "***** "

Número de identificación de la Agencia: *****

Exconsejero sénior | Agencia de Seguridad Nacional de EEUU, bajo cobertura corporativa.

Exoficial de campo | Agencia de Seguridad Nacional de EEUU, bajo cobertura diplomática.

Excatedrático | Agencia de Inteligencia de la Defensa de EEUU, bajo cobertura corporativa."

TomDispatch. Traducido del inglés para Rebelión por Germán Leyens

---

https://www.lahaine.org/mundo.php/comienza-la-saga-de-snowden