Los Espiones (…y II)
Entre la Libertad y la Vigilancia

Quien trueca la libertad por la seguridad
no merece ni la libertad ni la seguridad

BENJAMIN FRANKLIN

DOS AÑOS han transcurrido desde que Edward J. Snowden, ex empleado de *CIA* y *NSA* hoy refugiado en Rusia, revelara al *Washington Post,* al *Guardian* y a *Channel 4,* por corajudo escrúpulo de conciencia, la existencia en el seno de la *NSA* de *Prism, XKeyscore* y otros numerosos programas de un colosal y refinado sistema de espionaje y *malware* globales, de esencia comunicacional, celosamente manejado por los *Five Eyes,* los poderosos y sigilosos servicios secretos confederados de los cinco países wasp *(white anglo-saxon protestant):* Australia, Canadá, Estados Unidos, Nueva Zelanda y Reino Unido encabezados por la *NSA* norteamericana y el *GCHQ* inglés, con un generoso memorando de entendimientos que les permite ceder datos a Israel.

Dos años densos que justifican un primer balance bonus-malus de los adelantos y retrocesos en materia de espionaje, seguridad, derechos humanos y privacidad (un concepto, este último, en el que Marc Zuckerberg de *Facebook* acaba de declarar que ya no cree), en la medida en que de "balance" pueda hablarse tratándose de procesos en acelerada evolución conceptual, política y tecnológica. Adelantemos de una vez nuestra conclusión: pese a algunos avances de fachada en el campo de los derechos humanos, más nominales y ataráxicos que reales, ciertas libertades y la privacidad del género humano están en sus estertores finales, la vigilancia y espionaje masivos en indetenible expansión. Un pesimismo razonado y no ocasional, coherente con la presente coyuntura histórica que ve enquistarse en el *modus vivendi* de la humanidad una fuerte y particularmente cruel componente terrorista generadora de una panoplia de refinados e iliberales antídotos (panoplia a la que George W. Bush acordó subvenciones por 130 millardos de dólares anuales), un repunte de ingredientes de Guerra Fría y hasta la reaparición más o menos latente de las mega-confrontaciones, si es que tienen algún sentido los cohetes balísticos intercontinentales de última generación recién presentados al mundo por Putin, contra cuya velocidad de caída de 20.000km/hora nada podrán, por ahora, la cohetería antibalística tipo *Patriot* y demás armas de la "guerra de las galaxias".

Se trata de la segunda parte del ensayo* Espiones *que fuera publicado en el anterior número de la revista (ver revista* Comunicación *Nº 170, segundo trimestre 2015). En ese primer trabajo el autor nos plantea que los insólitos casos de Assange y Snowden, de* WikiLeaks *y* Prism*, obligan a una consideración antropológica-social: la cibernetización del espionaje ha dado al traste con la apasionante figura del viejo individuo-espía, reemplazado hoy por ejércitos de anónimos burócratas del espionaje. Esta nueva entrega nos va paseando por varios casos en donde la libertad y la privacidad están en juego. Al final el texto nos dice que "Hemos constatado que la sedicente necesidad de vigilar mucho para impedir el mal se ha convertido en uno de los más temibles atentados a nuestras libertades y privacidad tan penosamente conquistadas".

This is about the second part of the essay "Espiones" that was published in the last issue of the magazine (see* Communication *N° 170, second trimester 2015). In this first job the author explains to us that the unbelievable cases of Assange and Snowden, WikiLeaks and Prism, require an anthropological-social consideration: the cybernetization of espionage has defeated the thrilling figure of the old individual-spy, replacing it now for army of faceless bureaucrats of espionage. This new entry walks us through various cases where freedom and privacy are in stake. At the end of this text it says "We have found that the self-styled need to monitor to prevent much evil has become one of the most fearsome attacks on our freedoms and privacy so painfully conquered"

● **ANTONIO PASQUALI**

Edward Joseph Snowden, norteamericano, 32 años, ex empleado de CIA y NSA, actualmente refugiado en Rusia, en junio 2013 reveló al mundo la existencia de un sistema mundial de vigilancia electrónica en el seno de la NSA y el funcionamiento de *Prism* y *XKeyscore*. Es partidario del anonimato en Internet vía el programa *TOR*. La justicia de su país lo considera responsable de un "asunto criminal". En sus primeras declaracions al *Guardian* dijo: "estoy listo a sacrificarlo todo porque, en mi alma y conciencia, no puedo permitir que el gobierno americano destruya la vida privada, la libertad de Internet y otras libertades esenciales…con ese enorme sistema de monitoreo que está montando secretamente"

EL *BONUS*

Lo más resaltante en el capítulo *bonus* del expediente espionaje es sin duda la aprobación por el Senado norteamericano, el 2 de junio pasado con firma presidencial el mismo día, del *Usa Freedom Act,* una ley que limita el espionaje de la NSA a los metadata de todas las comunicaciones telefónicas norteamericanas bajo ciertas condiciones; una hermosa victoria de la *American Civil Liberties Union* contra el *Patriot Act* aprobado por la administración Bush después del 11.09 (véase en Wikipedia: *Patriot Act, Section* 215), iniciativa que en diciembre 2014 corriera el riesgo de empantanarse por falta de votos suficientes en el Senado. Una de las bases de esa victoria fue una sentencia de casi cien páginas del Tribunal Federal de Apelaciones de Nueva York, que juzgó el *Patriot Act* como "una contracción de la privacidad sin precedentes" constatando que "pese a las exigencias de seguridad, no hay evidencia de ningún debate público sobre la materia". Esa ley fue saludada por el mundo entero como una gran batalla ganada por las libertades civiles contra el control y el espionaje sistemáticos de enteras sociedades. En los hechos, muchos detalles parecieran indicar que estamos ante una victoria pírrica inteligentemente piloteada para calmar la opinión pública y dejar inalterados los tremebundos mecanismos de espionaje instalados. A Snowden lo asisten desde luego verdades fácticas, como la caída del imperio soviético o las torres gemelas del 11.09 que nadie supo prever, cuando proclama (lo dijo en diferido el pasado abril ante un congreso de Periodistas en Perugia, ver *infra)* que mucho espionaje podía eliminarse porque "el monitoreo de la entera humanidad es completamente ineficaz"; pero ¿qué jefe de Estado se atrevería hoy a desmantelar o reducir siquiera sus propios servicios de inteligencia, a correr el riesgo de ser enjuiciado por desactivar defensas vitales del país? Lo cierto es que Ned Price, portavoz de la Casa Blanca, tras reconocer en mayo pasado que la colecta directa de metadata por la NSA conforme a la sección 215 del *Patriot Act* debía cesar, declaró "hay que crear un mecanismo alternativo aun manteniendo los rasgos esenciales de aquel programa". "Aun manteniendo los rasgos esenciales de aquel programa" ¿entendido? Dicho y hecho: el *Usa Freedom Act* pide a las compañías telefónicas y servidores electrónicos de no remitir más automáticamente los metadata a la NSA u otras agencias gubernamentales, de seguir recolectándolos y almacenándolos, y de enviarlos a las centrales de espionaje solo tras explícita solicitud gubernamental aprobada por el Tribunal de Control de la Inteligencia Extranjera en los Estados Unidos. ¡Una clásica decisión gatopardesca: solo un trámite burocrático más para que todo siga igual! Esto, sin olvidar que a cualquiera de esas agencias siempre le queda la posibilidad de cortocircuitar la nueva ley solicitando a otra agencia amiga de la confraternidad *Five Eyes* el monitoreo de ciudadanos norteamericanos.

El segundo capítulo del *bonus* lo pudiera ocupar otra batalla aparentemente exitosa también conducida en territorio norteamericano por la administración Obama: una Corte de Apelaciones del distrito de Columbia opuso el pasado 12 de junio un rotundo "no" al Internet de dos velocidades –una para ricos, la otra para pobres– y un rotundo "sí" a la llamada neutralidad de la red y a la banda ancha como *public utility* disfrutable por la totalidad de la población. Este juicio vino a sellar la decisión adoptada el 26.02 por la *Federal Communication Commission FCC,* de garantizar idéntico acceso a la red a todos sin distinción y sin tarifas diferenciadas, haciendo del Internet de alta velocidad un verdadero Servicio Público como el agua o la electricidad. En esa ocasión el presidente de la FCC, Tom Wheleer, pronunció una frase histórica: "Internet es el último instrumento de la libertad de expresión, algo demasiado importante para permitir a los proveedores de acceso a la alta velocidad que establezcan las reglas". Otra batalla y otra jurisprudencia americano-americana de interés universal, pues así como todos los datos de origen Echelon o NSA confluyen en los Estados Unidos, casi del mismo modo está configurada la red Internet, el 85 % de cuyos flujos transitan por Norteamérica (véase artículo anterior), lo que hace que un estornudo norteamericano en espionaje e Internet produzca gripe en el espionaje y el Internet del resto de la humanidad.

El sano principio queda establecido; resta por ver el rumbo que tomarán las cosas en los meses venideros. El lobby de las telecoms, reunidas en la *National Cable &Telecom Association,* anuncia que apelará la norma y desconocerá la autoridad de la FCC en la materia. Google y Facebook están realizando en este momento grandes inversiones en sistemas para cubrir con señal de Internet zonas remotas del mundo donde viven los 2/3 de la humanidad que no la reciben (por satélites *leo,* globos lanzados a la estratósfera o aviones movidos por fotovoltaico capaces de dar vueltas en el aire hasta por cinco años), y ya han indicado a las claras que entienden cubrir dichas regiones con una señal de segunda, como ya es el caso de uno de los primeros experimentos del género, el de Colombia, donde Facebook distribuye una farsa de Internet gratuita que solo recibe…Facebook y otras once opciones. Otro punto a seguir con mucha atención.

La tercera evidencia de un *bonus,* esta vez un gran estímulo a convertir en virtuoso hábito político el llamado "gobierno abierto" que asegure una democrática difusión pública de informaciones generadas o manejadas por gobiernos, se desprende de la noticia siguiente: para abril de 2015 ya pasaban de noventa las democracias del mundo que han incorporado a su propia legislación normas que facilitan y regulan el libre acceso a la información pública. Dichas normas son genéricamente conocidas bajo el nombre de FOIA por *Freedom of Information Act,* en homenaje al primer país que se dotó de leyes de ese tipo en el lejano 1967, para variar… los EE.UU. Esas normas establecen que un ciudadano puede pedir y obtener informaciones en poder de la administración pública, con ámbitos vetados que en aquel momento se fijaron así: seguridad nacional, reglas internas de la administración pública, de divulgación negada por otras leyes federales, secretos comerciales, secretos profesionales (como patentes), invasión de otras privacidades, instituciones financieras, atentatorias al orden público e informaciones geológicas; excepciones que poco han variado en estos decenios en los diferentes países. En legislaciones más recientes ya no es el ciudadano quien debe aclarar a la administración pública las razones de su pedido de información, sino la administración pública la que debe precisar al ciudadano la norma jurídica que le impide proporcionársela.

Sede del *Government Communication Headquarter GCHQ* inglés en Chentelham, inaugurada en 2003, principalmente dedicado a la inteligencia de señales SIGINT. Cuenta con unos 5.000 empleados. En 2011, en el marco de su proyecto *Tempora,* afinó e hizo operacional una tecnología capaz de succionar la mensajería que transita por cables de fibra óptica. Inglaterra es el país de Alan Turing, el matemático y criptógrafo que durante la Segunda Guerra Mundial logró descifrar *Enigma,* el sistema ultrasecreto nazi de comunicaciones militares.

“En legislaciones más recientes ya no es el ciudadano quien debe aclarar a la administración pública las razones de su pedido de información, sino la administración pública la que debe precisar al ciudadano la norma jurídica que le impide proporcionársela.

El del acceso difícil o imposible a informaciones de fuente pública, y hasta denegadas sistemáticamente a comunicadores y solicitantes de la oposición, es uno de los aspectos más invalidantes y antidemocráticos de la presente coyuntura comunicacional venezolana, signada por una opacidad y un “secretismo” propios de mentalidades militares y castristas. En 2011/12 una Coalición nacional *ProAcceso* sometió al Legislativo un ponderoso *Proyecto de Ley Orgánica para la Transparencia y el Acceso a la Información Pública* (www.proacceso.org.ve) que el régimen militarista obviamente archivó, y se conocen sentencias del Tribunal Supremo de Justicia denegatorias de solicitudes ciudadanas de información, como las 01177 y 01736 de 2014, francamente inverecundas. Véase por ejemplo este antológico fragmento de la primera, en respuesta a una solicitud de información de 4 ONG sobre irregularidades en compra de medicamentos a Cuba : “(…) peticiones como las de autos, donde se pretende recabar información sobre la actividad que ejecuta o va a ejecutar el Estado para el logro de uno de sus fines, esto es, la obtención de medicinas en pro de garantizar la salud de la población, atenta contra la eficacia y eficiencia que debe imperar en el ejercicio de la Administración” (ver Torrealba: http://saber.ucv.ve/jspui/handle/123456789/10229). Hasta un cambio de gobierno no habrá pues FOIA venezolana pese a que Naciones Unidas, en su reporte del 19.06.2015 (véase http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=EC.12%20VEN%20CO%203&Lang=en) urge a Venezuela darse “una ley que garantice el acceso a la información y la transparencia de la administración pública”. En América Latina, Antigua y Barbuda, Belice, Colombia, Chile, Ecuador, Guatemala, Jamaica, México, Nicaragua, Panamá, Perú, República Dominicana y Trinidad y Tobago ya tienen la propia, y en casi todas ellas el solicitante de información al gobierno está exento de la obligación de exponer razones que legitimen su demanda.

Off the record, una última buena noticia menor: la combativa *Electronic Frontier Foundation* de San Francisco que lucha en favor de la privacidad y contra la vigilancia masiva indiscriminada logró en febrero del pasado año, en unión de organizaciones similares, hacer del 11 de febrero de cada año el Día Mundial en Defensa de la Privacidad y, más importante aún, obtuvo en mayo el consenso de 360 asociaciones similares de 60 países para unos *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* (versión española en https://es.necessaryandproportionate.org/text)

Edward Snowden (véase http://prodavinci.com/2015/06/17/vivir/como-han-cambiado-el-mundo-y-las-comunicaciones-despues-de-edward-snowden-monitorprodavinci/) es optimista por las siete razones siguientes: ahora sabemos más lo que hacen los gobiernos, nació una oposición a la vigilancia masiva, hay tribunales que reconocen irregularidades, se crean más programas para proteger la privacidad, ciertos OIG estiman que la vigilancia masiva es una amenaza, algunas empresas se enfrentan a gobiernos, hay más regulaciones sobre vigilancia masiva. Nosotros, lamentablemente, lo somos un poco menos, como veremos.

EL *MALUS*

Nuestro breve repaso anterior del *bonus* ha revelado un exceso de incertidumbres, conflictos ideales-realidad, victorias pírricas y lagunas, y no sería exagerar de pesimismo enunciar la hipótesis que ese *pot-pourri* de las hazañas de Assange y Snowden, las presiones de organizaciones civiles, el repunte de la Guerra Fría y la dramática recrudescencia del terrorismo tipo masacre de *Charlie Hebdo,* han finalmente obrado de consuno para fortalecer más bien, y en todas partes, el principio de la seguridad y la necesidad de sistemas de espionaje masivo, volviéndolos aún más sigilosos, eficientes e invisibles.

Desde 1972 y luego en 1979, 1982, 1987, 1990-91, 2002 y 2010, las dos superpotencias negociaron su común propósito de desmantelar parcialmente su arsenal nuclear hasta un mínimo de 1.500 cabezas cada país, y pese a muchos vaivenes y cambios de visión estratégica global (como *Salt I* y *Salt II)* sí cumplieron con las reducciones, logrando hasta suscribir en 1997 una Convención sobre Armas Químicas (a la que se adhirieron prácticamente todos los países de la Tierra) que dio vida a una organización de Naciones Unidas, la OPAQ, encargada de realizar y supervisar el desarme químico universal.

Nada de similar, absolutamente nada, se vislumbra siquiera para actividades de espionaje. Solo se sabe de adelantos tecnológicos y estratégicos de la industria y políticas de vigilancia; se nos previene, por ejemplo, que para 2020 habrá en los Estados Unidos unos 30.000 drones perennemente en el aire monitoreando el país, o que el *Prism* de la NSA, ya en obsolescencia, es progresivamente remplazado por *Xkeyscore,* un nuevo programa que permite al investigador-espía ingresar con enorme facilidad y sin autorización legal al uso que la persona investigada está haciendo de Facebook, Google, Apple, Microsoft, Yahoo, Youtube, Skype, e-mails, cronología del *browser* y *chats online.* El robo de toda esa información es realizado por 700 equipos hackeadores instalados en 150 lugares del mundo, cuatro de ellos en Colombia, Ecuador, México y Venezuela (ver en Google las primeras ocho entradas a *Xkeyscore).* También se ha informado que la NSA viene invirtiendo 80 millones de dólares en un proyecto de largo aliento y suerte de arma definitiva, *Penetrating Hard Targets* (ver https://www.washingtonpost.com/apps/g/page/world/a-description-of-the-penetrating-hard-targets-project/691/#document/p1/a138758): una computadora cuántica que se estaría montando en una jaula de Faraday en College Park (Maryland) con una potencia de cálculo exponencialmente más elevada que las binarias, la cual sería finalmente capaz de descifrar todos los códigos de enciframiento habidos y por haber, y de proteger radicalmente los propios de cualquier intento de intrusión.

El multi-premiado experto en estas materias Shane Harris, recientemente entrevistado por Moisés Naím, asegura que el sistema mi-

> **El dígito binario y la electrónica han vuelto al hombre y su mundo en exceso transparentes porque todo lo que cuenta es hoy un dato, un manojo de bits finalmente mal protegido. Un maná para espiones.**

litar mundial está incorporando a sus arsenales un quinto dominio, el de Internet, lo que hará que el sector privado y los hackers sean co-protagonistas de las próximas ciberguerras, un modelo de guerra al que se estarían preparando hoy unos sesenta países. En febrero del pasado año, irritado por las revelaciones de Snowden, el gobierno de Angela Merkel ordenó a la *Bundesnachtrichtendienst BND,* su servicio de espionaje internacional, de "espiar a todo el mundo" incluyendo gobiernos aliados; desde abril, tras los ataques terroristas de Volgograd, una ley rusa obliga a los server a guardar en territorio ruso el registro de todas las comunicaciones cursadas y asimila los *bloggers* con más de 3.000 seguidores, a todos los efectos legales, a los propietarios responsables de periódicos. Poco después, en junio, una acción judicial intentada por *Privacy International* contra el CGHQ reveló que la inteligencia inglesa sí espía a sus propios ciudadanos usuarios de Google o Facebook a cuenta de que estas son "conexiones externas"; esto, sin olvidar que ya Snowden había declarado al *Guardian* que los hombres de la inteligencia inglesa "eran peores que los de la NSA" gracias sobre todo a su refinado Programa *Tempora* (ver *Tempora* en Google) –considerado "la joya de la corona" por haber hecho del CGHQ "una superpotencia del espionaje"– pues había perfeccionado la tecnología capaz de succionar los datos que transitan por cables de fibra óptica, 200 de los cuales tienen "pinchados" con la colaboración de las telecom locales, lo que les permite enterarse *inter alia* del contenido de unos 600 millones de llamadas diarias cuyo conocimiento comparten con NSA (la Comunidad Europea pidió al Reino Unido explicaciones, insatisfechas, sobre este caso). Organizaciones internacionales de derechos humanos vienen denunciando un Proyecto de Ley pakistaní *Prevention of Electronic Crimes Bill* que atentaría contra libertades fundamentales; el pasado 12 de mayo, bajo el impacto de la masacre de *Charlie Hebdo,* la Asamblea francesa aprobó por 438 votos contra 86, una *Loi sur le Renseignement* que legaliza la recolección masiva de metadata e instalación de sistemas de monitoreo electrónico de comunicaciones sin mandato de jueces, con tan solo un permiso presidencial y de dos delegados. A los pocos días, bajo el impacto del asesinato en sus predios de un soldado por un terrorista, el Parlamento Canadiense votó una Ley Antiterrorista que amplía considerablemente los poderes de sus servicios de inteligencia habilitándolos para "perturbar" mensajería electrónica supuestamente terrorista y espiar cualquier ciudadano sospechoso, y se anuncia que en los Países Bajos y Suiza se están elaborando análogas legitimaciones para un poder casi ilimitado de espiar. En precedencia, hace un año, el Senado norteamericano había finalmente aprobado (tras intentos fallidos en 2012 y 2013) el *Cybersecurity Information Sharing Act CISA,* que facilita la transferencia al gobierno de informaciones privadas en nombre de la ciber-seguridad. Los servicios de inteligencia del mundo entero, hostigando con armas impares a los defensores de una Internet libre y anónima, tratan por todos los medios de impedir el uso, por parte de instituciones y privados, de sistemas antivigilancia tipo *Tor* que ofrecen anonimato, alegando que sus usuarios son principalmente criminales. Así que *mala tempora currunt,* diría Cicerón, para las libertades civiles de la humanidad.

Lo que sigue es un importante subcapítulo del *malus* que no tratamos en la ocasión anterior, el que tiene de protagonistas a los *hackers*. Una manera muy esclarecedora de retomarle el pulso a las dimensiones colosales, capilares y desconsideradas de ese inmenso campo de Agramante que han llegado a ser las actividades de espionaje, vigilancia y monitoreo electrónico de todos hacia todos.

LOS INVASORES MALINTENCIONADOS O *"BLACK HAT HACKERS"*

Es el sector de la artesanía refinada y puntual en el universo del espionaje. Pese a los siempre más sofisticados sistemas de protección instalados en bancos de datos, programas y mensajería (casi siempre ineficaces –declaran a veces con desparpajo sus propios fabricantes– porque los violadores de programas los perforan al poco tiempo), la superestructura electrónica o ciberesfera que ya recubre toda actividad humana relevante sigue siendo pavorosamente vulnerable, y muchos se preguntan a veces con temor y temblor, para el caso nacional, qué tan bien protegidos estarán de ataques informáticos la represa del Guri (la tercera más grande del mundo) y la distribución eléctrica, las grandes refinerías o los principales acueductos del país. ¡Esperemos que sí, con el beneficio de la duda! Pero cuando se lee en *Le Monde* del 7.02.2014 que hasta Francia, un país con 58 centrales nucleares y la tercera fuerza atómica de disuasión más grande de la Tierra, comienza apenas a estudiar una ley "para poner a seguro nuestros operadores vitales, esas empresas y centros de poder sin los cuales se paralizaría el país", un frío glacial vuelve a bajar por la espalda.

El dígito binario y la electrónica han vuelto al hombre y su mundo en exceso transparentes porque todo lo que cuenta es hoy un dato, un manojo de bits finalmente mal protegido. Un maná para espiones. En artículo anterior recordábamos la definición de "espionaje" del documento *A5-264/2001* que la Comunidad europea consagró en 2001 al caso Echelon: "robo organizado de información", uno de los posibles corolarios del axioma general *Información es Poder,* y robar bits es infinitamente más fácil que violar la *Enigma* nazi. Dicho robo, casi totalmente efectuado hoy con y contra medios electrónicos, es llevado a cabo masivamente, a escala mundial, por conglomerados del espionaje tan enormes como la NSA o el CGHQ (creadores justamente del primer sistema global, el Echelon), o más artesanalmente si se quiere, por empresas o lobos solitarios especializados en perforar barreras protectoras e invadir predios ajenos, genéricamente conocidos como *hackers*.

No todos saben, empero, que la de los *hackers* es una multifacética familia que va de arcángeles a demonios; por un lado, organizaciones difusas como *Anonymous*, uno de los grupos *hackers* más grandes del mundo, que defienden en Occidente la libertad de Internet y de expresión, o los profesionales bienintencionados y voluntariosos llamados "sombreros blancos" que descubren analizan y corrigen debilidades de sistemas, redes y protecciones, diplomados en escuelas especializadas, con vocabulario propio (el *Jargon File)*, publicaciones propias (por ej. *The Intercept)* y hasta apologetas (como Steven Levy), y por el otro el invasor malicioso, delincuente, extorsionador o agente de empresas en competición o de desafiantes gobiernos, los "som-

Sede de la *National Security Agency NSA* norteamericana en Fort Meade, Maryland, una dependencia del Departamento de Defensa creada en secreto en 1952, rodeada de 18.000 puestos de estacionamiento. Maneja un presupuesto de 52,6 millardos de dólares anuales y se le calculan unos 50.000 empleados. Wikipedia (véase) señala que sus instalaciones son las mayores consumidoras de electricidad de Maryland.

Vista de un sector de las memorias de la NSA en Bluffdale, Utah.

Una supercomputadora *Cray Titan* de 24,8 *PetaFlops* como las instaladas en el *datacenter* de la NSA.

Las unidades de enfriamiento de computadora y memorias de NSA en Bluffdale, Utah, consumen 6 millones de litros diarios de agua.

LA POTENCIA TECNOLÓGICA DE LA NSA

Para leer más cómodamente la nota explicativa del presente cuadro, conviene recordar la nomenclatura empleada para definir, por múltiplos de octetos (byte), una determinada capacidad de almacenamiento de datos:

1 Megabyte, 10,6 kb = 1024 Kilobytes
1 Gigabyte , 10,9 = 1024 Megabytes
1 Terabyte, 10,12 = 1024 Gigabytes

1 Petabyte 10,15 = 1024 Terabytes = 1.048.576 GB.
(toda la información de Google, hasta 10 petabytes)

1 Exabyte 10,18 = 1024 Petabytes = 1.073.741.824 GB
(el entero universo de Internet, hasta 350 Exabytes)

1 Zettabyte 10,21 = 1024 Exabytes = 1.099.511.627.776 GB *(1 billón, 99 millardos de Gb); orden de capacidad del datacenter NSA*

1 YottaByte 10,24 = 1024 Zettabytes = 1.125.889.990.604.800 GB *(1 billardo, 125 billones de Gb)*

1 Brontobyte 10,27 = 1024 YottaBytes
1 GeopByte 10,30 = 1024 Brontobytes
1 Saganbyte 10,33 = 1024 GeopBytes
1 Jotabyte 10,36 = 1024 Saganbytes

La actual posibilidad de manejar con enorme rapidez y facilidad volúmenes de datos absolutamente inmanejables en la era pre-digital, ha dado vida a una cultura, una industria y una voracidad especial por guardar memoria en renglones específicos, entre ellos, principalmente, los de carácter militar y los relacionados con espionaje. La capacidad de almacenamiento de datos de la *National Security Agency NSA* norteamericana, un prodigio tecnológico, es probablemente la más monstruosa jamás lograda por el hombre y seguramente la mejor equipada de todas para espiar a la humanidad entera. Su *datacenter* está ubicado en Bluffdale, Utah, costó 1.5 millardos de dólares, el espacio de sus computadoras y memorias ocupa 9,2 hectáreas, consume 65Mw de electricidad y sus acondicionadores de aire gastan unos seis millones de litros de agua diarios. Hasta 2013 disponía de una capacidad de almacenamiento de 6 *zettabytes* (ver nomenclatura anterior; 6 *zetta* representan aprox. 6 billones 600 millardos de Gb, lo que cabría en 1 billón 500 millardos de DVD de 1,2 mm de espesor los cuales, empilados uno encima del otro, darían casi para cinco columnas Tierra-Luna); pero tal capacidad se está volviendo insuficiente por lo que se construye una segunda sede en Fort Meade, Maryland. El ordenado manejo de esa mega-galáctica cantidad de información es asegurada desde 2012 por una supercomputadora digamos a la altura de las circunstancias, una *Cray Titan,* la segunda más poderosa del mundo, compuesta de 299.008 núcleos de procesado y una vertiginosa capacidad de procesamiento de hasta 24,8 *PetaFlops* (20.000 trillones de operaciones/segundo). Entre los incontables programas conocidos que este extraordinario combinado puede ejecutar, figura uno llamado *Mystic,* capaz de succionar, conservar hasta por un mes y analizar la totalidad de las conversaciones telefónicas de un determinado país.

“ En lo que sigue nos referimos tan solo a estos últimos, al sector *black hat* al que aparentemente perteneció en sus años mozos Assange, a los protagonistas menores de la llamada “guerra sucia del siglo XXI”

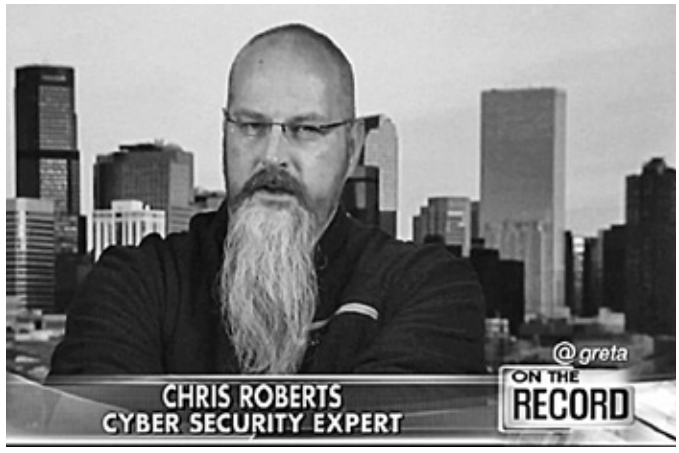
breros negros” que un sitio Internet llama sin medias tintas “los informáticos del lado del mal”. Estos últimos son los genuinos espiones de la familia al violar sistemas de seguridad de la competencia industrial, política o mercantil, o metiéndose sin invitación en coto ajeno para conocer, robar o infectar programas y contenidos de sus víctimas, víctimas que pueden ser en el más honesto de los casos traficantes de drogas, proxenetas o terroristas, y en el más deshonesto de los casos disidentes políticos, enemigos de dictadores, activistas de derechos humanos o intachables personas que alguien quiere arruinar. Muchos *black hat* están organizados en empresas que venden espionaje a sus clientes y que han creado un mercado multimillonario de la invasión electrónica *outsourcing*. Un empleado infiel de esas empresas puede “levantarse” con los secretos de una institución, de una persona, y salir a atacar a sus viejos patronos, a extorsionar gente o incluso a arruinar la reputación de alguien a cambio de dinero. Tampoco es infrecuente el caso de *hackers* que emprenden actos de piratería electrónica atrevidos y vistosos con la esperanza de llamar la atención y recibir jugosas ofertas de trabajo de agencias oficiales de espionaje o empresas que venden equipo de seguridad, como es a menudo el caso.

El estado mayor francés, por ejemplo, declaró en 2014 que los ciber-ataques a los sistemas nacionales de defensa habían sido más de 800 en 2013 con tendencia a doblar cada año. El norteamericano *Office of Civil Rights* –un segundo ejemplo– calculó en 2013 que de los *datacenter* de los hospitales habían sido jaqueados las fichas clínicas de 22 millones de ciudadanos para ser revendidas a empleadores y aseguradoras, y detectó casos en que el *hacker* había interceptado incluso los datos *wireless* transmitidos automáticamente a los médicos por desfibriladores que cargaban sus enfermos-víctimas.

En lo que sigue nos referimos tan solo a estos últimos, al sector *black hat* al que aparentemente perteneció en sus años mozos Assange, a los protagonistas menores de la llamada “guerra sucia del siglo XXI”. El “jaqueo” malintencionado también va peligrosamente in crescendo, y pocas dudas caben que los casos desclasificados y hechos del conocimiento público no representan más que la mínima punta de un iceberg de sordideces que victimarios y víctimas no desean divulgar. Durante el par de meses que duró la redacción del presente texto, por ejemplo, los medios impresos y electrónicos dieron a conocer los siguientes y multifacéticos casos, casi todos norteamericanos, del país donde siempre hay quien revele democráticamente a la ciudad y el mundo sus venturas y desventuras:

• MARZO 2015: en algún momento de marzo se descubre que al hacker ruso Evgeni Bogachev, muy *black hat* y creador del eficaz *software* ladrón de dinero Zeus, ha sustraído fraudulentamente de bancos norteamericanos sumas cuyo cálculo ya sobrepasa los 100 millones de dólares.

• 18 DE MAYO: Chris Roberts, un *hacker white hat* experto de ciber-seguridad, en intentos por comprobar las hipótesis del colega español Rubén Santamaría sobre inseguridad en aviónica, logró exitosamente, como pasajero de vuelos comerciales, introducirse unas 20 veces vía *wi-fi* en los comandos de aviones de línea en pleno vuelo,



El “white hat hacker” Chris Roberts, fundador de One World Lab; desde su computadora tomó el control del motor de un avión de línea en pleno vuelo. Fue arrestado; la United le tiene prohibición de montarse en sus aviones.

llegando en una oportunidad a tomar desde su laptop el control de uno de los motores hasta desequilibrar la aeronave. Fue arrestado en el aeropuerto de Syracuse; declaró la verdad, y que la informática de tres modelos Boeing y uno Airbus, dotados de sistemas Panasonic y Thales, presentaban fallas graves. Se descubrió incluso que el laptop previamente infectado de algún pasajero podía ser controlado a distancia para penetrar en la red informática del avión. El *General Accountig Office,* tras constatar que 35 % de la comunicación aviónica (el 60 % en 2020) pasa por Internet haciéndose vulnerable, recomendó a la *Federal Aviation Administration* adoptar muy urgentes medidas de seguridad.

• 20 DE MAYO: un grupo de *hackers* viola las computadoras de la Reserva Federal de St. Louis, una de las 12 sedes de la Banca Central norteamericana, contagiándolas y sembrando el caos en la institución.

• 21 DE MAYO: se informa de varias fuentes que los garantes de la privacidad de diferentes países están sucumbiendo a la voluntad patronal de controlar, generalmente vía *smartphone,* la conducta de sus empleados incluso dentro de las oficinas, y que en los EE.UU. más del 70 % de las empresas ya vigilan vía GPS a sus empleados que trabajan fuera de sede. Myrna Arias, empleada despedida por el empleador Intermex por haber desactivado el espía empresarial *Xora* instalado en su teléfono, está demandando a la compañía ante la Corte Suprema de California por 500 mil dólares por “un tipo de control altamente invasor de la vida privada”.

• 22 DE MAYO: la que se considera “la comunidad más grande del mundo de encuentros e intercambios sexuales” *Adult Friendfinder,* con 63 millones de inscritos, es atacada por *hackers* que sustraen datos y preferencias sexuales, e-mail y dirección de 3,5 millones de usuarios, publicándolos en la red (¡consecuencias domésticas a imaginar!).

Estas recientes revelaciones han puesto en manos del gobierno francés la evidencia que el espionaje de NSA no tenía como único propósito la lucha contra el terrorismo, sino también el de robar informaciones sobre telecomunicaciones, electricidad, gas, petróleo y energías renovables.

• 4 y 23 DE JUNIO: con cuatro meses de retraso sobre lo sucedido, la *Oficina de Administración del Personal OPM,* norteamericana, descubre que un ciberataque masivo, según el FBI proveniente del *Guabuo,* los servicios secretos chinos, ha sustraído las fichas personales de 18 millones o más de empleados públicos y de aspirantes a cargos. Los invasores atacaron a tapete tanto la OPM como las numerosas empresas privadas a las que el gobierno subcontrata el análisis de expedientes de candidatos. Se declaró que era el peor ataque informático recibido por los EE.UU., y algunos observadores llegaron a considerar que fue un ensayo mayor de guerra cibernética. El Congreso acusa ahora al gobierno de no haber respetado los estándares de seguridad informática previstos por las leyes. Hay que precisar que en materia de espionaje las escaramuzas chino-americanas son de vieja data. En enero del pasado año, tras descubrírsele dos falsas sociedades comerciales instaladas en China que en realidad espiaban las fuerzas armadas de ese país, la NSA explicó que aquello respondía a su criterio de "defensa activa".

• 23 DE JUNIO: tres años después de producirse los hechos, la prensa francesa redescubre por nuevas revelaciones de WikiLeaks que entre 2006 y 2012 la NSA espió sistemáticamente a los tres presidentes Chirac, Sarkozy y Hollande y a numerosos ministros, diplomáticos y asesores presidenciales. El 24.06 se reúne en el Eliseo el Consejo de la Defensa y se convoca a la embajadora de los Estados Unidos; la TV pública gala precisa esa noche, con imágenes, que la captación de los celulares presidenciales se hizo desde equipos instalados en la sede de la embajada norteamericana en París. Estas recientes revelaciones han puesto en manos del gobierno francés la evidencia que el espionaje de NSA no tenía como único propósito la lucha contra el terrorismo, sino también el de robar informaciones sobre telecomunicaciones, electricidad, gas, petróleo y energías renovables. En marzo, el semanario alemán *Spiegel* había asegurado, con base en documentos NSA, que hasta 2012 esa agencia tenía confiada a su unidad especial *Tailored Access Operations TAO* la misión de espiar sistemáticamente hasta 122 jefes de estado y de gobierno extranjeros (para ello, la NSA llegó a infectar con chip-espías de acceso remoto computadoras compradas en Amazon por agencias extranjeras), y que los informes sobre Angela Merkel, cuyo celular estaba bajo escucha, llenaban 300 carpetas.

• 6 DE JULIO: una de las mayores empresas mundiales de *hacking,* la italiana *Hacking Team,* (véase https://en.wikipedia.org/wiki/Hacking_Team**;** véase también *Repubblica* del 06 al 15.07.2015) es saqueada en modo devastador. No vendía sus servicios a privados, sino a gobiernos; las dependencias judiciales italianas le habían contratado en 2013 labores de espionaje procesal por 400 millones de euros, pero su principal cliente era el gobierno de México, y más abajo en la lista el de Colombia. Su más exitoso programa (el *Da Vinci* de 635.000 dólares) era un *super-trojan* que reportaba absolutamente todo lo que decía, hablaba, escribía, comunicaba y escuchaba la persona o institución espiada; lo usaban unos 30 gobiernos, entre ellos algunos dictatoriales y represivos como Sudán y Bielorrusia, pese a que la empresa asegurase respetar integralmente el Acuerdo de Wassenaar sobre exportación de armas y equipos de ciberseguridad. "No es el ataque que lanza un tipo desde el garaje de casa…vino de una empresa con mucha habilidad y paciencia…no fue un ataque sino una masacre" declaró un técnico de la empresa. Los piratas lanzaron a la red 400 Gb de sus códigos secretos, y el día 09.07 *WikiLeaks* se sumó extrañamente al saqueo publicando un millón de mails internos. Desde el pasado año *Hacking Team* venía persiguiendo legalmente a seis ex empleados infieles. Como decíamos en el escrito anterior, uno de los mayores problemas de quienes diseñan las ciberguerras de mañana es determinar sin margen de error (que pudiera resultar fatal) de dónde viene el ataque. El presente caso es particularmente revelador al respecto, y por eso digno de algún seguimiento. ¿Vino el ataque de ONG filo-occidentales, de *Anonymous,* de algún competidor comercial, de exempleados infieles, de la mismísima *Camberdada* (ver *infra*)?

Este largo botón de muestra permite constatar que para el espionaje no hay tema, personaje o institución inviolable o tabú, que todo vendedor de protecciones antijaqueo puede ser jaqueado, que un jaqueo indeseado en ámbitos electrónicos sensibles, incluso si bienintencionado, puede generar desastres, y que el incremento exponencial del espionaje por monitoreo electrónico viene estrechando cada día más los ya angostos márgenes de la humana privacidad.

Pero en los predios de los *black hats* las cosas son más complicadas aún, porque mientras los "artesanos" del espionaje están en la imposibilidad técnica de escalar el negocio filtrando millardos de mensajes diarios como lo hacen los *big,* éstos sí pueden miniaturizar sus intervenciones y practicar a su vez el jaqueo a escala reducida, atacando blancos precisos. Hoy se comienza a saber que los dos *superbig,* NSA y CGHQ, decidieron hace rato ya, en 2008, que los sistemas de protección contra virus, *malware* y otras invasiones maliciosas producidos por medianas o pequeñas empresas, eran un estorbo para las tareas de espionaje masivo que tienen encomendadas, lo que los condujo a lanzar la operación ultrasecreta *Camberdada* (ver https://firstlook.org/ theintercept/document/2015/06/22/project-camberdada-nsa/),una operación con sus ribetes irónicos, porque se trataba de invadir exitosamente empresas que venden programas para no ser invadidos. Lo ha señalado recientemente la publicación *The Intercept* (ver https://es.wikipedia.org/wiki/The_Intercept) vinculada a E. Snowden, precisando que el objetivo de *Camberdada* es espiar sistemáticamente a los fabricantes de antivirus no para infectar su trabajo o impedirles vender sus mercancías, sino para robarse sus secretos y funcionamiento de programas a fin de conocer siempre y de antemano sus mejoras a venir y estar en condiciones de burlarse de todo nuevo filtro de seguridad aún antes de su salida al mercado. De las 23 grandes compañías productoras de antivirus "visitadas" por *Camberdada,* se precisó, ninguna es americana o inglesa (como lo son McAfee, Symantec o Sophos); su blanco principal fue la empresa rusa *Kaspersky* (270 mil clientes empresariales y 400 millones privados), tal vez en venganza de que en febrero había revelado al mundo la existencia de *Equation Group* (ver https://en.wikipedia.org/wiki/Equation_Group) un vástago de la NSA "probablemente el más secreto y sofisticado aparato de espionaje existente", responsable de *blitz* informáticos contra gobiernos, ejércitos, empresas de alta tecnología y centrales nucleares en 30 países.

“(...) el abigarrado e infatigable espionaje “civil” descrito en estas páginas, finalmente pudiera no ser más que una suerte de fase preparatoria o de adiestramiento al gran espionaje militar finalmente liberado –pensará más de un general– de las ataduras de leyes (...)

LA CIBER-GUERRA PRÓXIMA FUTURA

(VER ARTÍCULO ANTERIOR)

Hace pocas semanas, un breve filmado de la aviación norteamericana mostraba un militar de rango medio-bajo, cómodamente sentado delante de una computadora en su cuartel de Carolina del Norte, piloteando con su *joystick* un dron que ejecutaba una mortífera acción ofensiva por los lados de Pakistán, a 12 mil kilómetros de distancia. ¡Una perfecta representación de las ciber-guerras próximas futuras, donde el robot remplazará a un soldado-telepiloto que, concluida exitosamente su matanza, marca tarjeta y vuelve a casa a cenar tranquilamente y juguetear algo con los niños!

Traemos a colación este ejemplo porque la mayoría considera, a nuestro entender equivocadamente, que el término “ciberguerra” solo debe emplearse cuando se asume el universo de las comunicaciones como un campo de operaciones bélicas en que un sistema informático trata de destruir al otro. Si uno solo recuerda el *Stuxnet* americano-israelí que en 2011 volvió un caos los ordenadores de las centrales nucleares iraníes, esa limitada definición funciona. Pero hay razones etimológicas y lógicas, y hechos concretos, los cuales inducen más bien a pensar que, además de ese aspecto, el término debe denotar también la totalidad de aquellas operaciones bélicas en que la presencia, la orden o la decisión humana de proximidad son remplazadas por un pilotaje a distancia parcial o totalmente pre-programado (*kubernetés* en griego es “piloto”), es decir, por armas robotizadas siempre más “inteligentes”, en cuyo caso el *hacker* que viola o infecta un banco de datos enemigos y el piloto a distancia de un arma de ataque lejana caben en una misma definición de ciberguerra.

Ese tipo de guerra –mezcla de ataques informáticos con uso siempre más refinado de control y pilotaje electrónico, a la que como vimos más de sesenta países se están intensamente preparando– requerirá obviamente muchísima tecnología como armas robóticas, tele-comandos infalibles, finos sensores, geolocalizaciones al milímetro e implacables jaqueos y *malware,* más una labor previa, capilar y masiva de espionaje, al punto de poderse hasta pensar que el abigarrado e infatigable espionaje “civil” descrito en estas páginas, finalmente pudiera no ser más que una suerte de fase preparatoria o de adiestramiento al gran espionaje militar finalmente liberado –pensará más de un general– de las ataduras de leyes, normas, oposiciones, ONG y cortesías que rigen el comportamiento de la sociedad civil en tiempos de paz.

Los indicios de que de oriente a occidente se ensaya el ciberataque se multiplican y son inquietantes. A los casos ya citados cabe añadir otros recientes de carácter estrictamente militar o político, como el robo, aparentemente chino, de los planes del nuevo avión norteamericano de combate *stol* F.35, el bloqueo de Rusia desde Crimea, de hace meses, al sistema telefónico ucraniano, o los fuertes ataques, aparentemente norcoreanos, a bancos surcoreanos y a la americana Sony. Eso explica por qué el Pentágono anunció el pasado abril que se dispone a “utilizar las operaciones cibernéticas para entorpecer el mando y control de las redes enemigas, sus infraestructuras militares y la capacidad de su armamento” (o sea, anuncia oficialmente que pasará de la ciberdefensa al ciberataque), y por qué el pasado mayo la NATO organizó en Tallin, Estonia, en el marco de su *meeting anual Cooperative Cyber Defence Centre of Excellence* con la participación este año de 16 naciones, el simulacro de ciberguerra más grande efectuado hasta la fecha, llamado *Locked Shield 2015* (ver https://ccdcoe.org/).

El Lector apasionado de este tema consultará con provecho la amplia documentación de Google en la materia, a la que ha dedicado en marzo de este año *La Vanguardia* de Barcelona su dossier n° 54 (http://www.lavanguardia.com/internacional/20141211/54421704765/la-ciberguerra-vanguardia-dossier.html).

BREVE Y PRECARIO EPÍLOGO

El estado del arte 2015 en espionaje, que aquí y en un texto anterior se intentó esbozar, es casi seguramente incompleto por la inconmensurable cantidad de programas e iniciativas que los grandes patronos de la vigilancia logran mantener *top secret,* ciertamente inconcluso por faltarle un análisis de la mitad oculta de la luna, las grandes potencias opacas Rusia y China más los llamados “Estados canalla”, y poco incluyente por haber desatendido el menudo control que, según *Reporteros sin Fronteras* y la *Open Net Initiative* ejercen 74 países del mundo (incluyendo grandes democracias y muchos países latinoamericanos) sobre la mensajería electrónica de sus ciudadanos. Aun así, luce suficiente para una amarga constatación: pese a desear lo contrario, fuerza es constatar que las huestes de la Vigilancia global avanzan y se consolidan, y las defensas de la Libertad retroceden en orden disperso. Tras enterarse del tamaño, eficacia/eficiencia, omnipotencia y expansión de las grandes centrales de robo de información, luce muy poco real imaginar una desescalada mundial, un mundo desalienado que convierta unánimemente a Assange y Snowden de criminales en héroes.

El poder inercial de esos gigantescos conglomerados es tal, que hasta la opinión razonada de entendidos, de que ese espionaje a tapete o de arrastre es finalmente improductivo e incapaz de prever ataques, pareciera no alterar en lo más mínimo el *statu quo.* Citemos *in extenso,* por emblemática, la opinión del informático francés Philippe Agrain, vara alta de la oposición europea a la vigilancia masiva:

> La vigilancia no nos protege de los atentados… sólo limita nuestra libertad de expresión… La paradoja es que ese tipo de vigilancia puede aumentar grandemente el riesgo de falsas alarmas, de los llamados ‘falsos positivos’… Confrontamos una puesta en escena permanente del miedo… ante la cual estamos ya desarmados, sin saber cómo luchar por nuestras libertades… Ese clima de miedo y sospecha sólo facilita a quienes detentan el poder la tarea de conservarlo… El otro riesgo profundo es que comenzamos a autocensurarnos al sospechar que estamos bajo escucha… es la esterilización del espacio público democrático… (véase: http://www.repubblica.it/tecnologia/sicurezza/2015/06/28/news/francia_via_libera_alla_sorveglianza_di_massa_philippe_aigrain_cosi_siamo_solo_meno_liberi_-117871441/)

Deprime constatar que la convulsionada historia contemporánea, con sus reiterados resurgimientos de odios históricos y de fundamentalismos particularmente feroces, no hace más que convalidar los justificativos y métodos de los vigilantes universales, las visiones distópicas

El informático y politólogo francés Philippe Agrain, director de *La Quadrature du Net* y co-director del *Freedom Law Center.*

de una humanidad *blade-runner* en estado de radical des-privacidad, encaminándose hacia el chip de identificación debajo de la piel, regimentada y controlada por ordenadores.

A la Comunicología se le confirman las peores dudas: sí, una sociedad como la nuestra, que invierte en comunicaciones la barrabasada del 13% del PIB del mundo y el 10 % de la energía que produce –empleándolos en convertir el entero saber y praxis humanos en bits que luego almacena en inmensas bit-tecas y pone en circulación por cobres, micro-ondas, fibras, satélites y cables, todo ello fácil de violar, infectar y robar comenzando por sus propios almacenadores y transmisores–, no podía sino crear las condiciones para que prosperase hasta lo inverosímil el robo de esa codificación etérea de lo real. Aprovechando las fragilidades del nuevo código dígito binario, nuestro mundo agigantó la milenaria tarea de espiar, al punto de producir un salto cualitativo, una pesada interferencia en los delicados mecanismos de los derechos humanos, más indefensión del individuo y una degradación general en su privacidad y libertad de comunicar, de asociación y de acceso a la información. El pasado abril, interviniendo en diferido en un Festival del Periodismo en Perugia, Italia, Snowden dio al respecto declaraciones casi contradictorias con las anteriormente citadas:

> **La prioridad de las agencias es vigilar todos y siempre, sin reglas… El debate de la opinión pública al respecto es muy pobre… Asistimos a uno de los mayores sistemas de opresión de la historia… Cuando permitimos a la vigilancia masiva de instalarse, cambia de manera radical la relación entre gobiernos y gobernados… (ver http://www.repubblica.it/cultura/2015/04/17/news/edward_snowden_festival_giornalismo_perugia-112217422/)**

Todo indica que estos poderes omnímodos de vigilar y hurgar en la vida de cada quien han llegado para quedarse. Una difusa morosidad moral de los gobernantes hace que ningún gobierno esté realmente dando vida y sustancia, con praxis concretas más que con declaraciones, a uno de los más equilibrados postulados de los *Principios Internacionales*… de los 60 países (ver *supra*): combinar una vigilancia de las comunicaciones legítima y proporcionada con la protección de las libertades humanas fundamentales. Siempre prevalece la *raison d'état,* la voluntad de los Estados mayores y de los grandes combinados económicos y armamentistas, el miedo a un desarme unilateral de los propios servicios de espionaje e incluso a uno multilateral como se logró con las armas nucleares y químicas. Según una investigación del *Pew Research Center* de 2013/2014, las principales amenazas a la red no vendrán en el futuro de *hackers,* sino de gobiernos y de los propios administradores de redes, la vigilancia seguirá siendo ejercida al igual por totalitarismos y democracias con el pretexto de la seguridad, y

> **Aprovechando las fragilidades del nuevo código dígito binario, nuestro mundo agigantó la milenaria tarea de espiar, al punto de producir un salto cualitativo, una pesada interferencia en los delicados mecanismos de los derechos humanos, más indefensión del individuo y una degradación general en su privacidad y libertad de comunicar (...)**

seguirá la interesada confusión entre espionaje político e industrial. En su relación al gobierno de junio 2014, el Garante italiano de la Privacidad, A. Soro, denunció que "los datos coleccionados por los gigantes del web para fines comerciales se vuelven siempre más interesantes a los ojos de los gobiernos para fines de seguridad, a los cuales están inextricablemente enlazados" (ver: http://www.repubblica.it/tecnologia/2014/06/10/news/il_garante_della_privacy_nel_2013_sanzioni_per_oltre_4_milioni-88554777/). También Navi Pillay, alta comisionada de Derechos Humanos de la ONU, denunció el 16.07.2014 esa misma connivencia "de facto, de empresas y gobiernos, para acceder a la información de los ciudadanos" (véase: http://www.un.org/spanish/News/story.asp?NewsID=29974#.VZqd6_l_Oko). Hace días apenas, el 15.07.2015, el nuevo Relator de la ONU para la Libertad de Expresión, David Kaye, declaró: "es hora de que en la relación de los gobiernos con la industria de la vigilancia se tomen seriamente en cuenta los derechos humanos", y añadió: "La ecuación más criptografía más crimen no tiene el menor sentido. La criptografía es más bien el fundamento de la seguridad y la privacidad en la red; terroristas y pedófilos la usan también…pero así fue con cada nueva tecnología en la historia humana…Condenar la criptografía significa producir más, y no menos, criminales". (en http://www.repubblica.it/tecnologia/sicurezza/2015/07/15/news/intervista_kaye_hacking_team-119143712/)

Una aclaratoria final: todos los datos aquí proporcionados, absolutamente todos, son del dominio público y figuran publicados en impreso o electrónico; nos hemos limitado a reunirlos, jerarquizarlos y organizarlos de forma coherente. Ellos nos han conducido al borde de una vorágine socio-política-cultural, a mirar con fascinado horror el precipicio al que pudiéramos ser lanzados, donde nos esperaría una inaceptable pérdida de calidad en la relacionalidad humana de la mano de una tecnología descarriada y digresiva. Hemos constatado que la sedicente necesidad de vigilar mucho para impedir el mal se ha convertido en uno de los más temibles atentados a nuestras libertades y privacidad tan penosamente conquistadas.

Pero nuestras comprobaciones y constataciones hubieran sido imposibles fuera del ámbito de las democracias occidentales, que aún abrigan un fuerte poder de información y denuncia de lo ajeno y de lo propio, y donde siempre es posible que una sobreviviente libertad de comunicar termine salvándonos de lo peor. A los vigilados nos es connatural el Principio Esperanza.

ANTONIO PASQUALI
Egresado de la UCV, fundó en 1958 el Centro Audiovisual del Ministerio de Educación y en 1974 el Instituto de Investigaciones de la Comunicación, Ininco. Ha sido en 1984-86 SubDirector General de Unesco, a cargo del sector Comunicación.