ESPIONES

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

ANTONIO PASQUALI

Prolegómenos

Los decenios de la Guerra Fría (ella continúa en versión *soft*, con otras tecnologías) vieron la apoteosis del espionaje, peculiar inflexión del comunicar y oficio tan viejo como la prostitución. Sin embargo, el progreso venía colgando en las paredes del recuerdo la figura del individuo-espía, del espión solitario y *old fashioned* modelo Mata Hary o Philby al que tantas apasionantes obras dedicó sobre todo el cine (recordemos *Los Espiones* de F. Lang 1928, *Operación Cícero* de J. Mankiewicz 1952, *Los Espiones* de H. Clouzot 1957 y *El espía que vino del frío* de M. Ritt 1965). Mientras la cultura rendía homenaje a los héroes de un oficio en vía de transfiguración, este ascendía velozmente a la fase superior e irreversible de su masificación y digitalización. Algunos episodios emblemáticos del nuevo espiar. El U-2 primero y los satélites militares poco después comenzaron a escudriñar cada metro cuadrado del planeta Tierra (la cohetería rusa en los muelles de La Habana en 1962 no fue señalada por soplones sino fotografiada desde el cielo); el submarino norteamericano Halibut (con más electrónica que los soviéticos) sí logró sacar en 1968 de una fosa del Pacífico de 5 km de profundidad medio submarino "enemigo", el K 129, con sus cohetes nucleares, y en 1971 aplicó furtivamente al cable coaxial Kamchatka-Vladivostok un brazalete electrónico que durante años succionó y proporcionó al Pentágono informaciones vitales (se cree hoy que el submarino nuclear Jimmy Carter aprendió la difícil tarea de leer la mensajería de los cables de fibra); ni corto ni perezoso, el espionaje militar soviético GRU instalaba en 1964 en Lourdes, a 60 km de la Habana, una base de espionaje electrónico que llegó a ser la más grande del mundo; costó 3 millardos de dólares de la época, cubría 70 km2, ocupaba 2 mil técnicos rusos y hasta 2002 proporcionó a Rusia, se dice, 75 % de su inteligencia militar. Pero el ejemplo más elocuente del cambio en vigilancia pudiera ser el de las camaritas TV de circuito cerrado (CCTV), que hoy remplazan millones de "gorilas", espías de negro sombrero fingiendo leer el periódico en la esquina u ojeando el entorno desde un automóvil. En Inglaterra, con 6 millones de CCTV en uso, se graba hasta 300 veces diarias el transeúnte, y lo cierto es que miles de malhechores están hoy tras las rejas a fuerza de su eficacia.

Del precedente "Echelon"…

Toda la inteligencia militar y civil ha terminado adoptando las modernas tecnologías del espionaje a distancia, pero las rencillas siguen su curso. En 2000 la Comunidad Europea y países miembros de la OTAN se sintieron humillados al enterarse oficialmente de algo que en realidad se sabía desde 1976: los servicios secretos de los países WASP (*White anglo-saxon protestant*), la NSA de Estados Unidos, el GCHQ del Reino Unido, el CSE de Canadá, el DSD de Australia y el GCBS de Nueva Zelanda, habían formado grupo aparte para el espionaje sin informar a sus aliados, poniendo en obra el programa Echelon, 100 % electrónico y de cobertura global, aún hoy la red de espionaje más poderosa jamás creada por el hombre.

Principales razones de aquel malestar

1. Descubrir la existencia de un eficiente centro de inteligencia grupal en su propio seno que espiaba sistemáticamente a todos y cada uno de los aliados.

2. Haber comprobado que Echelon no solo realizaba espionaje militar sino también industrial y comercial a favor de los WASP, lo que le había hecho perder a Europa contratos de miles de millones de dólares.

El 11 de julio de 2001 el Parlamento europeo publicó su doc. A5-264/2001 sobre Echelon encabezándolo con un epígrafe de las Sátiras de Juvenal: *Sed quis custodiet ipsos custodes?* (pero ¿quién custodiará a los propios custodios?), un fascinante texto de 204 páginas (relator Gerhard Schmidt), suma de historia del espionaje y de sus cambios recientes, que define al espionaje como "el robo organizado de información" y que todo politólogo debería consultar. La tragicomedia concluyó… con la decisión de muchas potencias intermedias de equiparse con un Echelon propio, en medio de acrobacias teóricas destinadas a garantizar el respeto de las libertades privadas. Todo Occidente asegura, por ejemplo, no espiar a sus propios ciudadanos dentro de sus fronteras, pero cuando necesita poner bajo vigilancia a un compatriota, le pide el favor a una potencia amiga que espiará entonces a un "extranjero" y remitirá sus conclusiones al país interesado. ¡Elemental, Watson!

Se considera hoy que el recién revelado sistema de espionaje Prism (al igual que Echelon depende de la National Security Agency de los Estados Unidos) es apenas un subsector del anterior, que se hizo necesario para un aggiornamento tanto frente a las recientes tecnologías vinculadas con el Protocolo Internet IP, como al ocaso de los satélites y el auge del cable de fibra (que transporta hoy casi 100 % de la telefonía de larga distancia). Con sus casi 40 años a cuestas, Echelon sigue asombrando por su tamaño, eficacia y desmesurada ambición de espiar meticulosamente las emisiones radiales, el tráfico satelital, la telefonía, el fax y los correos electrónicos de la entera humanidad. Lo componen la barrabasada de unos 120 satélites geoestacionarios y unas 16 estaciones terrestres de rastreo (2 de las cuales son Menwith Hill en Inglaterra y Fort Meade, en Maryland, de dimensiones colosales, y una en Brasil operada conjuntamente por NSA y CIA), trabajan en él unos 300 mil empleados a escala mundial (100 mil en Maryland) y sus computadoras-receptoras, llamadas "diccionarios", pueden filtrar y procesar hasta 2 millardos de mensajes por hora, estando equipados –tanto la NSA como el GCHQ inglés– para trabajar en el rango del exabyte (un millardo de giga).

> *Muchas de las revelaciones sobre espionaje contemporáneo hoy del dominio público no son producto de extorsiones, doble espionaje, torturas a agentes enemigos o robo de microfilms (pura quincalla del pasado), sino exteriorizaciones espontáneas de anónimos burócratas del neo-espionaje electrónico.*

…al Prism de hoy

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, remplazado hoy por ejércitos de anónimos burócratas del espionaje, empleados de escritorio y hackers a sueldo de un gobierno (mucho menos simpáticos que los solitarios lobos de antaño), víctimas a veces de súbitos desequilibrios, exhibicionismos, arrepentimientos o escrúpulos de conciencia, que de repente amanecen soltando prenda. El hecho es comprensible: ¿cómo asegurarse 100 %, pongamos por caso, que todos y cada uno de los 300 mil espías de Echelon sean "patria o muerte" con su empleador? Muchas de las revelaciones sobre espionaje contemporáneo hoy del dominio público no son producto de extorsiones, doble espionaje, torturas a agentes enemigos o robo de microfilms (pura quincalla del pasado), sino exteriorizaciones espontáneas de anónimos burócratas del neo-espionaje electrónico. Casos memorables: en 1971 el analista del Pentágono Daniel Ellsberg reveló, en las 7 mil páginas de su Pentagon Papers, que la administración Johnson le había mentido al país y al Congreso sobre la Guerra de Vietnam; en 1972 William Kampiles, un empleado de la CIA, aburrido, vendió a los soviéticos por 3 mil dólares el manual de uso del satélite-espía americano KH-11(condenado a 40 años); en 1971 el analista de la NSA Wislow Peck (alias Perry Fellwock) reveló al mundo la existencia de esa segunda super-CIA por la que trabajaba, y en junio de 1976 informó a los europeos de la existencia de una tercera super-CIA llamada Echelon (durante la navidad de ese año desapareció sin dejar rastro); en 1980 un analista de la CIA agobiado por deudas de juego, Robert Pelton, vendió por 70 mil dólares a la Embajada de la Unión Soviética en Washington la información del brazalete electrónico instalado por Halibut sobre el cable submarino ruso (condenado a cadena perpetua; el sistema de espionaje, mejorado, fue reinstalado con éxito meses después); en 1996 los periodistas Duncan Campbell, escocés, y Nicky Hager, neozelandés, revelan en Secret Power el uso de Echelon para espionaje industrial a favor de los países anglosajones; en 2006 Julian Assange, hacker australiano con 2 docenas de cargos por delitos informáticos, revela en Wikyleaks el contenido de millones de documentos diplomáticos principalmente estadounidenses por él pirateados (perseguido; actualmente asilado en la Embajada de Ecuador en Londres); en 2013 Edward Snowden, ex empleado de CIA y NSA con escrúpulos de conciencia, revela al mundo documentos *top secret* sobre la existencia de una cuarta super-CIA, el nuevo programa de espionaje Prism (caso definido como "asunto criminal" por el Departamento de Justicia estadounidense; confinado en el aeropuerto de Moscú con ofertas de asilo, inclusive del actual régimen venezolano).

El nuevo sistema de espionaje Prism, probablemente creado en 2007 y con los ingleses de únicos *partners* desde 2010, ha sido implementado para añadir a lo ya espiado por Echelon lo que hoy viaja preferentemente por fibra: sms, videos, chats, fotos, paquetes de datos y transferencias de archivos, twiteos, voz, videoconferencias, tiempo de login y perfiles completos de redes sociales, combinando capturas *upstream* antes del enciframiento y envío a la fibra, con capturas *downstream* del mensaje procesado, lo que implica un acceso directo a servidores y la instalación de equipos captores de NSA directamente dentro de las empresas para copiar mensajes justo antes de su cifrado y envío. Esto sin contar con los vitales metadata de todos modos conservados por el transportista (ver explicación en el Cuadro 1) que a menudo revelan más que el propio mensaje.

El apetito de Estados Unidos por la sigilosa fibra óptica nació en 2003, cuando la telecom americana Global Crossing fue adquirida por la china Level 3 Communications. Ante un peligro potencial, la Homeland Security impuso al comprador

CUADRO 1
LOS METADATA

Se definen como metadata a la informacion que originamos automáticamente al hacer uso de un medio de comunicación (excepto su contenido), las cuales son sistemáticamente memorizadas y conservadas por el transportista del mensaje y posteriormente analizadas a la demanda de servicios de inteligencia y espionaje, los cuales estiman que el "contenedor" del mensaje, justamente los metadata, puede revelar hasta más que su contenido. Para el caso de la NSA, su colecta y clasificación estaría a cargo del subprograma Blarney. Como se constata en este Cuadro, los metadata aseguran al analista una masa imponente yz altamente significativa de informaciones (lista derivada de la publicada en *The Guardian* el 18 de junio de 2013).

Usando el e-mail: nombre del remitente, su e-mail y su dirección IP/ nombre del destinatario y su e-mail/ informaciones de transferencia del server/fecha, hora y huso horario / identificador unívoco de correo electrónico y de los relativos mensajes/ tipo de contenido codificado/*login* del cliente con dirección IP/prioridades y categorías/asunto del e-mail/condiciones del e-mail/solicitud de recepción contestada.

Usando el teléfono: número de cada usuario/número de identificación IMEI de cada celular/hora de llamada /duración de la llamada/ubicación de los interlocutores/número tarjeta telefónica empleada.

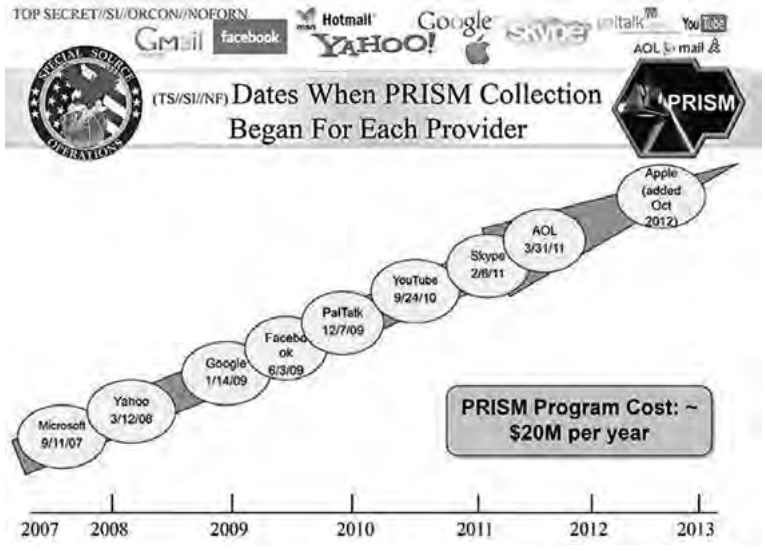
Usando *Facebook*: nombre del usuario y perfil bio: cumpleaños, lugar de residencia, profesión, intereses/ identificador único del remitente/sus suscripciones/su ubicación geográfica/ fecha del envío, hora y huso horario/ mensajes anexos/otras actividades, "me gusta", *geotag* y otros acontecimientos.

Usando *Twitter*: nombre del usuario, su lugar, su idioma, su perfil y su url /fecha de creación de su account/su nombre de usuario e identificador único/localización de envío y recepción del tweet, fecha, hora y huso horario/ ID unívoco del remitente y del destinatario/ID de quien contribuye/lista de seguidores del usuario, de seguidos por el usuario y de post favoritos/estado de la verificación /aplicación que emplea para enviar su tweet.

Haciendo búsquedas en la red: solicitud formulada/resultados aparecidos en pantalla/páginas visitadas.

Navegando por internet: toda la actividad, páginas visitadas y en qué momento/datos del usuario, detalles de login/dirección IP del usuario, su provider de servicios internet, detalles del *hardware* del aparato, de su sistema operativo y de su versión del *browser/cookies* de los datos memorizados en el *cache* de los sitios.

Cuadro 2



Este cuadro (uno de los seis *top secret* revelados por Snowden) muestra las fechas en que los grandes proveedores norteamericanos de servicios de mensajería electrónica se sometieron a las horcas caudinas de la NSA

la aceptación en el seno de la empresa de una estructura gubernamental paralela, concretamente "un equipo de ciudadanos estadounidense aprobado por el gobierno en posiciones de mando para el acceso a las comunicaciones". El precedente hizo escuela. El Cuadro 2 (una de las 6 hojas *top secret* del Power Point revelado por Snowden) muestra las fechas en que todos los *big* de la comunicación vía Internet –desde Microsoft en noviembre 2007 a Apple en octubre 2012– se plegaron a las horcas caudinas de Prism. Que nadie se rasgue las vestiduras: todas las telecom del mundo, sin excepción, colaboran activamente con los servicios de inteligencia del país huésped, o por estar nacionalizadas como nuestra Cantv (lo que facilita la discrecionalidad del espionaje) o por asentar en naciones cuyos gobiernos dejan el negocio telecom en manos privadas pero controlan férreamente la mensajería que transporta tanto, o mejor, que las dictaduras. Recientes normas estadounidenses obligan a la empresa telecom extranjera que desee operar en el país a instalar en territorio estadounidense su Network Operation Center, a aceptar que este "sea visitado por funcionarios federales con preaviso de 30 minutos" y a satisfacer solicitudes de información que "no podrán ser comunicadas al *top management* de la empresa".

Las actividades de Prism son supervisadas por la Foreign Intelligence Surveillance Court, el llamado "Tribunal Secreto" (nadie puede asistir a sus deliberaciones) o "Corte Suprema Paralela" (por su capacidad de violar derechos constitucionales). El pasado 20 de julio sus tres jueces volvieron a autorizar a Prism para la recolección y análisis de los metadata, y el 24 de ese mes la Cámara de Representantes rechazó por 217 a 205 votos, un intento bi-partidista de castigar ese monitoreo reduciéndole el presupuesto a la NSA (en un mundo en que todos se espían, nadie renuncia a la menor parcela de su propia capacidad de espiar).

¿Por qué los tentáculos del espionaje electrónico estadounidense monopolizan casi el poder de espiar la entera humanidad? El cuadro 3 proporciona una clara respuesta: de los 12.452 Giga/seg de tráfico mundial (datos de 2011), 10.609, esto es 85 %, transitan por Estados Unidos, más *free flow* en tránsito por los grandes nodos estadounidenses o por las glamorosas "redes sociales" como Facebook y Twitter, más incautos depósitos en el *cloud*, más material para un más fácil espionaje. Internet es un producto estadounidense (y casi pudiera decirse californianos) son Icann, la Corporación para la Asignación de Nombres y Números, Cisco el gigante

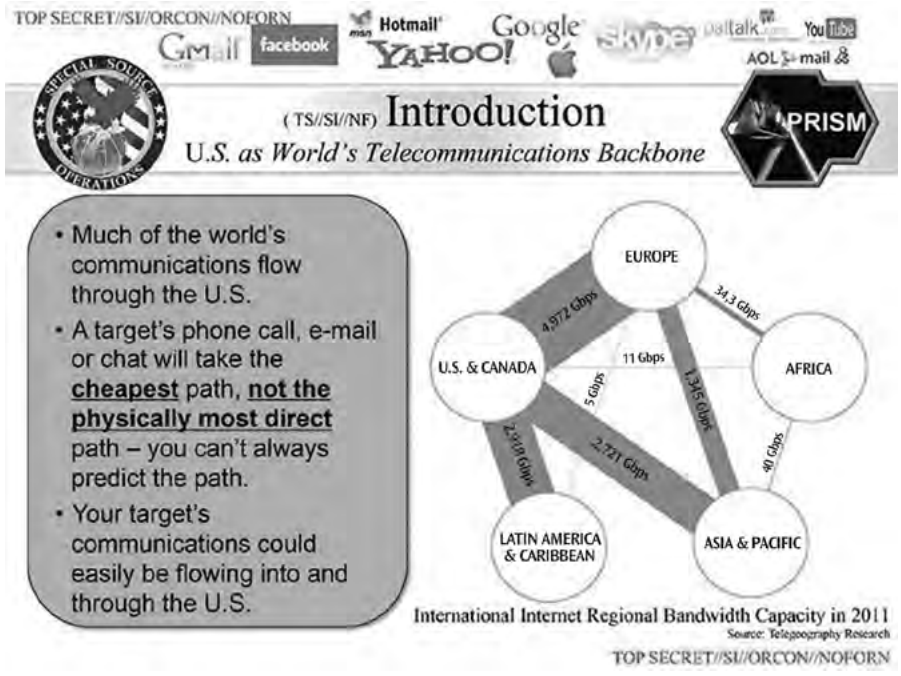
mundial de conmutadores, enrutadores y concentradores, Silicon Valley la mayor concentración del mundo de empresas de alta tecnología, todos los grandes y más conocidos servidores de la red, los principales y más avanzados productores mundiales de hardware y software, todos los gigantescos depósitos de información ajena eufemísticamente ubicados "en la nube" y las cabeceras de todas las redes sociales. Vanos han sido los intentos desplegados hasta la fecha ante la UIT por internacionalizar el gobierno de la red.

En una entrevista publicada en *Le Monde* el 13 de julio, el experto finlandés en seguridad Jarno Limnéll añade otra preocupación: Prism sería la punta del iceberg de la ciberguerra próxima futura a la que las grandes potencias se vienen preparando, con China, EE.UU. y Rusia en posición avanzada. Un espionaje infalible es condición *sine qua non* de las futuras ciberguerras, que comprenden tanto la ciberdefensa como el ciber-ataque, este último basado en malware (programas maliciosos, malignos u hostiles), una actividad privada en crecimiento exponencial pero elevada por primera vez a arma gubernamental por EE.UU. e Israel con Flame (un Prism dedicado que les permitió recolectar silenciosamente datos vitales sobre el programa nuclear iraní), y luego con Stuxnet, un malware que saboteó en profundidad durante meses sus instalaciones nucleares. La perspectiva de un conflicto mundial todo cibernético, basado en mecanismos masivos y automatizados de espionaje, es tan realista que los departamentos de ciberdefensa estadounidense y ruso preparan en estas semanas la rehabilitación del "teléfono rojo" Kremlin-Casa Blanca a fin de prevenir en lo posible fatales errores de apreciación, por cuanto la principal dificultad en una ciberguerra será determinar con exactitud de quién y de dónde se recibe un ciberataque (el proyecto es hoy prioritario para la Darpa estadounidense).

Facebook había anunciado meses atrás haber desarrollado un algoritmo que tamiza todas las conversaciones y envía automáticamente las sospechosas al FBI. Según *Guardian*, Microsoft habría asegurado a la NSA los medios para espiar los contenidos de Outlook, de todos los correos (incluyendo los de Hotmail) y de todas las llamadas vía Skype, garantizándole un bypass de todos sus sistemas de enciframiento. El esfuerzo estadounidense por asegurarse un espionaje eficientísimo e infalible, de defensa y ataque, no pareciera tener límite. En 2008 un funcionario de AT&T reveló que NSA espiaba directamente los servidores de la empresa; Spiegel declaró poseer pruebas de que las embajadas de Francia e Italia en Washington, y ciertas instituciones clave de la Unión Europea, estaban bajo escucha de NSA; un librero de Buffalo descubrió por azar la existencia de un espionaje… postal, con apertura de toda pieza sospechosa y escaneo del sobre de todos los envíos postales a Estados Unidos: 160 millardos de piezas en 2012. Las potencias intermedias no se quedaron a la zaga. Desde 1995, por comenzar, la Comunidad Europea dispone de su propia NSA, se llama Enfopol. El jefe del espionaje exterior de Alemania acaba de informar que utilizaron durante años programas NSA, y que Alemania envía a EE.UU. un promedio de 500 millones de datos mensualmente. Italia dispone de su propio "Echelon"; sus tres sistemas satelitales barren el Mediterráneo y responden desde 1997 al Reparto Informazione e Sicurezza, que dispone de una escuela de guerra cibernética. Tras precisar que "todos los servicios occidentales de inteligencia se espían el uno al otro" el periódico *Le Monde* revelaba el 4 de julio que también la Direction Générale de la Sécurité Extérieure de Francia "dispone de un *big brother* a la francesa". Quinta potencia mundial en espionaje detrás de EE.UU., Gran Bretaña, Israel y China, Francia también cuenta con sistemas satelitales propios, unas 20 estaciones terrestres de escucha, 4 mil 900 empleados y supercomputadoras en capacidad de procesar exabytes y millardos de mensajes diarios, ¿y qué no estarán cocinando en los campos del espionaje electrónico y de la ciberguerra esas grandes potencias opacas que son China y Rusia, países donde las revelaciones modelo Ellsberg, Kampiles, Peck, Pelton, Campbell, Hager, Assange y Snowden no son posibles?

CUADRO 3

Este cuadro (uno de los seis *top secret* revelados por Snowden) muestra que más del 85 por ciento de las comunicaciones mundiales llega a su destino vía los Estados Unidos



¿Conclusiones?

Dos por ahora. Debido al terrorismo en expansión con su síndrome del 11S, y a los exitosos intentos gubernamental-empresariales de apropiarse de la red, "las democracias han cambiado para siempre", en palabras del escritor Roberto Saviano. En sentido positivo, añadamos, si constatamos a), que una enorme cantidad de saberes antes manejada por pocos está ahora al alcance de todos, oxigenando una democracia participativa y mejor informada, y b), que las nuevas tecnologías han devuelto a todos una capacidad de emitir mensajes antes confiscada por oligarquías. En sentido negativo porque (habla ahora Tim Berners Lee, el inventor del www) asistimos a un intento "de gobiernos y grandes empresas de tomar el control de la red… de manipular opiniones y pensamientos, de interceptar comunicaciones…

que en manos de gobiernos corruptos pudiera eternizarlos en el poder".

La segunda: la hora parece haber llegado, definitivamente, de entonar un réquiem por la muerte de la privacidad; las nuevas tecnologías nos encierran en una vitrina llena de captores que todo saben de nosotros, nuestra esfera privada se evapora bajo el incesante impacto de centenares de sistemas globales de espionaje despiadadamente eficientes, por grabaciones y tomas ilícitas, por "perfiles del consumidor", análisis de metadata, cookies, "me gusta", cámaras ocultas, posicionamiento vía GPS, directorios y una acumulación sin fin, en monstruosas memorias electrónicas, de datos comportamentales y gustos civiles, políticos, económicos, sanitarios, educativos, consumistas, bancarios, culturales, alimenticios, higiénicos, sexuales y otras intimidades de cada ser humano. Opinan algunos, como Martin Cooper inventor del celular, que no todo es negativo, que "hemos perdido un tipo de libertad para ganar otra" y cita el caso del atentado de Boston resuelto en pocos días gracias a las cámaras de seguridad y los celulares de los transeúntes (añadamos el ejemplo del GPS, que permite a otros saber dónde estamos en cualquier momento, pero también de encontrarnos en caso de secuestro). Opinan otros, en cambio, como el ya citado Berners Lee, que urge un esfuerzo supremo de los gobiernos por devolver neutralidad e independencia a la web, salvaguardando todo lo que se pueda de la *privacy*. "Si el secreto se ha vuelto imposible –conjetura Saviano– también la *privacy*, ingrediente sagrado para conservar la propia dignidad, corre el riesgo de quedar violada para siempre".

ANTONIO PASQUALI
Profesor Titular de la Universidad Central de Venezuela(UCV). Fundador del Instituto de Investigaciones de la Comunicación de la UCV (Ininco-UCV). Fue , por varios años, representante de Venezuela ante la Unesco.

Galería de Papel. *Sin título.* Félix Perdomo. (1995)