LA BÚSQUEDA DE LA CONFIANZA EN EL CIBERESPACIO

Unión Internacional de Telecomunicaciones

LA BÚSQUEDA DE LA CONFIANZA EN EL CIBERESPACIO

por el Dr. Hamadoun I. Touré

Secretario General de la

Unión Internacional de Telecomunicaciones

y del

Panel Permanente de Supervisión sobre

la Seguridad de la Información

Federación Mundial de Científicos

NOVIEMBRE DE 2014

Aviso legal

Los diferentes autores mantienen sus derechos de autor sobre su trabajo. Se citan fuentes de terceros, en caso necesario. La Unión Internacional de Telecomunicaciones (UIT) no se hace responsable del contenido procedente de fuentes externas, incluidos sitios web a los que se hace referencia en la presente publicación.

Ni la UIT ni ninguna persona que actúe en su nombre se hacen responsables de la utilización que pudiera hacerse de la información recogida en esta publicación.

Limitación de responsabilidad

Los capítulos de la presente publicación representan los puntos de vista de cada uno de los autores, que no cuentan necesariamente con la aprobación de la organización en la que están empleados o de la que son afiliados ni representan sus puntos de vista. La mención y las referencias relativas a países, empresas, productos, iniciativas o directivas particulares no implican en modo alguno que la UIT, los autores o toda otra organización en la que están empleados o de la que son afiliados, las refrenden o las recomienden con preferencia a otros países, empresas, productos, iniciativas o directivas similares no mencionados.

Agradecimientos

El Secretario General de la UIT y la Federación Mundial de Científicos (WFS) desean dar las gracias a Henning Wegener y a todos los autores que han contribuido a dar a conocer sus puntos de vista sobre este tema incipiente de interés mundial. El Secretario General también expresa su agradecimiento a Marco Obiso, que se encargó de dirigir y coordinar esta publicación, y al equipo de la UIT encargado de la ciberseguridad, en particular a Alex Gamero Garrido, Aliya Abdul Razack, Despoina Sareidaki, Anthony Drummond, Preetam Maloor y Rosheen Awotar-Mauree, así como a todos los colaboradores de la UIT y la WFS sin cuya contribución esta publicación no hubiera sido posible.

Los lectores que deseen formular algún comentario, pueden dirigirse al equipo Ciberseguridad de la Unión Internacional de Telecomunicaciones, en la siguiente página web: cybersecurity@itu.int

ÍNDICE

Página

Sobre la Unión Internacional de Telecomunicaciones

La Unión Internacional de Telecomunicaciones (UIT) es la organización más importante de las Naciones Unidas en lo que concierne a las cuestiones relativas a las Tecnologías de la Información y la Comunicación (TIC) y a la coordinación entre los gobiernos y el sector privado para el desarrollo de redes y servicios.

Tras la celebración de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y de la Conferencia de Plenipotenciarios de la UIT de 2006, una de las principales funciones de la UIT es la creación de confianza y seguridad en la utilización de las TIC. Los Jefes de Estado y de Gobierno y otros líderes mundiales que participaron en la CMSI, al igual que los Estados Miembros de la UIT, confiaron a esta organización la tarea de adoptar medidas concretas para reducir las amenazas e inseguridades relacionadas con la sociedad de la información. Para llevar a cabo su mandato, el Dr. Hamadoun I. Touré, Secretario General de la UIT, puso en marcha la Agenda sobre Ciberseguridad Global (GCA), marco de la cooperación internacional multipartita en materia de ciberseguridad, encaminada a establecer sinergias con los asociados actuales y futuros y a colaborar con iniciativas en vigor o previstas. Esa Agenda da prioridad a los cinco ámbitos de trabajo siguientes: medidas jurídicas, medidas técnicas y de procedimiento, estructuras organizativas, creación de capacidades y cooperación internacional.

Enumeramos también ciertas iniciativas fundamentales para ayudar a los Estados Miembros a crear capacidades en materia de ciberseguridad bajo la égida de la GCA y con el apoyo de asociados internacionales:

- El programa relativo a los CIRT (equipos de intervención en caso de incidente informático) nacionales, en virtud del cual se evalúan las actividades de esos equipos y su realización y se llevan a cabo ejercicios regionales de ciberseguridad en respuesta a la demanda de los Estados Miembros.
- El establecimiento de centros regionales de ciberseguridad cuya finalidad es acelerar y reforzar la cooperación, coordinación y colaboración regionales para afrontar el aumento de las ciberamenazas.
- El proyecto "Mejora de la ciberseguridad en los países menos adelantados", en el marco del cual la UIT ayuda a los PMA a reforzar sus capacidades, su preparación, sus aptitudes y sus conocimientos en materia de ciberseguridad.
- El Índice Mundial de Ciberseguridad (GCI), que mide el grado de desarrollo de la ciberseguridad en cada país, trata de ser el incentivo adecuado para que los países intensifiquen sus esfuerzos en materia de ciberseguridad. Su meta final es promover una cultura mundial de la ciberseguridad e integrarla como elemento fundamental de las tecnologías de la información y la comunicación.

Sobre la Federación Mundial de Científicos

La Federación Mundial de Científicos (WFS) fue fundada en Erice (Sicilia) en 1973 por un grupo de eminentes científicos dirigidos por Isidor Isaac Rabi y Antonino Zichichi. Desde entonces, otros numerosos científicos se han hecho miembros de la Federación, entre ellos T. D. Lee, Laura Fermi, Eugene Wigner, Paul Dirac y Piotr Kapitza.

La WFS es una asociación abierta a todos, que cuenta en la actualidad con más de 10 000 científicos de 110 países. Todos sus miembros tienen los mismos objetivos e ideales y adhieren voluntariamente a los principios de la Federación. La WFS promueve la colaboración internacional en ciencia y tecnología entre los científicos e investigadores de todas las regiones del mundo: Norte, Sud, Este y Oeste. La Federación y sus miembros persiguen el ideal del libre intercambio de información y procuran que los descubrimientos y avances científicos dejen de estar sólo al alcance de algunos. El objetivo es compartir los conocimientos con todos los habitantes del mundo, de manera que cada uno pueda beneficiarse de las ventajas del progreso científico.

La creación de la Federación Mundial de Científicos ha sido posible gracias a la existencia, en Erice, de un centro de cultura científica que lleva el nombre del físico Ettore Majorana, la ***Fundación y Centro de Cultura Científica Ettore Majorana*** (el Centro). Este Centro, que también se conoce como "Universidad del Tercer Milenio", se ha convertido en una entidad educativa mundial. Desde su fundación en 1963, el Centro ha organizado 123 escuelas y 1 497 cursos para 103 484 participantes (125 de los cuales han recibido el Premio Nobel), procedentes de 932 universidades y laboratorios de 140 países.

El Centro Ettore Majorana fue el precursor de la Federación Mundial de Científicos y sus actividades para hacer frente a situaciones de emergencia planetarias. La Federación Mundial de Científicos identificó rápidamente 15 categorías de **situaciones de emergencia planetarias** y empezó a organizar la lucha contra esas amenazas. Uno de sus mayores logros fue la elaboración en 1982 de la **Declaración de Erice**, redactada por Paul Dirac, Piotr Kapitza y Antonino Zichichi, en la que se establecen claramente los ideales de la Federación y se presenta una serie de propuestas para ponerlos en práctica. Otro hito en la historia de la Federación fue la celebración de una serie de seminarios internacionales sobre la guerra nuclear, que han resultado de gran eficacia para alejar el peligro de catástrofe nuclear a escala planetaria y que contribuyeron en último instancia a poner fin a la Guerra Fría. En 1986, por iniciativa de un grupo de eminentes científicos (la mayoría de los ellos, miembros de la WFS)

se fundó en Ginebra el **Laboratorio Mundial del Centro Internacional de Cultura Científica** para contribuir a lograr los objetivos enunciados en la Declaración de Erice.

En 2001, la WFS creó su Panel Permanente de Supervisión (PMP) sobre la Seguridad de la Información. Su Informe, *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar* ("Hacia un orden universal en el ciberespacio: Gestión de las amenazas, desde el ciberdelito hasta la ciberguerra") fue uno de los documentos más importantes presentados por la sociedad civil a la Cumbre de Mundial sobre la Sociedad de la Información (CMSI) de las Naciones Unidas, que se celebró por primera vez en Ginebra en 2003. El PMP ha publicado numerosos artículos sobre ciberseguridad y ciberguerra, y presenta periódicamente cuestiones vinculadas a la seguridad de la información, considerado un tema esencial en materia de situaciones de emergencia planetarias, en las sesiones plenarias de la WFS, celebradas en Erice cada año en el mes de agosto. En agosto de 2009, el PMP estaba tan inquieto ante el peligro que podría representar una ciberguerra para la sociedad y los daños y sufrimientos innecesarios que podía causar que elaboró la **Declaración de Erice sobre los Principios de la paz y la estabilidad en el ciberespacio**, adoptada por la Plenaria de la WFS con ocasión de la 42ª sesión de Seminarios Internacionales sobre situaciones de emergencia planetarias, que tuvo lugar en Erice el 20 de agosto de 2009.

Esa Declaración, que ha sido distribuida a todos los Estados Miembros de las Naciones Unidas, se puede consultar, así como otras declaraciones y publicaciones y otros documentos internos del Panel Permanente de Supervisión sobre la Seguridad de la Información, en la siguiente página web: www.unibw.de/infosecur.

El PMP está presidido por el Embajador Henning Wegener. Los miembros de ese Panel que han contribuido a la presente publicación son los siguientes:

Miembros del PMP autores de contribuciones

Mona Al-Achkar

La Sra. Mona Al-Achkar Jabbour, que tiene un doctorado (PhD) en derecho privado, dirigió los departamentos jurídicos y de investigación de la Universidad del Líbano de 1998 y 2009. Ha sido también consultora para la puesta en servicio de la base de datos jurídicos del Ministerio de Justicia de Kuwait, que se encargó además de supervisar.

Actualmente es profesora de derecho de la Facultad de Derecho del Líbano, profesora encargada de investigaciones en el Centro de Informática Jurídica de la Universidad del Líbano, fundadora y Presidenta de la Asociación libanesa de Tecnologías de la Información (LITA), fundadora del Centro libanés de lucha contra el ciberdelito, miembro y fundadora del Observatorio panárabe para la ciberseguridad y miembro de Online Arab writers, de la Federación árabe de arbitraje en línea, del Comité jurídico

para la protección de la infancia en línea en el Ministerio de Asuntos Sociales del Líbano, del "equipo francófono" de la ICANN y el FGI, del Centro Internet Libanés (LINC) y del Panel Permanente de Supervisión sobre la Seguridad de la Información de la Federación Mundial de Científicos.

La Sra. Al-Achkar ha publicado numerosos libros y artículos sobre diversas cuestiones jurídicas, algunas de ellas relativas a la informática jurídica y el derecho del ciberespacio, el blanqueo de dinero y el terrorismo.

William Barletta

William Barletta es profesor adjunto de física en el Instituto de Tecnología de Massachusetts (MIT) y en la Universidad de California-Los Ángeles (UCLA), y profesor invitado de la Facultad de Economía de la Universidad de Ljubljana. Es también Director de la United States Particle Accelerator School y la Korean Particle Accelerator School. Es asimismo coordinador y editor en jefe de la revista Nuclear Instruments and Methods. Ocupa además el cargo de Asesor principal del Presidente de Sincrotrone Trieste (Italia). Copreside el Panel Permanente de Supervisión (PMP) sobre Energía de la Federación Mundial de Científicos y es miembro del Panel Permanente de Supervisión sobre la Seguridad de la Información. Es Presidente electo del Panel sobre Asuntos Públicos de la Asociación Americana de Física (APS, American Physical Society) y ha sido Presidente del Foro sobre Física Internacional y la División de Física de Haces. Es miembro activo del Comité de la APS para cuestiones científicas internacionales.

Es editor de cuatro libros sobre la ciencia de los aceleradores y coautor de cuatro libros relativos a la ciberseguridad, al respeto de la vida privada y al derecho internacional del ciberespacio. Es asimismo titular de cuatro patentes y autor de más de 170 artículos científicos. Tiene un doctorado en Física de la Universidad de Chicago.

Pavan Duggal

Pavan Duggal es reconocido como uno de los cuatro juristas especializados en el ciberespacio más importantes del mundo. Sus actividades en calidad de experto en derecho del ciberespacio y del comercio electrónico, y su autoridad en la materia, han alcanzado un importante reconocimiento internacional.

Pavan Duggal es abogado de la Corte Suprema de la India. Ha sido autor de trabajos innovadores sobre derecho de la convergencia y derecho de las comunicaciones móviles. Al respecto, trabaja como consultor de la UNCTAD y la CESPAP para cuestiones relativas al derecho del ciberespacio y al ciberdelito, respectivamente. También es miembro del Grupo de trabajo jurídico AFACT de UN/CEFAT, consultor experto en ciberdelito para el Consejo de Europa y miembro de la Junta de expertos

sobre comercio electrónico de la Comisión Europea. Sus actividades de experto en derecho del ciberespacio para el Grupo Especial e-ASEAN y de colaborador especial del Banco Asiático de Desarrollo dan muestra de su autoridad en estas cuestiones y de su reconocimiento a escala mundial. Asimismo, es Presidente de Cyberlaw Asia & Cyberlaws.Net.

El Sr. Duggal ha hecho uso de la palabra en más de 1 200 conferencias, seminarios y talleres, y es autor de 42 libros publicados en los últimos años sobre diversos aspectos del derecho indicados anteriormente.

Para una información más completa sobre Pavan Duggal, consultar la siguiente página web: http://www.linkedin.com/in/pavanduggal.

Solange Ghernaouti

Solange Ghernaouti, Doctora en Informática (Universidad de París), es Profesora de la Universidad de Lausana y dirige el Swiss Cybersecurity Advisory and Research Group. Es una experta reconocida internacionalmente en cuestiones vinculadas a la ciberseguridad, la ciberdefensa, el ciberdelito y el control de los riesgos planteados por las TIC. Ha contribuido a varias iniciativas formuladas por organizaciones internacionales, instituciones públicas y privadas, centros de investigación y órganos encargados del cumplimiento de la ley, entre otras instancias del mundo entero. Sus principales trabajos en esos ámbitos se centran ante todo desde hace varios años en la instauración de una ciberseguridad interdisciplinaria e integradora, tanto para los ciudadanos como para las organizaciones y los Estados.

La Sra. Ghernaouti es asesora independiente en cuestiones de seguridad. Sus análisis son sumamente valorados e interviene periódicamente en los medios. Ha sido reconocida por la prensa suiza como una de las mujeres más destacadas en los medios profesionales y académicos. Ha recibido la distinción de Caballero de la Legión de Honor y es miembro de la Academia suiza de Ciencias Naturales. Es autora de más de 300 publicaciones y 28 libros, entre ellos, "Cyberpower: Crime, Conflict and Security in Cyberspace" (EPFL Press 2013), y en colaboración con Judge Schjølberg, "A Global Treaty on Cybersecurity and Cybercrime – A contribution for peace, justice and security in cyberspace" (Cybercrimedata, 2009). Es además miembro del Panel Permanente de Supervisión sobre la Seguridad de la Información de la Federación Mundial de Científicos.

Para una información más completa, consultar la siguiente página web: www.scarg.org

Gabor Iklody

Gabor Iklody ocupa actualmente el cargo de Director de la Gestión y Planificación de Crisis en el Servicio Europeo de Acción Exterior (SEAE) de la Unión Europea en Bruselas. Anteriormente, en calidad de Secretario General adjunto de la OTAN para problemas de seguridad emergentes, creó y dirigió en esa organización la División más reciente encargada de problemas de seguridad no tradicionales como, por ejemplo, la ciberdefensa, el contraterrorismo, la no proliferación de armas de destrucción masiva y la seguridad energética, así como la política nuclear y el análisis estratégico. Presidió además la Junta de Gestión de la Ciberdefensa (CDMB) de la OTAN.

Antes de cumplir funciones internacionales, el Sr. Iklody trabajó durante casi 30 años en el Ministerio de Asuntos Extranjeros de Hungría, ocupando recientemente el cargo de Director Político y de Secretario de Estado encargado de asuntos multilaterales y de seguridad. Fue Embajador en Escandinavia durante dos mandatos de cuatro años, primero en Noruega (1999-2003) y luego en Suecia (2005-2009). Consagró gran parte de su carrera a la integración euroatlántica, la diplomacia multilateral y el control de armamentos.

Danil Kerimi

Danil Kerimi está encargado de elaborar el programa tecnológico, definir la estrategia de comunicación con el sector público en el mundo y reunir diversas iniciativas vinculadas a las TIC con miras a constituir una plataforma hiperconectada (ciberseguridad, datos, tecnología al servicio de la humanidad, TIC para la competitividad, gobernanza de Internet) para el Foro Económico Mundial (WEF). Supervisa la participación de altos dirigentes del sector público y privado, de expertos del conocimiento y de la sociedad civil en los proyectos del Foro sobre las TIC. Asimismo, el Sr. Kerimi es responsable del Global Agenda Council on Cyber Security y del Informe anual del WEF sobre tecnologías de la información mundiales (*Annual Global Information Technology Report*). Antes de trabajar en el WEF, ha ocupado diversos cargos de responsabilidad en las Naciones Unidas, la Organización para la Cooperación y la Seguridad en Europa, la Organización Internacional para las Migraciones y otros organismos internacionales importantes.

Axel Lehmann

Axel Lehmann es profesor emérito en el Departamento de Informática de la Universidad de las Fuerzas Armadas en Múnich (Universität der Bundeswehr München) (Alemania), donde ha ocupado una cátedra de modelización y simulación hasta 2011. En la actualidad es Director Ejecutivo del Instituto de Investigación para Sistemas Inteligentes (ITIS) de esa Universidad. Sus principales esferas de investigación

son variadas: modelización y simulación informática, aplicación de sistemas fundados en el conocimiento para el diagnóstico y apoyo a la toma de decisiones, concepción de arquitecturas informáticas innovadoras. Fue Presidente de la Society for Modelling and Simulation International. Es miembro de la Sociedad alemana de Informática y de la Federation of Asian Simulation Societies. Es miembro además del comité de redacción de varias revistas científicas especializadas en modelización y simulación, y miembro de diversas asociaciones internacionales y de normalización, así como de comités de examen, por ejemplo para la Unión Europea y la OTAN. Es por otra parte miembro del Panel Permanente de Supervisión sobre la Seguridad de la Información de la Federación Mundial de Científicos desde su creación en 2001.

Stefan Lüders

Stefan Lüders, titular de un doctorado, se graduó en la Escuela Politécnica Federal de Zürich. Comenzó a trabajar en el CERN en 2002. Autor de un sistema común de seguridad utilizado en cuatro experimentos efectuados en el marco del Gran Colisionador de Hadrones del CERN, ha adquirido una experiencia práctica en cuestiones de ciberseguridad relacionadas con los sistemas de control. En 2004, tuvo a su cargo la protección de los sistemas de control del acelerador y de las infraestructuras del CERN contra las ciberamenazas. Integró seguidamente el equipo de seguridad del CERN para intervenciones en caso de incidentes informáticos, que dirige actualmente en calidad de Director de Seguridad Informática, con el mandato de coordinar todos los aspectos de dicha seguridad: seguridad en las oficinas, seguridad del centro informático, seguridad de la red eléctrica y del sistema de control, teniendo en cuenta las necesidades operacionales del CERN. El Sr. Lüders ha hecho a menudo presentaciones sobre la seguridad informática y la ciberseguridad de los sistemas de control ante organismos internacionales, gobiernos y empresas. Ha publicado además varios artículos sobre esos temas.

Howard A. Schmidt

Howard A. Schmidt está actualmente asociado a Ridge-Schmidt Cyber, una empresa de servicios ejecutivos y asesoramiento estratégico que ayuda a dirigentes de empresas privadas y públicas a responder a las demandas crecientes en materia de ciberseguridad. Ocupa ese cargo junto a Tom Ridge, primer Secretario del Departamento de Seguridad Interior. Se desempeña además como Director Ejecutivo de Software Assurance Forum for Excellence in Code (SAFECode).

En más de 40 años de carrera, el Sr. Schmidt ha adquirido una serie de profundos conocimientos en economía, defensa, servicios de información, aplicación de la ley, cuestiones sobre confidencialidad, vida académica y relaciones internacionales. Ha ocupado recientemente el cargo de Asistente especial del Presidente y Coordinador de

la ciberseguridad para los Estados Unidos. Entre otras funciones desempeñadas en la Casa Blanca, ha sido Consejero en materia de seguridad de los Presidentes Barack Obama y George W. Bush.

Anteriormente, el Sr. Schmidt fue Presidente y Director General del Information Security Forum (ISF). Ha sido además Vicepresidente y Jefe de Seguridad de la Información, así como responsable de estrategias sobre seguridad para eBay Inc., tras haberse desempeñado como Jefe de Seguridad para Microsoft Corp. Asimismo, tuvo a su cargo las estrategias de seguridad para el programa US-CERT en el Departamento de Seguridad Interior.

El Sr. Schmidt tiene una licencia en Administración de empresas (BSBA) y una maestría en Gestión Institucional (MAOM) de la Universidad de Phoenix. Es también Doctor *honoris causa* (Honorary Doctorate degree in Humane Letters) y Adjunct Distinguished Fellow del CyLab de Carnegie Mellon, así como Distinguished Fellow del Ponemon Privacy Institute. Anteriormente fue miembro del Grupo Permanente de Interesados (PSG) de la European Union Agency for Network and Information Security (ENISA). Es actualmente profesor de Investigación en la Universidad del Estado de Idaho. También es miembro del Panel Permanente de Supervisión sobre la Seguridad de la Información de la Federación Mundial de Científicos.

El Sr. Schmidt es operador de radiocomunicaciones (W7HAS) y piloto privado, practica actividades al aire libre y es un aficionado a la Harley-Davidson. Está casado con Raemarie J. Schmidt, una especialista de la policía científica ya jubilada, investigadora y docente en informática forense. Son padres de familia y han tenido nietos.

Hamadoun I. Touré

El Dr. Hamadoun I. Touré, nombrado Secretario General de la UIT en enero de 2007, fue reelegido para un segundo mandato en octubre de 2010. Tiene una vasta experiencia profesional en el sector público y el sector privado.

Nacido en Malí, el Dr. Touré se ha empeñado en hacer de la UIT una organización innovadora y volcada al futuro que esté en condiciones de afrontar las dificultades planteadas por los rápidos cambios del entorno de las TIC, y a impulsarla a llevar a la práctica las resoluciones de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y los Objetivos de Desarrollo del Milenio (ODM).

El Dr. Touré está casado, tiene cuatro hijos y dos nietos.

Henning Wegener

Henning Wegener ha sido Embajador de Alemania. Ha ocupado además los cargos de Embajador para el Desarme en Ginebra (1981-1986), Secretario General Adjunto para Asuntos Políticos en la OTAN (1986-1991), Director General en la Cancillería Federal Alemana (1991-1994) y Embajador en España (1995-1999). Desde su creación en 2001, es Presidente del Panel Permanente de Supervisión sobre la Seguridad de la Información, del que ha sido copresidente de 2009 a 2012. Sus trabajos se han reunido en publicaciones en el ámbito de la política de seguridad y la política extranjera, incluida la ciberseguridad. El Sr. Wegener es miembro del Capítulo Español del Club de Roma y participa en los consejos de administración de varias fundaciones. Entre otros títulos, el Sr. Wegener es Doctor en Ciencias Jurídicas de la Yale Law School. henningwegener@hotmail.com.

Prefacio del Secretario General de la UIT, Dr. Hamadoun I. Touré

La presente publicación está consagrada a una tarea que adquiere cada vez más enormes proporciones: instaurar la confianza en la utilización de plataformas y tecnologías del ciberespacio, en un contexto de violaciones de la seguridad, de las que se ha hablado mucho últimamente, y de una plétora de nuevas amenazas que afectan la confianza depositada en esos medios esenciales en nuestra vida.

Sigue en la misma línea que otra publicación presentada en 2009, *La búsqueda de la paz en el ciberespacio,* centrada en la promoción de la paz en el ciberespacio en una esfera que ha generado enormes ventajas y progresos para la humanidad, pero que ha dado también lugar a actividades delictivas y ha creado nuevas vías para la recopilación de información, el espionaje industrial y los conflictos.

La presente publicación retoma necesariamente esas cuestiones que giran en torno al tema general de la utilización del ciberespacio al servicio del bien o del mal, en particular en lo que respecta a las repercusiones del "lado oscuro" de Internet en la confianza en el ciberespacio (o ciberconfianza). Aquí, no obstante, el tema central es el concepto de ciberconfianza. Como se indica en la Introducción, ya no es exagerado hablar de "crisis de confianza" en el ciberspacio. De hecho, un análisis de las tendencias más recientes muestra que la convergencia de varios acontecimientos ha incidido negativamente en la ciberconfianza. A título de ejemplo, la creciente militarización del ciberespacio y el surgimiento de capacidades militares ofensivas que no sólo apuntan a objetivos militares sino también, a la vez, a infraestructuras civiles esenciales, son particularmente preocupantes. La elaboración del concepto de ciberespacio respondía a la necesidad de contribuir a frenar esa evolución. Reviste una importancia incluso mayor el número sin precedentes de casos de espionaje digital y de violaciones al respeto de la vida privada en el ciberespacio que ha comenzado a preocupar seriamente a la opinión pública.

A lo largo de esta publicación, los autores evocan, desde diversos ángulos, el conjunto de motivos que explican la erosión de la confianza, los analizan y elaboran estrategias para combatirlos. Para ello, dan prioridad a tres ámbitos que consideran decisivos para restablecer e instaurar la confianza: 1) formulación de *políticas normativas y marcos reglamentarios* específicamente aplicables a la era digital; 2) reforzamiento de la *resiliencia* ante los numerosísimos casos de utilización indebida del ciberespacio; y 3) garantía de las *libertades* fundamentales, como la libertad de acceso y la libertad de expresión en el ciberespacio. En estos tres ámbitos, los autores describen y evalúan las iniciativas en curso a escala mundial, regional y nacional para alcanzar esos objetivos.

La presente publicación es un llamamiento ferviente a la acción para tratar de resolver estos problemas, y presenta poderosos argumentos al respecto. Como la publicación que la precede, *La búsqueda de la paz en el ciberespacio*, ha contado con el apoyo de la Federación Mundial de Científicos y la Unión Internacional de Telecomunicaciones, organizaciones que están a la vanguardia de esta iniciativa.

Prefacio del Presidente de la Federación Mundial de Científicos, profesor Antonino Zichichi

En los albores del Tercer Milenio, la ciencia es más que nunca el factor determinante del cambio y la evolución histórica. Gracias a ella, la humanidad puede explorar más a fondo el funcionamiento y los secretos del universo. En el curso de ese proceso, sistemas ya complejos adquieren aún mayor complejidad. Se observan nuevas formas de interacción entre los seres humanos y su entorno: las relaciones entre la mente y la máquina, en plena evolución, deben replantearse. Entramos en un periodo de descubrimientos, pero también de retos sin precedentes.

Las tecnologías digitales cumplen una función en la ciencia y las ciencias aplicadas. Esas tecnologías y sus herramientas son omnipresentes, trazan una curva de crecimiento espectacular del conocimiento existente y proponen dispositivos y sistemas de control aplicables a prácticamente todas las actividades humanas. Las aplicaciones informáticas especializadas; la computación distribuida, en redes y en la nube, fundadas en infraestructuras de información sumamente desarrolladas; la evolución de la microelectrónica y los nuevos sensores; el universo de la interconectividad, a menudo automático, de una miríada de dispositivos digitales y la rápida transformación de los procesos de fabricación, son algunas de las principales características de esta nueva era.

Lejos de la intención de enumerar las ventajas y posibilidades innumerables de la era digital, en mi calidad de Presidente de la Federación Mundial de Científicos, quisiera insistir en la importancia de la ciencia y la evolución de la tecnología digital para promover la paz y afrontar las emergencias planetarias, tarea que depende de la recopilación de datos en tiempo real a los fines de la prevención, la intervención, la recuperación y el restablecimiento. En este sentido, soy plenamente consciente de la responsabilidad moral de los científicos.

El ciberespacio no conoce fronteras; su omnipresencia ha modificado nuestra percepción del mundo y reducido drásticamente la distancia y el tiempo. La ambigüedad inherente a las cibertecnologías, como a todas las tecnologías modernas, es decir, su posible utilización al servicio del bien o del mal, adquiere dimensiones mundiales. El ciberespacio es un ámbito que abre inmensas posibilidades, pero donde los daños se agravan debido a la ausencia de marcos reglamentarios sólidos y adecuados en todo el mundo. La utilización hostil de las tecnologías digitales es cada vez más amenazadora. La ciberseguridad y la protección de los datos son componentes aún más cruciales de la gestión de los riesgos digitales. Son ahora un aspecto fundamental de la revolución digital y deben constituir un sector verdaderamente propicio para poner freno a esas amenazas.

Hace más de diez años que la Federación Mundial de Científicos y su grupo multidisciplinario sobre la seguridad de la información trabajan en este sentido. En una publicación anterior, *La búsqueda de la paz en el ciberespacio*, realizada en colaboración con el Secretario General de la UIT, se hacía hincapié en la utilización segura y pacífica de las tecnologías digitales. En la publicación que hoy presentamos se aborda otro aspecto fundamental de una sociedad digital funcional: la confianza. Los usuarios, y la sociedad en su conjunto, no sólo deben estar seguros de que la tecnología funciona sin dificultades, sino además tener confianza en la integridad y la confidencialidad de los datos y dispositivos digitales, así como de las infraestructuras de las redes subyacentes. La mutua confianza es indispensable para una cooperación útil y durable. En el ciberespacio y en una sociedad de la información cada vez más conectada, la confianza adquiere una relevancia decisiva. Refuerza la eficacia y productividad de las interacciones internacionales, puesto que en ella se apoyan las expectativas mutuas de buena fe y reciprocidad. Quiero expresar mi reconocimiento al Dr. Touré, Secretario General de la UIT, y a los coautores de esta publicación, que han sabido evocar las numerosas dimensiones de la confianza en el ciberespacio y formular las recomendaciones convenientes.

Introducción: La crisis de la confianza en el ciberespacio

por Henning Wegener

Hace tres años, el Secretario General de la UIT y los miembros del Panel Permanente de Supervisión sobre la Seguridad de la Información de la Federación Mundial de Científicos publicaron *La búsqueda de la paz en el ciberespacio*[1], que alertaba contra la proliferación de peligros en el ciberespacio y exhortaba a todos los interesados a aunar sus esfuerzos para asegurar la adecuada estabilidad de Internet y las estructuras digitales y hacer avanzar el concepto de paz mundial en el ciberespacio. Esa publicación, deliberadamente concisa y que ponía de manifiesto un vasto debate público de actualidad, no ha envejecido. Sus autores, en general los mismos que los de la presente publicación, son fieles a los análisis y recomendaciones que formularon en ese momento.

No obstante, la situación se ha agravado desde entonces y no es exagerado hablar de una nueva dimensión de amenazas en el ciberespacio que evolucionan ante nuestros ojos. La publicación anterior daba particular prioridad a la perspectiva inquietante de un ciberconflicto o una ciberguerra. Esas amenazas, lejos de desaparecer, están aún más presentes. Por ello, el ciberconflicto ocupa un lugar importante en la presente publicación, estableciendo de esa forma una clara continuidad entre ambos títulos. Sin embargo, los temas de las contribuciones reunidas en esta publicación han evolucionado al mismo ritmo que las amenazas. El tema central es ahora el concepto de confianza en el ciberespacio (o ciberconfianza), y su finalidad analizar las tendencias que la socavan, así como las estrategias y técnicas necesarias para restablecerla[2].

---

1 *La búsqueda de la paz en el ciberespacio*, Unión Internacional de Telecomunicaciones y Federación Mundial de Científicos, Ginebra, enero de 2011.

2 Con el fin de demostrar la continuidad entre las dos publicaciones, el título elegido es *La búsqueda de la confianza en el ciberespacio*. Con todo, el término *búsqueda* no tiene el mismo significado en ambos casos. En la primera publicación, expresa la aspiración a un estado de paz aún no alcanzado; en la segunda, la idea de confianza ya existe pero ha sido gravemente socavada y, por tanto, conviene restablecerla y reforzarla.

El concepto de confianza, condición esencial del funcionamiento de una sociedad de la información fundada en la tecnología digital, no tiene nada de nuevo. Cuando se consultan los documentos adoptados en la Cumbre Mundial sobre la Sociedad de la Información (CMSI), en sus dos fases de 2003 y 2005, se observa inmediatamente que el concepto de confianza es el hilo conductor de esos textos y recomendaciones. "La confianza y la seguridad son unos de los pilares más importantes de la Sociedad de la Información", leemos, y "Creación de confianza y seguridad" es la tarea principal de la Línea de Acción C5 de la CMSI.

En el curso de los debates posteriores a la celebración de la CMSI, el Informe del facilitador para la Línea de Acción C5, publicado en 2014, indica como principal preocupación (extraído del Resumen analítico): "Fortalecimiento del marco de confianza: Aumentar la confianza en los dispositivos digitales, en la ciberseguridad, y crear un entorno de confianza entre organizaciones del sector público y el sector privado, son tareas fundamentales. Se debe mejorar el grado de confianza de los ciudadanos en los servicios digitales e Internet."[3]

Dado que la confianza es un elemento central de la sociedad de la información, es evidente que influye en todos los aspectos del universo digital. Por ese motivo, aunque el tema de la publicación *La búsqueda de la paz en el ciberespacio* es diferente, el texto presenta un análisis a fondo del concepto de confianza y de su omnipresencia en la sociedad[4]. El autor afirma: "La confianza y la fiabilidad son conceptos básicos de la existencia humana", que sustentan todas las relaciones sociales y permiten afrontar numerosas incertidumbres y la complejidad de la vida contemporánea, y por tanto reducir los riesgos percibidos. En su análisis presenta un panorama general de los trabajos anteriores sobre el concepto central de vida social. Puesto que la publicación sigue estando a disposición del público, nos limitamos a citarla como referencia general[5].

En inglés, los términos "trust" y "confidence" (traducidos por "confianza" en español) son en gran medida sinónimos, pero "trust" alude más a las relaciones entre las personas, en tanto que "confidence" se aplica ante todo a las relaciones entre las personas y una entidad que no es humana o una institución. Para el tema que nos ocupa, esta última acepción comprende dispositivos y productos digitales, como

---

3 Doc. WSIS+10/4/2.

4 Jacques Bus, Necesidad de confianza – El concepto de confianza y su función en la sociedad, "*La búsqueda de la paz en el ciberespacio*", p. 17.

5 Los principales autores citados son O'Hara, Luhmann, Hardin y Fukuyama.

equipos, programas informáticos, redes, infraestructuras, aplicaciones y procedimientos de tratamiento. Por consiguiente, la presente publicación aborda principalmente la confianza ("confidence") sin olvidar no obstante las expectativas y percepciones personales inherentes al término "trust".

Como ya se ha indicado, la confianza es la condición esencial del funcionamiento del universo digital. Ahora bien, ciertos acontecimientos que han tenido repercusiones en ese universo en plena expansión han socavado seriamente esta confianza. No es exagerado hablar hoy de una crisis de la confianza en el ciberespacio.

Los factores que se han conjugado para generar esa crisis son los siguientes:

- Preocupa cada vez más la militarización del ciberespacio y el hecho de que un número creciente de Estados refuercen sus capacidades militares ofensivas, que no sólo apuntan a objetivos militares sino también, en realidad, a infraestructuras civiles esenciales y a los modos de vida de la población civil, lo que entraña repercusiones incontrolables y podría dar lugar al comienzo de una carrera de armamentos digitales. Más de un centenar de Estados refuerzan actualmente sus capacidades de ataque digital y participan en un juego desenfrenado y cada vez más peligroso de reciprocidad estratégica, en el cual la utilización perniciosa de las capacidades TIC se anuncia claramente en doctrinas que sirven a objetivos militares y políticos. Esas preocupaciones no excluyen el recurso a la autodefensa cuando es legítima y necesaria.

- Si bien es primordial adaptar el derecho internacional a la era digital y definir los límites de la utilización hostil de las tecnologías digitales, es inquietante que, en lugar de promover la paz en el ciberespacio, los esfuerzos desplegados en la actualidad para elaborar herramientas normativas legitiman la integración a gran escala de las ciberarmas en los arsenales militares de los Estados, incorporando de esa manera su implantación operacional en el marco normal de la planificación estratégica.

- Es incesante el temor de que infraestructuras civiles de vital importancia sean atacadas por los Estados u otros actores que no son Estados, con el pretexto de actividades militares legítimas o con fines delictivos.

- La incertitud relativa a las reglas y normas de comportamiento que podrían aplicarse a todos esos sucesos y servir de criterios de referencia contribuirían a poner fin a los daños y a restablecer la ciberconfianza. Esas incertitudes se agravan aún más debido al fracaso, en los últimos diez años, de la labor normativa que no ha conseguido elaborar códigos universalmente armonizados aplicables a gran escala.

- La complejidad creciente del entorno técnico, de grandes posibilidades pero también más vulnerable y expuesto a consecuencias imprevisibles en un universo interconectado. Los miedos son alimentados por varios factores: crecimiento exponencial de dispositivos digitales; nuevas situaciones de vulnerabilidad debidas a la utilización incesante de aplicaciones por los usuarios digitales; problemas de seguridad causados por el paso a aplicaciones móviles y a aplicaciones en la nube; aumento alarmante de nuevos componentes de software perniciosos[6]; aumento del ciberdelito, que cuesta fortunas a las economías nacionales, a las empresas y a los particulares; surgimiento de organizaciones criminales cada vez más poderosas y que operan a escala internacional, con capacidades y posibilidades de actuar como mercenarios en caso de ciberdelito o ciberconflicto. Como ya se ha indicado, estos acontecimientos en su conjunto representan una nueva dimensión y un salto cualitativo de las ciberamenazas, y pueden socavar aún más la confianza en el ciberespacio.

- Las incertitudes que persisten con respecto a la gobernanza de Internet conducen a plantearse interrogantes sobre las posibilidades de mantener "una red mundial, interoperativa, resistente, estable, descentralizada, segura e interconectada, accesible a todos"[7].

- La multiplicación de obstáculos contra el ejercicio de los derechos humanos por la red debido a la censura generalizada ejercida por ciertos gobiernos sobre el acceso y los contenidos (ciberrepresión) en un número creciente de países.

- Quizá lo más importante, y que se ha convertido en un tema candente de actualidad, es que asistimos al surgimiento de intrusiones ilimitadas, sin control técnico, en los sistemas digitales, a través de la búsqueda de *Big Data*. Esto ha llevado al aumento sin precedentes del espionaje industrial digital, así como del espionaje en masa, incontrolado y a menudo aparentemente infundado, puesto en práctica por los servicios de inteligencia de ciertos

---

6 En el momento de redactar este texto, cada vez es más frecuente que se descubran situaciones de vulnerabilidad importantes y que surjan nuevas amenazas. A título de ejemplo, tras el descubrimiento de la falla Heartbleed en abril de 2014, el rápido surgimiento del virus Shellshock, descrito como una "amenaza mortal" que podría infectar más de 500 millones de máquinas.

7 Declaración Multipartita de NETmundial, 24 de abril de 2014.

> Estados, que no siempre se limita al ámbito nacional y viola inescrupulosamente la soberanía y el orden jurídico de otros países[8].

No cabe ninguna duda que el restablecimiento de la confianza es un reto que todos los interesados en el mundo digital deben afrontar, y esperamos que la presente publicación contribuya a ese fin, en colaboración con otras instituciones y organizaciones que persiguen el mismo objetivo de restaurar la confianza de manera concertada y equilibrada[9].

El criterio adoptado en la presente publicación consiste en dar prioridad a tres esferas problemáticas que es importante abordar de inmediato para restablecer la confianza en el ciberespacio, y que ya han sido objeto de intensos debates públicos.

El lector de esos tres capítulos debe tener en cuenta que la presente publicación no es un manual ni un tratado destinado a examinar en detalle un tema complejo o a formular un opinión única y fuente de autoridad sobre todos los aspectos que conlleva. Está estructurada de tal forma que combina diversos textos redactados por la UIT y contribuciones presentadas por miembros de la Federación Mundial de Científicos, que se expresan a título personal. Al margen del Aviso legal y la Limitación de responsabilidad que figuran al comienzo de la publicación, conviene señalar que los editores han impulsado deliberadamente la presentación de diversas perspectivas para enriquecer el debate procurando al mismo tiempo que las opiniones expresadas sean compatibles.

La primera parte contempla la búsqueda de un marco normativo exhaustivo que regule el comportamiento en el ciberespacio y lo haga más previsible y cuantificable. Describe en particular las actividades internacionales encaminadas a elaborar, hacer aceptar y poner en práctica medidas de fomento de la confianza y códigos de conducta, así como otras herramientas jurídicas más amplias destinadas a aumentar la ciberconfianza, en términos de armonización de disposiciones jurídicas y de cooperación en lo que concierne al cumplimiento de la ley en el plano internacional. La finalidad de esta tarea es trazar el camino a seguir para lograr, de manera

---

8 Sobre la importancia de la confianza en esta esfera, véase Leif-Eric Easley, *Spying on Allies,* SURVIVAL, Vol. 56 número 4, agosto-septiembre de 2014, p. 141.

9 Recientemente, en conferencias internacionales a las que asistieron numerosos participantes se trató el tema de la confianza, por ejemplo en la Segunda Cumbre sobre Ciberseguridad, organizada por la Munich Security Conference and Deutsche Telekom, en Bonn en noviembre de 2013, en la que participó y pronunció un discurso Howard A. Schmidt, uno de los autores de esta publicación.

progresiva pero sistemática, un consenso internacional y nacional en la esfera normativa.

La segunda parte trata de la ciberdefensa y la capacidad de los sistemas digitales de resistir a los ataques y conflictos, así como los medios de reducir los puntos vulnerables, atenuar los efectos de los ataques o suprimirlos, o restablecer las capacidades de los sistemas dañados a causa de ataques, o de perturbaciones debidas a fallos, errores y fracasos en el ciberespacio. El término clave al respecto es resiliencia[10]. Tras un análisis de las amenazas actuales o previsibles, ese capítulo describe una amplia variedad de técnicas y estrategias que, utilizadas en conjunto, pueden inclinar la balanza hacia el éxito de tácticas de defensa, en el marco del violento enfrentamiento que las opone desde hace tiempo a las tácticas de ataque y que vuelven a ponerse en juego ante nuestros ojos en el universo digital.

El último capítulo examina la manera de conciliar la libertad de Internet – y de todas las demás comunicaciones digitales – y las injerencias de origen gubernamental; en otras palabras, conciliar el respeto de la vida privada en el universo digital y la seguridad del Estado. ¿Es cierto que "ya no existe el respeto de la vida privada" a raíz de los innumerables medios técnicos que permiten espiar impunemente todo sitio de almacenamiento de datos, sea particular o de una empresa? En ese capítulo se trata de arrojar luz al alcance de las actividades legítimas de vigilancia llevadas a cabo por los servicios de inteligencia extranjeros y nacionales, y de los fundamentos jurídicos – en particular si pertenecen a países distintos de los que organizan esa vigilancia – que autorizan actividades de esa envergadura. Se analizan además las posibles sanciones contra ese tipo de prácticas abusivas. Es de esperar que ese texto contribuya a la adopción de un marco concertado de medidas vinculantes que concilien las inquietudes legítimas en materia de seguridad y los derechos fundamentales, la validez de las legislaciones nacionales que aseguran la protección y seguridad de los datos, y el concepto fundamental de libertad de Internet. Este tema candente, como el de la censura ilegítima de Internet por los gobiernos, debe ser examinado más a fondo desde una perspectiva internacional.

Como es natural, el propósito general de la presente publicación es evitar que la erosión de la confianza en el ciberespacio se agrave y restablecer esa confianza de manera eficaz y perdurable. Debemos resolver la crisis de la ciberconfianza.

---

10 La resiliencia, capacidad de resistir a la adversidad, de perseverar y de restablecer el estado o situación anterior, es más que la suma de ajustes técnicos. Este término entraña también la idea de solidez general, en oposición a la fragilidad, de los sistemas en el tiempo. Véase Dhruva Jaishankar, *Resilience and the Future Balance of Power,* Survival, vol. 56, p. 217, junio-julio de 2014.

Capítulo I: Cibernormas

Introducción

Este capítulo traza un panorama general de las tareas que se están llevando a cabo para definir una serie de normas, principios y prácticas óptimas en materia de ciberseguridad a escala internacional y de las dificultades que ello plantea. Las nuevas amenazas, como el espionaje o los ataques similares a actos de guerra, y las peculiaridades de Internet (red transnacional de naturaleza técnica que supone numerosos interesados) lleva a que los Estados encuentran en el ciberespacio un terreno inhabitual: los gobiernos nacionales afrontan una situación de la que apenas tienen control, pero que les obliga a proteger a sus ciudadanos, en particular en el plano de los derechos humanos. Se realizan actualmente algunos esfuerzos, de forma exhaustiva a escala regional, pero más limitados a escala mundial, para establecer normas de base comunes encaminadas a lograr dicha protección.

La omnipresencia de las Tecnologías de la Información y la Comunicación (TIC) es incesante y su utilización aumenta de forma exponencial en los países desarrollados y los países en desarrollo. La confianza en la utilización de las TIC se conseguirá con la creación de TIC seguras y fiables. Sin embargo, varias tendencias actuales socavan esa confianza:

- el espionaje a gran escala a los fines de la seguridad nacional, facilitado por la gran disminución de los costos de la recogida y almacenamiento de datos personales;
- la utilización de códigos informáticos para actos similares a los actos de guerra que trascienden las fronteras nacionales;
- la presencia de un grupo aparentemente heterogéneo e incontrolable de personas malintencionadas, ya sean *spammers* o diseñadores de redes robot que alquilan sus servicios;
- las dificultades para procurar que los ciberdelincuentes den cuenta de sus actos cuando operan desde una jurisdicción diferente a la que está situado el sistema atacado.

Una respuesta eficaz a estos problemas complejos exige la cooperación transnacional. El presente capítulo describe los esfuerzos desplegados en este sentido, especialmente los que han realizado las organizaciones del sistema de las Naciones Unidas y otros organismos intergubernamentales, así como algunas recomendaciones básicas para concertar un acuerdo mundial sobre ciberseguridad. Las medidas de

fomento de la confianza, término utilizado por primera vez en los años de la Guerra Fría, constituyen un elemento central de esas iniciativas.

El presente capítulo se divide en cuatro secciones. En la primera, se destaca la necesidad de que los Estados se comprometan a adoptar medidas de fomento de la confianza, cuyos inconvenientes y posibles ventajas se describen. Se menciona además el enfoque adoptado por las Naciones Unidas con respecto a normas, reglas y principios en materia de ciberseguridad, comprendidos principios y recomendaciones para el futuro, y la aplicabilidad del derecho internacional a las TIC. En la tercera sección, consagrada a este último punto, se presenta una visión general de las similitudes entre los actores y los actos en el ciberespacio y en otros dominios de la guerra y el espionaje, así como una amplia serie de directrices para la elaboración de un instrumento internacional con valor de tratado en materia de ciberseguridad. Por último, en la cuarta sesión se describe la perspectiva de las Naciones Unidas con respecto a la ciberseguridad, haciendo hincapié en los mecanismos, ya establecidos o en proyecto, de los organismos especializados y en una visión a largo plazo del papel del sistema internacional en lo que concierne a la ciberseguridad y el ciberdelito.

Habría sido tentador – y, en cierta forma, necesario – incluir otra sección sobre gobernanza de Internet, dado que esta publicación considera que las incertitudes sobre el futuro de Internet figuran entre las causas evidentes de la erosión de la confianza en el ciberespacio. No obstante, el debate internacional en curso sobre la gobernanza, que no ha permitido aún superar posiciones gubernamentales divergentes, hace difícil para la UIT adoptar una firme opinión. Se puede sin embargo observar con satisfacción que los debates que han permitido recientemente la negociación de la Declaración Multisectorial, adoptada en la Conferencia NETmundial celebrada en Brasil en abril de 2014, han dado lugar a progresos tangibles y que, pese a que ese documento es voluntariamente no vinculante, se constata un inicio de consenso mundial sobre ciertas cuestiones de base. Debido a su carácter internacional, la UIT puede por cierto sostener todos los esfuerzos encaminados a lograr que Internet siga siendo "una red mundial, interoperativa, resistente, estable, descentralizada, segura e interconectada, accesible a todos" en tanto que espacio unificado y no fragmentado. En el mismo espíritu, puede respaldar la Declaración de la Conferencia NETmundial, según la cual "la vigilancia en masa y arbitraria socava la confianza en Internet y en el ecosistema de la gobernanza de Internet".

1.1 El papel de las medidas de fomento de la confianza en una nueva visión de la ciberseguridad internacional: perspectivas de una respuesta mundial y un tratado internacional

por Solange Ghernaouti

Confianza en el ciberespacio: una necesidad esencial

En apenas unos pocos años, Internet ha pasado a ser un elemento omnipresente y prácticamente indispensable de nuestra vida cotidiana. Nadie escapa a esta irrupción. Con los dispositivos inteligentes, se ha virtualizado un número creciente de servicios, incluidos los relativos a la salud y la medicina, la informática en la nube y la Internet de las Cosas. No podemos prescindir de ellos, nos habituamos a estar conectados permanentemente y a depender de las TIC. En la actualidad, Internet puede ser considerada una especie de prótesis digital y el ciberespacio, una prolongación "natural" de nuestro entorno. En tanto que factor de cambio y de la civilización, Internet estructura la sociedad de la información que construimos a escala mundial. Forma parte del proceso continuo de evolución y de la invención humana constitutiva de nuestra historia.

La adopción de las tecnologías digitales ha modificado profunda e irreversiblemente nuestros modos de comunicación, comportamiento, pensamiento, diversión, aprendizaje y transacciones económicas, así como la forma en que podemos ejercer influencia, desestabilizar o hacer daño, e incluso de vigilar, conducir una guerra o hacer cumplir la ley. La tecnología, por tanto, no es neutra, dado que se acompaña de cambios estructurales que nos afectan directamente.

Todos utilizamos la misma Internet, ya sea para aplicaciones privadas, personales y profesionales o para la salud, la energía, el abastecimiento, la cultura, e incluso la seguridad. Del esparcimiento a las finanzas, y para todos los sistemas de control de infraestructuras, de la información y de las telecomunicaciones esenciales, su utilización es inevitable.

Internet y todos sus accesorios han acelerado la dependencia de la sociedad, y en cierta manera de las personas, a la tecnología. Creamos y tratamos un volumen incesante de informaciones, de tráfico de datos y de interacciones. Consumimos cada vez más informaciones, recursos informáticos y energía y, en consecuencia, generamos cada vez más desechos.

Las tecnologías de la información constituyen pues el común denominador de todas las disciplinas y la memoria de nuestro patrimonio (patrimonio cultural digital, patrimonio digital de las empresas y los particulares). El conocimiento y la ciencia no pueden existir sin ellas. Conviene recordar por otra parte que los grandes principios fundadores de nuestra sociedad, como la democracia, la identidad individual y la soberanía del Estado, dependen también hasta cierto punto de esas tecnologías, que mal utilizadas o pirateadas pueden contribuir a desestabilizarla.

No hay que olvidar tampoco el papel que los medios sociales y las diversas herramientas de comunicación en Internet pueden cumplir en el marco de estrategias destinadas a ejercer influencia, si son impulsadas por Estados, grupos de presión o grupos terroristas o criminales. Si se la utiliza para destruir una reputación, influir en personas, multitudes y dirigentes, desinformar y manipular la opinión, Internet se transforma en un verdadero campo de batalla de la información. Al mismo tiempo, gracias a las tecnologías de la información, organizaciones malintencionadas o criminales pueden dar libre curso a su imaginación y emprender nuevas guerras en el ciberespacio, incluidas guerras de la información. Negar esta realidad supone exponerse innecesariamente al riesgo de perder competitividad económica, estabilidad, soberanía nacional o credibilidad internacional. Los medios, del mismo modo que los especialistas en la materia, señalan una serie interminable de casos de empresas víctimas de robos de datos a gran escala, ciberataques o secuestros de información, para cuya devolución se exige el pago de un rescate.

La confianza en el ciberespacio es por tanto fundamental, no sólo en relación con las infraestructuras TIC, los servicios ofrecidos y las informaciones tratadas, sino también para su seguridad.

Por encima de su complejidad, el ciberespacio modifica el concepto de territorios que deben protegerse

El mundo actual es un universo complejo y globalizado, dominado ante todo por la utilización intensiva de dispositivos, infraestructuras y servicios TIC. La dependencia de esas infraestructuras esenciales y su interdependencia exponen la sociedad a nuevos riesgos. Resulta cada vez más complejo asegurar, proteger y defender nuestras actividades fundamentales a nivel político, económico, social e individual. Asimismo, la interdependencia de los riesgos afecta negativamente el marco global de la resiliencia, tanto en el plano nacional como internacional. Si la ciberseguridad – se la llame así o seguridad de la información o seguridad digital – ha adquirido hoy tanta importancia, se debe a las preocupaciones que suscita en el plano político, económico, jurídico y tecnológico. Su gestión es pues determinante, y los diversos elementos que entraña la búsqueda de soluciones son complejos.

El ciberespacio es un ámbito a la vez virtual y real, que comprende tecnologías, servicios y datos Internet. Es un elemento del paisaje – al menos para las nuevas generaciones – del mismo modo que la tierra, el mar, el aire y el espacio, tan natural para nosotros como la electricidad. Algunos lo consideran un territorio dinámico en constante evolución, o un territorio a conquistar, dominar o controlar. Para otros, es un ámbito en el que se expresa o ejerce el poder, o una fuente de enriquecimiento personal o económico, legal o no, o un reducto de la libertad, o un campo de batalla. En realidad, constituye en mayor o menor medida un mosaico de todos esos elementos al mismo tiempo. Globalmente, pone de manifiesto nuestra realidad política, económica y social, y no es ni mejor ni peor que ella. Da cuenta de la realidad de la mundialización, de cuya unificación técnico-económica forma parte.

Aunque es difícil definir el concepto de territorio en un mundo hiperconectado, lo es aún más hacerlo en relación con la seguridad y la defensa de territorios digitales. Los modos tradicionales de pensar la seguridad no se aplican más. Debido a la evolución de las tecnologías (datos móviles, dispositivos inteligentes y la computación en la nube) y su utilización (redes sociales, pagos electrónicos, etc.), es imposible delimitar un perímetro de seguridad para aislar el entorno informático. La aplicación de técnicas criptográficas frena por lo general la integración de los servicios, dificulta la utilización y disminuye la calidad de funcionamiento. La criptografía sigue siendo poco utilizada y no inspira demasiada confianza. El caso "Heartbleed"[11] en abril de 2014 reveló la existencia de un fallo importante de seguridad en una de las opciones más utilizadas en los servicios web. Una vez más, el público tomó conciencia de la vulnerabilidad de los servicios que supuestamente mejoran la robustez de las infraestructuras y la seguridad de las transacciones electrónicas.

La fragilidad de la confianza

Con Internet, los particulares, las organizaciones y los Estados afrontan nuevas ciberamenazas y nuevos riesgos. El ciberespacio experimenta fallos y perturbaciones y está expuesto a delincuentes y agresores. Muy a menudo todavía, las ciberamenazas son insuficientemente reconocidas o malinterpretadas y, por tanto, dan miedo. Por otra parte, no se puede prever cuándo y cómo se harán realidad ni las reacciones en cadena o las secuencias de eventos que suscitarán, ni mucho menos identificar a los autores o a quienes se esconden detrás de ellos.

---

11 https://www.schneier.com/blog/archives/2014/04/heartbleed.html

Debido en particular a los casos WikiLeaks (2010)[12] y Prism (2013)[13], sabemos con certeza que, en el universo digital, el secreto no existe y que nos siguen, nos observan y nos vigilan a distancia por medios electrónicos. Tenemos que reconocer que esa vigilancia se ejerce a muy gran escala y que participamos activamente en ella mediante la utilización de ciertos servicios web o de nuestros teléfonos móviles. No podemos ignorar más que nuestros datos personales, nuestro comportamiento, nuestros gustos y nuestras relaciones constituyen el fundamento de modelos económicos adoptados por la mayoría de proveedores de servicios llamados "gratuitos" y que esa información despierta sumo interés.

En la actualidad, las capacidades de vigilancia de las tecnologías de la información y de sus proveedores entrañan en todo el mundo una crisis de confianza en esas tecnologías y en los principales actores del sector. Estamos tomando conciencia de la fragilidad de los entornos digitales y también de la fragilidad de nuestra confianza en las tecnologías y los profesionales de la ciberseguridad.

Restablecer la confianza en las infraestructuras TIC exige resolver las dificultades a diversos niveles:

- La dificultad de expresar nuestras necesidades en materia de ciberseguridad y de establecer los derechos y obligaciones de los diferentes actores, y de procurar que sean respetados.
- La dificultad de proteger a los ciudadanos, los consumidores, los niños, así como nuestro patrimonio digital y nuestros secretos.
- La dificultad de impedir los abusos y excesos en el ciberespacio y de gestionar los incidentes, y hasta las crisis, que podrían ocasionar.
- Las dificultades que tienen los particulares, las organizaciones y las autoridades de comprender las amenazas, identificar los riesgos y poner en práctica medidas eficaces para contrarrestarlas, incluida la dificultad de desbloquear los medios necesarios para combatir el ciberdelito.

---

12 http://www.theguardian.com/world/2010/nov/29/wikileaks-embassy-cables-key-points

13 http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/

Superar las dificultades e insuficiencias: identificar las necesidades reales

El ciberespacio presenta nuevos puntos vulnerables y una mayor diversidad de amenazas que pueden explotarlas. Las noticias nos lo recuerdan cada día al darnos información sobre robos de datos, pérdidas de control, secuestros de información para cuya devolución se exige el pago de un rescate, piratería de cuentas de correo electrónico, estafas de todo tipo y abusos de confianza. Términos como "piratas", "Anonymous" o "virus informático" forman parte del lenguaje común y las cibermolestias son una realidad para todos los usuarios de Internet.

Debemos tener en cuenta una serie de insuficiencias con respecto a:

- las medidas de seguridad en vigor;
- la resiliencia de nuestras infraestructuras y de nuestra capacidad de gestionar las crisis complejas que pueden plantearse;
- las medidas adoptadas para sensibilizar al público y en el marco de estructuras educativas, de la escuela primaria a la universidad, incluido el aprendizaje permanente, y los intentos de elaboración de soluciones "nacionales";
- las cibercompetencias y los recursos humanos en cada esfera de actividad;
- los medios atribuidos a sistemas judiciales y a la policía para hacer frente a la expansión del ciberdelito y la cibercriminalidad.

Hay que señalar además la insuficiencia de conocimientos y de un enfoque multidisciplinario y sistemático de la gestión de los riesgos en el ciberespacio, además de la insuficiencia de cooperación y colaboración nacionales e internacionales, de asistencia jurídica y de alianzas entre el sector público y el sector privado, así como entre civiles y militares.

He mencionado los conceptos de fragilidad, dificultad e insuficiencia, todos ellos vinculados a la noción de complejidad. Me refiero a la complejidad de una tarea que contempla dimensiones políticas, diplomáticas, económicas, de gestión, judiciales, tecnológicas y humanas, cuya finalidad es la protección contra todo tipo de ciberriesgos. Sabemos ahora que la sociedad de la información debe fundarse en la confianza y la seguridad, que la vigilancia no es sinónimo de seguridad y que la seguridad exige medidas de control fiables y ajustadas a un marco jurídico apropiado, y no impuestas por tecnologías, proveedores o actores que ejercen una posición dominante. Se debe además poner límite a la mundialización y al imperialismo tecnológicos.

Es necesario comprender que los ciberriesgos constituyen hoy una emergencia planetaria puesto que amplifican todos los riesgos tradicionales asociados, por ejemplo, a las instalaciones nucleares, a la contaminación o al terrorismo, y que resulta **indispensable** actuar en consecuencia. Es primordial aunar voluntad individual y voluntad colectiva, así como elaborar y poner a disposición los medios necesarios para afrontar los problemas de seguridad del siglo XXI.

Es verdaderamente urgente pues liberar recursos y poner en marcha estructuras institucionales y procedimientos ad hoc a todos los niveles –cantonal, regional, nacional e internacional– para aprovechar al máximo las ventajas de las tecnologías de la información y sacar partido de las nuevas posibilidades que ofrecen. Al mismo tiempo, hay que reducir sus inconvenientes, para asegurar ante todo la competitividad y la seguridad económica, puesto que de ellas depende el bienestar de todos.

Necesidad urgente de un instrumento internacional

Si se considera el ciberespacio como el quinto bien común, del mismo modo que la tierra, el aire, los mares y el espacio, es urgente asegurar la coordinación y la cooperación de todas las naciones.

Estamos convencidos de la necesidad y la urgencia de concertar un acuerdo internacional que aborde de manera coherente y global las cuestiones de ciberseguridad. Las organizaciones, las empresas y los Estados están expuestos a riesgos considerables vinculados a la divulgación, utilización indebida y destrucción de datos o informaciones. Este tipo de incidentes, vistos a escala microscópica, pueden ser considerados amenazas potenciales no sólo para la competitividad o reputación de una empresa, sino también para la seguridad pública o la democracia de un país.

Si pensamos que el ciberespacio es considerado cada vez más un campo de batalla económico y militar universal donde pueden desencadenarse ciberconflictos, reflejos de la competencia política y económica, ha llegado la hora de definir y aprobar en común qué es aceptable o no y de elaborar un instrumento internacional de control eficaz. Sin un enfoque común ni acuerdos internacionales, será imposible adoptar medidas de seguridad para proteger eficazmente los recursos TIC (comprendidas las infraestructuras esenciales de información), para luchar contra el ciberdelito y para preservar los derechos humanos fundamentales. Una tarea como esta exige la firme determinación de todos los actores e interesados en el plano nacional e internacional.

Habría que poner en práctica estrategias nacionales e internacionales no sólo para responder a los ciberataques, definiendo de esa forma las medidas de respuesta, sino también para definir por anticipado medidas que eviten los fallos de seguridad y los incidentes no deseados. Se podría, por ejemplo, instaurar una cultura eficaz de la

ciberseguridad limitando el número de puntos débiles que se aprovechan para atacar los sistemas, teniendo sistemáticamente en cuenta todos los factores que pueden dar lugar, entre otras cosas, a comportamientos impropios, crisis, actos de venganza o delitos, y reforzando la adopción de medidas complementarias y concertadas.

Estos problemas pueden ser tratados con eficacia desde un punto de vista estrictamente nacional. Así como el Protocolo de Tokio[14] es un acuerdo internacional vinculado a la Convención Marco de las Naciones Unidas sobre el Cambio Climático, sería de utilidad definir un Protocolo mundial sobre ciberseguridad y ciberdelito, gracias al cual se podrían reducir los riesgos y las amenazas en el ciberespacio a una escala verdaderamente universal. Un instrumento de esa naturaleza constituiría un marco esencial para la adopción de medidas eficaces de lucha contra los ciberataques, en el plano nacional e internacional, y contemplaría una definición clara de los comportamientos aceptables e inaceptables, así como de los medios de control necesarios.

Impulsar el diálogo internacional

En mayo de 2007, la UIT lanzó la Agenda sobre Ciberseguridad Global (GCA)[15], un marco de coordinación para dar respuesta a la multiplicación de ataques contra la ciberseguridad. Para ayudar a la UIT a elaborar esta estrategia, se creó un Grupo de Expertos de Alto Nivel (HLEG), cuyos miembros fueron nombrados por el Secretario General de la UIT, teniendo debidamente en cuenta la diversidad geográfica y los conocimientos necesarios, con objeto de garantizar una representación multipartita. Ese Grupo está integrado por más de 100 especialistas de renombre mundial de muy diverso origen[16]: representantes de administraciones miembros de la UIT, de Estados Miembros, del sector privado, de organizaciones regionales e internacionales, de entidades de investigación y de instituciones académicas[17]. En noviembre de 2008,

---

14 http://unfccc.int/essential_background/kyoto_protocol/items/1678.php

15 http://www.itu.int/osg/csd/cybersecurity/gca/index.html

16 http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html

17 El juez Stein Schjolberg (Noruega) fue el Presidente del HLEG y Solange Ghernaouti, corresponsable de los ámbitos de trabajo consagrados a las estructuras orgánicas y a la creación de capacidades.

la UIT[18] publicó el *Informe Estratégico Mundial*[19], que define estrategias en cinco ámbitos de trabajo: medidas jurídicas, medidas técnicas y de procedimiento, estructuras orgánicas, creación de capacidades y cooperación internacional. La GCA establece el marco esencial para la elaboración de medidas eficaces en el plano nacional e internacional que alientan a los países a poner en marcha programas nacionales de ciberseguridad y a cooperar a escala internacional. Debe considerarse una primera etapa importante de la estrategia mundial de la ciberseguridad. Desde entonces, esta cuestión ha suscitado intensos debates en el mundo entero[20].

La propuesta de un "Tratado mundial sobre ciberseguridad y ciberdelito: una contribución a la paz, la justicia y la seguridad en el ciberespacio" es el resultado de un largo periodo de cooperación internacional[21].

Camino a un instrumento al servicio de la comunidad internacional

Con objeto de contribuir a cumplir el imperativo universalmente reconocido de gestionar los ciberriesgos y luchar contra los ciberataques, el ciberdelito y las utilizaciones abusivas e indebidas de Internet, trataremos de identificar la necesidad de una nueva visión de la ciberseguridad internacional, fundada en el diálogo y en acuerdos internacionales eficaces. Al hacerlo, esperamos contribuir a que el ciberespacio y, por tanto, el mundo real, sean más pacíficos, justos y seguros.

---

18 Por otra parte, en 2008, la UIT creó la Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT), iniciativa internacional entre el sector público y el sector privado destinada a reforzar la capacidad de la comunidad internacional para prevenir las ciberamenazas, protegerse de ellas y darles respuesta (www.itu.int/osg/csd/cybersecurity/gca/impact_index.html)

19 http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

20 Puede hallarse una información más completa en "The baseline review ICT-related process and events, Implications for international and regional security", ICT for Peace Foundation. Ver http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-for-international-and-regional-security

21 En 2009, el juez Schjolberg y la profesora S. Ghernaouti publicaron una primera propuesta de tratado internacional en un pequeño libro que lleva por título "A global treaty on cybersecurity and cybercrime: a contribution for peace, justice and security in cyberspace" ("Tratado mundial sobre ciberseguridad y ciberdelito: una contribución a la paz, la justicia y la seguridad en el ciberespacio"), disponible en www.cybercrimedata.net. Esta publicación fue presentada en el Foro para la Gobernanza de Internet en Sharm El Sheikh: http://www.intgovforum.org/cms/2009-igf-sharm-el-sheikh. Ver también Ahmad Kamal, The Law of Cyber-Space. An Invitation to the Table of Negotiation. UNITAR, 2005. El embajador Kamal era miembro del PMP cuando escribió ese texto y UNITAR es un organismo de las Naciones Unidas.

Podríamos también plantearnos la creación de un tratado internacional, o de una serie de tratados, relacionados con el ciberespacio.

Ese tratado o esa serie de tratados sobre ciberseguridad y ciberdelito concertados a nivel de las Naciones Unidas deberían constituir un marco para la paz, la justicia y la seguridad en el ciberespacio y facilitar la elaboración de una estrategia mundial destinada a evitar las ciberamenazas, cualquiera sea su origen. La negociación de un tratado de ese tipo permitiría definir una perspectiva común de todos los aspectos de la ciberseguridad en los países, a diferentes niveles de desarrollo económico.

Todos los interesados deben ponerse de acuerdo en qué constituye el ciberdelito, el ciberterrorismo y otras ciberamenazas, condición previa a la elaboración de soluciones nacionales e internacionales encaminadas a armonizar medidas en materia de ciberseguridad. Por otra parte, un mutuo entendimiento ayudaría a reducir las disparidades de percepción de la ciberseguridad entre países desarrollados y países en desarrollo. Dado que los comportamientos delictivos en el ciberespacio se han difundido en el mundo entero, es necesario armonizar las legislaciones relativas al ciberdelito, asegurar la eficacia de la justicia internacional y la cooperación entre la policía, y mostrar una verdadera determinación al respecto.

Un tratado sobre el ciberespacio concertado a nivel de las Naciones Unidas debería establecer el principio según el cual los graves atentados a la paz y la seguridad cometidos en Internet y en el ciberespacio son delitos en virtud del derecho internacional, sean o no punibles con arreglo a la legislación nacional. Estamos profundamente convencidos de que los delitos más graves cometidos en el ciberespacio deberían ser definidos y sancionados en virtud del derecho internacional.

Conviene recordar que el Convenio del Consejo de Europa sobre la Ciberdelincuencia (2001), que entró en vigor el 1 de julio de 2004, marca un hito histórico en la lucha contra el ciberdelito[22]. Ese Convenio constituye apenas un ejemplo de iniciativa regional y numerosos países prefieren aplicarlo únicamente como referencia dado que siempre será un instrumento de origen europeo. En otras palabras, es necesario establecer, en el marco mundial y a nivel de las Naciones Unidas, un tratado o una serie de tratados que contemplen normas y principios ampliamente aceptados en ese

22 http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

Convenio, a los que se añadirán otras disposiciones importantes[23]. De hecho, como se ha indicado claramente en el Informe Estratégico Mundial del Presidente del HLEG a la UIT, las medidas pertinentes están vinculadas a las dimensiones jurídicas, técnicas y de procedimiento que se apoyan en estructuras orgánicas, en capacidades efectivas y en la cooperación internacional.

La concertación de un tratado internacional será considerada una actividad consecutiva a la elaboración de Informes del HLEG y marcará un nuevo paso de la GCA de la UIT, que impulsa a los países a poner en marcha programas nacionales de ciberseguridad y a promover la cooperación internacional. Un tratado mundial los obligaría a cumplir sus compromisos.

Perspectivas de futuro

La creación de un ciberespacio seguro y fiable exigirá recursos y competencias de toda índole. Ese proyecto se apoyará no sólo en tecnologías y procedimientos de gestión especializados, dentro de un marco jurídico concreto aplicable en el plano nacional y compatible en el plano internacional, sino además en medios de gobernanza y control reconocidos y verificables a escala internacional.

La comunidad internacional, como lo ha hecho en la Declaración Universal de Derechos Humanos de 1948[24], tendrá que identificar, adoptar y reconocer ampliamente ciertos principios fundamentales.

No será fácil definir esos valores comunes, habida cuenta de las diferencias entre países, culturas e intereses económicos o políticos. Sin ninguna duda, la elaboración de un tratado internacional llevará mucho tiempo. Por eso es tan urgente crear desde ahora un mecanismo para facilitar un diálogo internacional que logre su cometido en un plazo proporcional a la urgencia de los desafíos.

Pese a las dificultades que entraña la negociación de un tratado de esa naturaleza y, naturalmente, a la probabilidad de que no siempre sea respetado, como lo pone tristemente de manifiesto la Declaración Universal de Derechos Humanos citada como ejemplo, ese instrumento podría servir para luchar contra los comportamientos

---

23 Varios países no aceptaron ciertas normas y principios, en particular el principio enunciado en el Artículo 32 del Convenio sobre "Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público". La opinión de esos países debe ser respetada (fuente: Informe del Presidente del HLEG, UIT, 2008).

24 http://www.un.org/en/documents/udhr/

indebidos de particulares, organizaciones o Estados. Debería asimismo evitar el alejamiento de los valores comunes, o al menos poner de relieve las divergencias y autorizar, llegado el caso, una reparación por vía judicial.

Con todo, una especie de "tratado de no proliferación de la cibertecnología" podría ser insuficiente, en la medida en que reduciría el ciberespacio y las tecnologías de la información a meras herramientas militares similares a las armas. Pero las fronteras entre el mundo militar y el mundo civil no son claras; ambos utilizan las mismas tecnologías y la misma Internet, tanto los usuarios más jóvenes como los de mayor edad.

Se podría establecer una analogía con el Tratado de 1968 sobre la no proliferación de las armas nucleares[25], cuyas ventajas ya no se ponen en tela de juicio, a pesar de las dificultades permanentes de su aplicación. Ese Tratado no pudo evitar la catástrofe nuclear de Fukushima en marzo de 2011, que no fue el resultado de operaciones militares. En cambio, una organización como el Organismo Internacional de Energía Atómica (OIEA) ha dado prueba de su utilidad en la coordinación del seguimiento de una catástrofe y la creación posterior de medidas de seguridad. Tendría que haber una estructura equivalente aplicada al ciberespacio con el fin de alentar al público a utilizar las tecnologías de la información y la comunicación de forma segura y pacífica.

Esa analogía, sin duda atrevida, con las armas y las centrales nucleares, no se aplica, como es natural, a la necesidad de adoptar una política global frente a los problemas de seguridad del ciberespacio. Esos problemas justifican la adopción de un tratado (o una serie de tratados) que reconozca, entre otras, la dimensión militar de esa política.

El ciberespacio reúne a todo tipo de delincuentes, cuyas actividades, como el blanqueo de dinero y el tráfico de personas, inciden en el ámbito militar y en el ámbito civil. Con todo, ¿es aceptable que los derechos humanos no se respeten en el ciberespacio?

---

25 Tratado sobre la no proliferación de las armas nucleares. Abierto a la firma en Londres, Moscú y Washington el 1 de julio de 1968: http://www.un.org/en/disarmament/instruments/npt.shtml (UNODA United Nations Office for Disarmament Affairs: http://www.un.org/disarmament/ UNIDIR – United Nations Institute for Disarmament Research: http://www.unidir.org/html/en/home.html)

Internet y el ciberespacio han pasado a ser, en todo el mundo, componentes de la civilización que dejaremos en herencia a las generaciones futuras. Tenemos pues el deber y la responsabilidad, a título individual y colectivo, de definir entre todos los valores comunes que queremos promover y de poner en práctica y hacer respetar mecanismos de control en la materia.

Medidas de fomento de la confianza

Cada eslabón de la cadena digital, y cada país, cumplen una función en la ciberseguridad y la ciberconfianza. La seguridad tiene un precio, pero la inseguridad y la falta de confianza en el universo digital también. En la actualidad, esos costos corren esencialmente a cargo de los usuarios y la sociedad en general; por una parte, para financiar los sistemas policiales y judiciales que combaten el ciberdelito y, por la otra, debido a la desestabilización económica causada por los ciberataques, el robo de datos y el ciberespionaje. Los riesgos que se corren son diversos: quiebra de empresas, deterioro de la imagen, pérdida de confianza del cliente, pérdida de partes del mercado y pérdida de empleos.

El ciberespacio no debe ser un campo de batalla ni una zona de delincuencia organizada, y por eso tenemos que colaborar con honestidad y absoluta sinceridad para encontrar la forma de protegerlo, para nosotros y para las generaciones futuras. No tengo ninguna duda de que lo lograremos por medio de un tratado internacional, una verdadera Declaración Universal de Derechos Humanos (de los hombres, las mujeres y los niños) en el ciberespacio. Un tratado de ese tipo contribuirá a instaurar la confianza en el ciberespacio, siempre que los particulares, las organizaciones y los Estados en el mundo entero tengan la determinación y el compromiso necesarios para respetarlo y para elaborar prácticas encaminadas a protegerlo.

Aunque no debemos olvidar los límites de una iniciativa de ese tipo y de la creación de un nuevo tratado internacional, su principal ventaja será indudablemente la toma de conciencia de la necesidad de seguridad y confianza.

En el marco de un conjunto de medidas de fomento de la confianza, por ejemplo un tratado, el diálogo internacional podría constituir:

- un medio eficaz de comunicación y de sensibilización respecto de las cuestiones de la paz y la seguridad en el ciberespacio y en el mundo real;
- un trabajo de referencia que aliente a los actores económicos e institucionales (comprendidos la policía y el poder judicial) a adoptar buenas prácticas;
- un punto de partida para la implantación de servicios y tecnologías que permitan reforzar la confianza y los mecanismos judiciales, y facilitar la lucha contra el ciberdelito;

- un instrumento que contribuya a hacer respetar un mínimo de seguridad en Internet y que disminuya el umbral de tolerancia de la población a la ciberviolencia.

Conclusión

Ha llegado el momento de adoptar medidas pragmáticas que preserven y protejan nuestro patrimonio digital y lo ayuden a prosperar, y que contribuyan al desarrollo de la seguridad económica, el empleo y la competitividad. Son estos algunos imperativos y desafíos para los ciudadanos, sin que sea necesario insistir en el respeto de sus derechos fundamentales que son, en última instancia, idénticos en materia de seguridad, con grados diferentes de importancia para los particulares, las sociedades y los Estados.

Juntos seremos más fuertes y podremos dar mayor cohesión y coherencia a las medidas de seguridad. Los territorios digitales ya no pueden ser protegidos de forma aislada dado que los virus, electrónicos o biológicos, no reconocen fronteras. Tampoco los ciberataques, que acometen numerosas infraestructuras, hasta las que pertenecen a nuestros aliados y vecinos tradicionales.

Para la creación de una sociedad de la información viable y duradera, los ciudadanos bien informados deben exigir la protección de infraestructuras, el desarrollo de la resiliencia, la lucha contra el ciberdelito y el fortalecimiento de posiciones nacionales en materia de ciberseguridad y ciberdefensa.

Según la sabiduría popular, con buen tiempo se construye el techo que nos protegerá de la lluvia; en otras palabras, reaccionemos antes de que sea demasiado tarde.

Sería ingenuo y peligroso esperar que los puntos vulnerables desaparezcan por sí solos y que las amenazas que los explotan se hagan realidad. Tenemos que anticiparnos y reforzar la ciberseguridad para evitar, entre otras cosas, la depredación de nuestros recursos de información, conocimientos, propiedad intelectual y datas personales, y para impedir también que ciertos actores refuercen su poder y hegemonía, se trate de entidades legítimas o delictivas.

Sin pecar de ingenuidad o paranoia, ha llegado la hora de integrar en nuestras estrategias de seguridad el hecho de que Internet ha modificado profundamente las formas de ejercer el poder y creado nuevos tipos de conflictos entre los particulares, las instituciones y los Estados.

1.2 Normas, reglas y principios aplicables a Internet según las Naciones Unidas y los Estados Miembros: Evaluación del Informe del Grupo de Expertos Gubernamentales de las Naciones Unidas

por Henning Wegener

Como se deduce claramente de la lectura de análisis precedentes, los países han tomado profunda conciencia de la necesidad de establecer un orden universal en el ciberespacio y de fijar en él normas de comportamiento responsable para las autoridades públicas y otros interesados. Aunque en un primer momento el ciberespacio no era un vacío ni estaba librado a la anarquía, ha seguido teniendo como particularidad la falta de un marco jurídico detallado y consensual aplicable no sólo a los Estados sino también a todos los interesados. Lo fundamental era, y todavía lo es, adoptar paulatinamente un comportamiento de respeto que incite a la creación de normas universales. Con esta perspectiva de universalidad, la presente contribución hace especial hincapié en las actividades recientes de las Naciones Unidas, especialmente en los resultados de los trabajos del Grupo de Expertos Gubernamentales.

Ha habido varios intentos concertados en estos últimos años para regular el ciberespacio: la serie de Resoluciones adoptadas por las Naciones Unidas desde 1998; la adopción del Convenio de Budapest sobre la Ciberdelincuencia en 2001; el proceso de la CMSI; legislaciones nacionales específicas para regímenes de derecho civil aplicables a delitos civiles y daños, el derecho penal; los reglamentos administrativos, así como el derecho internacional privado aplicable. Pero, según la opinión general, es a partir de 2008 que tiene lugar una actividad diplomática sistemática y exhaustiva en materia de ciberespacio. Desde entonces, se ha observado un gran número de actividades en numerosos países y una profusión impresionante de iniciativas y procesos que, reunidos, han hecho evolucionar de forma diferente el consenso con respecto a la necesidad de establecer normas. Aunque llevaría mucho tiempo enumerar y analizar aquí todas esas actividades[26], esperamos contribuir a un proceso

[26] En vez de presentar una lista completa, hacemos referencia *infra* a los documentos más importantes en su contexto.

"iterativo: cada paso del camino partirá del anterior".[27] Muchas de ellas recurren a herramientas útiles, como la elaboración de medidas adecuadas para restaurar la confianza, o códigos de conducta, o incluso técnicas de negociación, que se examinan en otras partes de la presente publicación.[28]

Afortunadamente, esas actividades han dado lugar a un gran número de excelentes informes analíticos que facilitan el examen y la prosecución de las tareas[29].

El bienio 2013-2014 ha sido particularmente fértil al respecto. Ha tenido lugar, entre otras cosas, la publicación de al menos tres documentos fundamentales: el Manual de Tallinn sobre la Aplicabilidad del derecho internacional a los ciberconflictos[30], el documento de NetMundial sobre Gobernanza de Internet[31] y, ante todo, el Informe del Grupo de Expertos Gubernamentales (GEG) de las Naciones Unidas, concluido en el verano de 2013 y presentado a la Asamblea General de las Naciones Unidas en su

---

27 Doc. A/68/98, p. 11.

28 El concepto de códigos de conducta, o según algunos, de transparencia, y de medidas de fomento de la confianza ha visiblemente sustituido la fascinación que ejercía antes el concepto de Convención global sobre el ciberespacio, comparable a la Convención de las Naciones Unidas sobre el Derecho del Mar establecida en 1982. Poco a poco se comprendió que los obstáculos contra la creación de un instrumento de esa naturaleza eran abrumadores. El ciberespacio podría ser incluso más complejo que el mundo de los océanos. Las tecnologías digitales y su utilización siguen evolucionando rápidamente. La elaboración de un tratado de valor universal sería frenada por divergencias aún más nítidas en las posiciones de cada país. La negociación de un tratado llevaría mucho tiempo, del mismo modo que los procedimientos de ratificación a escala nacional. La duración del proceso sería desproporcionada con respecto a la necesidad urgente de llenar el vacío jurídico y frente a la percepción general de que la amenaza de ciberconflicto y de ciberdaño irreparable aumenta peligrosamente. Por ello, aunque serían preferibles un tratado o una legislación universal sobre el ciberespacio, convendría en esta etapa y por el momento adoptar otra opción por motivos prácticos.

29 Camino Kavanagh, Tim Maurer y Eneken Tikk-Ringas "Baseline Review. ICT-Related Processes and International and regional Security (2011-2013)" www.ict4peace.org, Ginebra, marzo de 2014; *Annegret Bendieck,* "Umstrittene Partnerschaft. Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit", DGAP, Berlin, diciembre de 2013. Ver también *Henning Wegener,* "Regulating Cyber Behavior: Some Initial Reflections on Codes of Conduct and Confidence-Building Measures", Erice, agosto de 2012, disponible en www.unibw.de/infosecur

30 "Manual de Tallinn sobre la Aplicabilidad del derecho internacional a los ciberconflictos", editado por Michael N. Schmitt. Preparado por el Grupo Internacional de Expertos gracias a la invitación del Centro de Excelencia para la Cooperación en la defensa del Ciberespacio de la OTAN, Cambridge University Press 2013.

31 Declaración Multipartita de NETmundial, http://netmundial.br

68º Periodo de Sesiones[32]. Esos tres documentos esenciales son examinados en la presente publicación. Este artículo da mayor prioridad al tercero de ellos, pero hace también referencia, llegado el caso, a los otros dos.

El Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, elaborado en 2013, no es un documento único en su género. El mandato de este Grupo consistía en "[…] continuar examinando las amenazas reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para encararlas, como normas, reglas o principios de comportamiento responsable de los Estados y medidas de fomento de la confianza respecto del espacio informativo, así como los conceptos encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones". Este documento se apoya en los resultados obtenidos por el 2º Grupo de Expertos Gubernamentales, que elaboró un Informe en julio de 2010 (A/65/201). Saca además partido de las tendencias puestas de relieve por una serie de conferencias multipartitas organizadas con el apoyo de gobiernos, de Londres a Budapest, cuyos debates se consagraron en particular a las normas y al fomento de la confianza, como indica el mandato del Grupo de Expertos. Las numerosas consultas realizadas en organizaciones regionales e importantes organismos internacionales, como la Asamblea General de las Naciones Unidas, la Unión Europea, el G8, la OTAN y organizaciones regionales de las Naciones Unidas han hecho aportes interesantes. En su Informe, el Grupo de Expertos expresa puntos de vista comunes que evolucionan y, en ciertos casos, consensos logrados. Insiste en mantener una reflexión seria con respecto a los problemas prácticos del ciberespacio y marca al mismo tiempo una nueva etapa en la medida en que los problemas ya examinados en otras instancias son presentados desde otro ángulo, en forma sintética, por un grupo representativo de gobiernos del mundo entero. Por otra parte, la continuidad del proceso está asegurada por la creación de un nuevo (4º) Grupo de Expertos Gubernamentales, compuesto de representantes de un número mayor de países (20 en este caso) que examinarán en detalle las recomendaciones del Informe (A/RES/68/243) y cuyo mandato ampliado contempla el examen de "[...] las cuestiones relativas al uso de las tecnologías de la información y las comunicaciones en los conflictos". También está asegurada por diferentes eventos internacionales: en 2015, los Países Bajos organizarán una serie de grandes conferencias sobre el ciberespacio, en el marco de las cuales cada gobierno contribuirá a aumentar ese consenso. La Conferencia de Seúl sobre el ciberespacio, celebrada en 2013, inmediatamente

---

32 Documento A/68/98 de las Naciones Unidas.

después de la publicación del Informe del Grupo de Expertos Gubernamentales, reunió unos 90 Estados que aprobaron por consenso la mayoría de las recomendaciones contenidas en el Informe, en el Marco y los Compromisos de Seúl para un ciberespacio abierto y seguro. Aunque el Informe del Grupo, como ocurre con la Declaración Multipartita de NETmundial, no es vinculante, imprime una dinámica que permite esperar nuevos consensos internacionales.

Los últimos dos capítulos del Informe del Grupo de Expertos Gubernamentales contemplaron recomendaciones que tienen un interés central para este artículo. Se trata de recomendaciones sobre normas, reglas y principios de conducta estatal responsable, así como de recomendaciones sobre medidas de fomento a la confianza y el intercambio de información. Puesto que la función de esas medidas en una nueva visión de la ciberseguridad internacional será objeto de otra contribución a la presente publicación, nos ocuparemos de ella brevemente.

Las medidas de fomento de la confianza apuntan esencialmente a combatir las amenazas, aumentar la transparencia y prever el comportamiento de los Estados. Son además flexibles, de aplicación voluntaria, permiten una participación sumamente variable (posibilidad de participación de actores que no pertenecen al sector público) y facilitan el seguimiento. Contrariamente a lo que ocurre con la elaboración de tratados, que es un proceso coherente, los participantes son libres de adoptar soluciones parciales y ponerlas en práctica sin demora e independientemente o en colaboración con otros interesados que comparten sus puntos de vista. Ese tipo de medidas adoptadas por los Estados no necesitan ser ratificadas; sirven de ejemplo y, en el mejor de los casos, son vinculantes en el plano político. Son pues ideales para facilitar la búsqueda de un consenso internacional de manera progresiva. Un conjunto bien negociado de esas medidas, adoptadas por un número suficiente de participantes, puede dar lugar a un proceso de cambios paulatinos y a una mayor sensibilización sobre el tema. Una mejor comprensión de las normas de comportamiento puede servir de incentivo para ir más lejos.

El concepto de medidas de fomento de la confianza, que surgió en el contexto de la confrontación Este-Oeste y en el marco de la entonces CSCE y de las Naciones Unidas, es hoy de aplicación universal[33].

Las recomendaciones contempladas en el Informe del Grupo de Expertos Gubernamentales hacen referencia a la cooperación internacional, la transparencia, los intercambios de informaciones urgentes en el plano internacional, los procedimientos de alerta avanzados durante las 24 horas del día y los mecanismos CERT, la armonización de disposiciones jurídicas, el cumplimiento de las leyes, el diálogo institucionalizado y otras consideraciones "prácticas". Hacen también hincapié en la necesidad de la participación del sector privado y la sociedad civil, promoviendo de esa forma el concepto de participación multipartita. Esas recomendaciones se inscriben en "catálogos" sobre comportamientos ya tradicionales que refuerzan la confianza en otras actividades internacionales y se inspiran en documentos como la Agenda sobre Ciberseguridad Global de la UIT, que define tareas en materia de cooperación internacional que culminan en "[...] un marco conducente a una estrategia mundial multipartita que fomente la cooperación, el diálogo y la coordinación internacionales".

Numerosas medidas recomendadas se inspiran también en las presentadas por el G8 en 1998, en la Decisión marco de la Unión Europea de 2003 o en el capítulo pertinente del Convenio de Budapest. Adquiere particular importancia la Serie inicial de medidas de fomento de la confianza de la OSCE para reducir los riesgos de conflictos ocasionados por la utilización de las tecnologías de la información y la comunicación[34], recientemente adoptada por el Consejo Permanente de la OCSE. Esa organización, integrada por miembros del Este y del Oeste, agrupa un gran número de países situados en un vasto territorio y que expresan por lo general puntos de vista diferentes. En el plano no gubernamental, el análisis más completo y sistemático de las medidas de fomento de la confianza en el ciberespacio es sin duda la recopilación

---

33 Para las primeras aplicaciones de este concepto en Europa y otras regiones, ver Henning Wegener "CBMs: European and Global Dimensions" en: F. Stephen Larrabee and Dietrich Stobbe, eds., "Confidence-Building Measures in Europe", Institute for East-West Studies, New York, 1983. Las directrices adoptadas por las Naciones Unidas se volvieron a publicar en el documento de las Naciones Unidas A/S-15/3. Para otras aplicaciones, ver por ejemplo el Documento de Montreux sobre Operaciones de empresas de servicios militares y de seguridad privadas durante los conflictos armados, www.icrc.org, o el proyecto de Código de conducta sobre las actividades en el espacio ultraterrestre (2010), http://register.consilium.europa.eu

34 OSCE Documento PC.DEC/1106 del 3 de diciembre de 2013.

efectuada por ICT4Peace en Ginebra en 2013, basada en parte en los resultados de la conferencia convocada en Zúrich por la misma excelente organización[35].

Dado que las recomendaciones relativas a normas, reglas y principios son incluso quizás de mayor utilidad para la gestión del ciberespacio y la ciberseguridad, deben por tanto examinarse más a fondo. Habrá también que demostrar las lagunas y ambigüedades del texto y, a partir de un primer análisis, señalar las tareas aún pendientes y las dificultades que afrontará el 4º Grupo de Expertos Gubernamentales de las Naciones Unidas, y otras instancias que se ocupan de la ciberseguridad, en su incipiente labor.

El hecho de que los representantes gubernamentales de cinco miembros permanentes del Consejo de Seguridad de las Naciones Unidas, así como India y Japón, se hayan asociado al consenso pone de manifiesto la importancia de esa breve lista de normas y principios esenciales. Pese a su carácter no vinculante, es pues un documento de referencia fundamental.

En varias ocasiones se ha indicado que la conclusión del Grupo, según la cual el derecho internacional, en particular la Carta de las Naciones Unidas, se aplica plenamente a la utilización de las TIC, reviste una importancia particular. Ese principio se ha evocado ya en numerosos acuerdos internacionales, pero nunca de forma tan clara. Es un avance decisivo, pese al añadido inmediato de dos frases que indican, por una parte, la necesidad de seguir examinando de qué manera esas normas se aplican al comportamiento de los Estados y, por la otra, la posibilidad de que, en el futuro, se elaboren nuevas normas adaptadas a las particularidades de esas tecnologías.

Estas salvedades reflejan diferencias bien conocidas y perdurables entre los grandes países con respecto a la concepción de la gestión de las TIC a escala mundial. Los autores del presente Informe han debido por tanto mantener, a lo largo de todo el texto, un delicado equilibrio. Al párrafo sobre la aplicabilidad del derecho internacional le sigue inmediatamente otro que afirma la aplicabilidad de la soberanía de los Estados a las actividades e infraestructuras vinculadas a las TIC que corresponden al ámbito de competencia del Estado.

La reafirmación de la validez del derecho internacional en el ciberespacio contempla, como se indica más adelante, el respeto de los derechos humanos y de las libertades fundamentales en el marco de los convenios internacionales pertinentes. Este principio, aunque ya ha sido enunciado en numerosos documentos internacionales

---

35 "Confidence Building Measures and International Cyber Security", www.ict4peace.org

desde la celebración de la CMSI, tiene sin duda una gran importancia para el futuro de la libertad en Internet y la lucha contra la censura de Internet por los poderes públicos.

La aplicabilidad de la Carta de las Naciones Unidas se extiende también a sus disposiciones fundamentales sobre el mantenimiento de la paz y la seguridad internacionales, la abstención de recurrir a la amenaza o al uso de la fuerza y el derecho de autodefensa contra ataques armados al ciberespacio. No obstante, en espera de un "nuevo estudio", el Informe no aborda la cuestión de la utilización hostil de las TIC. Aunque ciertamente tiene conocimiento del proyecto de código de conducta internacional para la seguridad de la información presentado en 2011 por Rusia, China y otros países[36], documento expresamente citado en el capítulo sobre recomendaciones y normas, el Grupo no ha incluido el equivalente del proyecto anterior de norma, a saber: "No utilizar las tecnologías de la información y las comunicaciones, inclusive en red, para realizar actividades hostiles o actos de agresión, plantear amenazas a la paz y la seguridad internacionales ni contribuir a la proliferación de armas informáticas o tecnologías conexas". Se trata de una omisión lamentable, desde el punto de vista del autor del presente artículo. Con todo, las otras normas y los otros principios enunciados son plenamente respetables y teóricamente incontrovertibles, en particular las recomendaciones relativas al fortalecimiento de la cooperación contra la utilización de las TIC con fines delictivos o terroristas, la armonización de enfoques jurídicos y la colaboración con miras al cumplimiento de la ley y entre los magistrados.

Resulta también digna de consideración la lista de normas y principios enunciada en el párrafo 23 del Informe: los Estados deben cumplir sus obligaciones internacionales en lo que respecta a los hechos internacionalmente ilícitos que se les puedan atribuir, aunque sea difícil definir los autores de actos abusivos cometidos en el ciberespacio; no deben valerse de agentes que cometan esos hechos por su cuenta y "asegurarse" de que su territorio no sea utilizado por ciberdelincuentes no estatales. El hecho que un gran número de países esté obligado a adoptar esas normas y ajustarlas a las legislaciones nacionales podría constituir un instrumento eficaz en la lucha contra las actividades de los operadores de redes robot y las bandas de ciberdelincuentes. Por otra parte, cabe esperar que las presiones internacionales faciliten la aplicación de las medidas necesarias en el plano nacional para hacer cumplir la ley.

---

36 A/66/359.

Por último, el texto hace referencia al papel del sector privado y la sociedad civil para contribuir a mejorar la ciberseguridad, "incluida la seguridad de la cadena de suministro de productos y servicios de las tecnologías de la información y las comunicaciones". Nos recuerda que la ciberseguridad es una labor de toda la sociedad que supone la participación de numerosos interesados, cuyas responsabilidades no se limitan al "comportamiento responsable de los Estados".

Evaluadas en su totalidad, las diferentes secciones del Informe -al margen de la parte consagrada a las normas y principios, y del capítulo sobre medidas de fomento de la confianza, hay también un capítulo sobre medidas de creación de capacidad que contiene recomendaciones útiles aunque menos interesantes- constituyen indiscutiblemente un avance. El Informe no elimina ciertas divergencias fundamentales entre los países con respecto a la gestión futura del ciberespacio, pero las atenúa. Las diferencias en cuanto a los conceptos de base plantean un problema espinoso, especialmente cuando se sabe que en su próxima reunión, el Grupo de Expertos Gubernamentales "examinará más a fondo" el inicio de consenso y tratará de establecer disposiciones detalladas.

Con todo, el Informe, que representa la continuidad de una serie de conferencias internacionales importantes (Londres, Budapest, Seúl y otras) y los trabajos de organizaciones regionales e internacionales, consagra una doble estrategia: por una parte, elabora medidas de fomento de la confianza y, por la otra, normas y principios para el establecimiento de uno o más códigos de conducta en el ciberespacio. Cualesquiera sean las modalidades de negociación que se apliquen, la estrategia adoptada hará que el comportamiento del Estado sea más previsible y más flexible, será de aplicación voluntaria, permitirá una participación sumamente variable (Estados e instancias no estatales) y facilitará el seguimiento. Contrariamente a lo que ocurre en un proceso coherente de negociación de tratados, los participantes son libres de adoptar soluciones parciales y ponerlas en práctica sin demora e independientemente o en colaboración con otros interesados que comparten sus puntos de vista. No obstante, el Grupo de Expertos Gubernamentales sólo ha logrado un consenso parcial y las dificultades que afrontará el Grupo que lo suceda serán inmensas.

El Grupo, creado a fines de julio de 2014, eligió Presidente al representante de Brasil, definió su calendario de trabajo y distribuyó las tareas entre sus 20 expertos gubernamentales que, a partir de ahora, establecerán o revisarán sus posiciones y presentarán proyectos de contribución en consecuencia. El Grupo se reunirá nuevamente en enero de 2015 para presentar su Informe antes del verano de 2015.

Una de las tareas fundamentales y más complejas del Grupo será definir más en detalle las reglas del derecho internacional relativas a la seguridad y la paz internacionales, en particular definir lo que constituye un "ataque armado" en el ciberespacio, qué se entiende por soberanía en el ciberespacio y cómo se puede poner límite a las utilizaciones hostiles de las cibertecnologías ("ciberarmas", comprendidos los programas informáticos malignos concebidos para atacar y dañar infraestructuras militares) e integrarlas en un marco reglamentario. Estas cuestiones, que nos planteamos desde el inicio de la era de la informática, son cada día más inquietantes debido a que, en la actualidad, un número incesante de Estados se lanza a una carrera desenfrenada de ciberarmamentos sin que se sepa cómo ponerle límites desde el punto de vista jurídico o político.

El Manual de Tallinn, que será examinado en otra parte de la presente publicación, ofrece sin ninguna duda reflexiones y directrices interesantes que permiten establecer analogías con el derecho internacional clásico. No obstante, ha sido redactado por un grupo de expertos juristas principalmente "occidentales" y carece de una perspectiva más internacional. Al efectuar una evaluación crítica del Manual se observa que un análisis que toma como punto de partida la legislación aplicada a conflictos armados tiende a considerar como una opción corriente las utilizaciones hostiles o militares de la cibertecnología, aunque los autores del Manual describen más o menos claramente los límites y modalidades de esa posible utilización. No es sorprendente que este Manual, pese a su estilo cuidadoso y prudente, haya sido interpretado por muchos como una "invitación a la ciberguerra". Es indudable que hubiera sido conveniente haber afirmado con determinación el rechazo categórico a la ciberguerra y a los peligros que supone.

Hay otra dificultad que guarda relación con el carácter – necesariamente – general de las recomendaciones del Informe. En cada caso, será sumamente difícil poner en práctica y cumplir las disposiciones correspondientes en la medida en que la integración de los diversos procesos regionales y del amplio conjunto de interesados debe ser gestionada con el propósito de obtener resultados compatibles.

En esas circunstancias, la creación de uno o más foros que sirvan de marco a debates intensivos, y luego a negociaciones, es una tarea compleja. En su Informe, el Grupo de Expertos Gubernamentales recomienda celebrar con regularidad un diálogo institucional con una amplia participación, bajo los auspicios de las Naciones Unidas, así como diálogos en foros bilaterales, regionales y multilaterales y otras organizaciones internacionales. Esa recomendación avanza en la dirección adecuada pero es aún demasiado vaga para permitir una adopción de decisiones rápida. Sería sin duda acertado limitar las opciones institucionales acordando en primer lugar los criterios que deberían cumplir esos foros (inclusión y apertura, plena participación de

un gran número de interesados, asistencia prestada por una secretaría internacional que reúna los conocimientos necesarios en materia de TIC, etc.). Naturalmente, lo más conveniente sería disponer de un foro único con perspectiva universal. Por otra parte, ya se han formulado iniciativas preliminares a escala regional y convendría no desaprovechar esa dinámica. Una conferencia autónoma de los Estados, capaz de establecer su propio reglamento interno y las modalidades de una amplia participación de los interesados, podría constituir una instancia adecuada.

Retomando el capítulo del Informe que formula recomendaciones sobre normas, reglas y principios, se podría señalar que, con todo el respeto que nos merecen sus autores y teniendo en cuenta el contexto político de las Naciones Unidas así como la necesidad de obtener un consenso en plazos limitados, la lista que presentan es selectiva, e incluso incompleta. Seguramente, el 4º Grupo de Expertos Gubernamentales examinará a fondo otras normas y principios propuestos recientemente[37].

Es particularmente necesario establecer normas más explícitas en las esferas esenciales de la seguridad, la estabilidad en el ciberespacio y la paz en el ciberespacio[38]. Quedan por colmar aún varias lagunas, por ejemplo el llamamiento a la concertación de un acuerdo vinculante sobre el principio fundamental según el cual un ciberataque contra otro Estado, ya sea directamente o por intermedio de delincuentes reclutados con ese fin, constituye una violación del derecho internacional; o el compromiso de todos los Estados a no ser el primero en recurrir a ciberarmas contra otro Estado, mientras no haya sido atacado por armas convencionales. Los Estados deberían además suscribir, en el plano nacional e internacional, una política de prevención de ciberconflictos dando prioridad a la ciberdefensa, limitando la fabricación, utilización y exportación de cibermedios ofensivos, en particular los software de ataque especializados, y no dándoles legitimidad. Las infraestructuras esenciales tendrían que estar protegidas incluso más de lo propuesto en el párrafo 26 e) relativo a la mayor cooperación internacional, en

---

37 Como complemento de los trabajos de las organizaciones regionales enumeradas en parte en el párrafo 27 del Informe del Grupo de Expertos Gubernamentales, ver la referencia anterior a los trabajos de ICT4Peace (nota al pie de página 6); el artículo de Henning Wegener (nota al pie de página 3); los cinco principios en materia de paz en el ciberespacio enunciados por el Secretario General de la UIT en la *Declaración de Erice sobre los Principios de paz y estabilidad en el ciberespacio*, 2009, retomada en la publicación *La búsqueda de la paz en el ciberespacio*, pág. 123.

38 El mandato del 4º Grupo de Expertos Gubernamentales, a partir de ahora constituido, hace hincapié en los casos de "conflicto".

virtud del principio según el cual los Estados son responsables de la protección de esas infraestructuras esenciales en su territorio nacional y los ataques contra las mismas están prohibidos, con objeto de garantizar la inviolabilidad de las estructuras digitales transnacionales de la red. Otro principio omitido: la obligación de todos los Estados de proteger a sus ciudadanos en el ciberespacio. No limitándose a la recomendación formulada en el párrafo 23, habría que enunciar con claridad la prohibición de utilizar redes robot y otras prácticas irregulares vinculadas al ciberdelito y a la ciberguerra, así como la obligación de los Estados a que se aplique esa prohibición en su territorio nacional. Por último, la neutralidad sigue siendo un concepto válido en el ciberespacio y no se debe perpetrar ningún ciberataque, incluso en caso de autodefensa, a través de estructuras de la red en Estados neutrales.

1.3 ¿Se aplica el derecho internacional al ciberespacio?

por Gábor Iklódy

La era digital supone ventajas excepcionales pero también numerosas amenazas que pueden ocasionar perturbaciones profundas, incluso destrucciones. La principal dificultad es descubrir cómo proteger el ciberespacio y conservar su fiabilidad para que siga siendo un entorno en el que podamos navegar libremente y aprovechar a fondo todas sus posibilidades, teniendo más en cuenta la seguridad. Para ello, hay que encontrar el justo equilibrio entre libertad y seguridad. No debemos ignorar los riesgos en materia de seguridad ni utilizarlos como un pretexto para justificar la restricción de la libertad y de libertades públicas. Para inspirar confianza, hay que velar por que los organismos públicos respeten plenamente los imperativos de responsabilidad democrática en sus intentos de prevenir las actividades delictivas en el ciberespacio.

La confianza es tan decisiva para los ciudadanos como para los Estados en sus relaciones internacionales, tema del presente artículo. Observamos en la actualidad una especie de "ciberguerra fría" acompañada de actividades de espionaje en el ciberespacio y de importantísimas inversiones, especialmente por parte de países avanzados que disponen de recursos suficientes en capacidades ofensivas.

Para los militares de nuestra época, es esencial preservar su capacidad de maniobrar libremente en el ciberespacio, condición que se pone de relieve en un número creciente de estrategias de defensa nacional para las cuales el ciberespacio constituye "un nuevo espacio de guerra que ha adquirido una importancia tan fundamental para

las operaciones militares como la tierra, los mares y el espacio"[39]. La conclusión es perfectamente clara: la guerra moderna también se desencadena en el ciberespacio y, probablemente, los conflictos a gran escala estallarán también en el ciberespacio, como se ha observado en numerosas ocasiones estos últimos años.

Para seguir teniendo confianza en el ciberespacio hay que establecer una cooperación en el marco de la cual se apliquen reglas de aceptación común. Las normas internacionales que rigen el comportamiento de los Estados son factores esenciales en ese entorno, pero no suficientes. En el ciberespacio, un ámbito singular en el que participan numerosos interesados, los Estados son un participante más. Mucho más que en cualquier otro ámbito, se debe establecer y mantener en el ciberespacio una verdadera alianza público-privada. "El sector privado posee y explota la mayor parte de las infraestructuras del ciberespacio y es el que produce la tecnología necesaria. El sector privado representa además la primera línea de defensa, en tanto que las empresas privadas y los científicos conciben el futuro entorno tecnológico en el que los Estados operarán."[40] Ello no quita de ninguna manera responsabilidad a los Estados en materia de soberanía, de la cual no pueden librarse.

No disponemos actualmente de disposiciones de tratado o de normas que se apliquen expresamente al ciberespacio. ¿Significa por tanto que debe ser considerado un ámbito no sujeto a reglamentación, una especie de jungla en la que no se aplica ninguna norma? ¿Está justificado afirmar que es urgente elaborar una serie de normas jurídicamente vinculantes, y es factible en la práctica? ¿O habría que tomar como punto de partida la afirmación formulada por el Secretario de Estado para Asuntos Exteriores del Reino Unido, William Hague: "Un comportamiento inaceptable en el mundo real también es inaceptable en línea, corresponda a un individuo o a un gobierno"[41]?

---

39 Política de la OTAN sobre ciberdefensa, Bruselas, 8 de junio de 2010.

40 Gabor Iklody: Discurso pronunciado en el marco del *NATO Information Assurance Symposium*, 11 de septiembre de 2012, Mons.

41 William Hague, Secretario de Estado para Asuntos Exteriores, 11 de noviembre de 2011, en su discurso pronunciado en ocasión de la primera *Cyberspace Conference*, organizada en Londres.

Aplicabilidad del derecho internacional en el ciberespacio

Los expertos debaten desde hace cierto tiempo la cuestión de saber si los instrumentos internacionales elaborados para ámbitos tradicionales se aplican igualmente al ciberespacio. Ese debate, que había perdido un poco de interés después del 11 de septiembre de 2001, cuando se dio prioridad a la guerra contra el terrorismo, ha reaparecido con vigor en 2007-2008. La necesidad de luchar contra el terrorismo ha reavivado en ciertos aspectos ese debate con interrogantes de gran actualidad, por ejemplo: "¿Cómo atribuir los actos de agentes no estatales a un Estado?"; "¿Cuáles son las responsabilidades de un Estado con respecto a las actividades de grupos que operan en su territorio y lanzan ataques contra bienes situados en otro Estado?"; "¿Cómo utilizar legalmente la fuerza contra agentes no estatales que residen en un Estado diferente?" o "¿Se puede hacer uso de la fuerza para prevenir un ataque posiblemente devastador y, en ese caso, en qué condiciones?" Todas estas preguntas son muy habituales en el ciberentorno.

Al parecer, sería conveniente elaborar un acuerdo mundial y jurídicamente vinculante que establezca las principales normas de aplicación en el ciberespacio y que describa las consecuencias del incumplimiento de esas normas. Pero, por el momento, no es posible, ni siquiera deseable, por varios motivos. En primer lugar, la situación evoluciona tan rápidamente que sería prácticamente imposible concertar una serie completa y durable de normas relativas al ciberespacio. En segundo lugar, es innegable la divergencia de las posiciones nacionales sobre cuestiones decisivas que tienen consecuencias prácticas, como la definición de umbrales, los modos de reacción y el cumplimiento. Por tanto, intentar "grabar en el mármol" nuestra interpretación actual del ciberespacio y, ante todo, las posibles concesiones que estaríamos dispuestos a hacer, nos ataría en cierta forma las manos e incluso podría llegar a tener un efecto contraproducente (en particular en países con una cultura más legalista). En tercer lugar, el valor de las obligaciones legales, cuya aplicación es prácticamente imposible de verificar, es cuestionable.

Como muestra la experiencia en otros ámbitos, por ejemplo en el control de armas y el desarme nuclear, si las partes desconfían entre sí es preferible optar por pequeñas etapas para restaurar y consolidar progresivamente la confianza y no poner el listón demasiado alto e intentar imponerse por la fuerza. La experiencia adquirida en el control de armas nucleares nos ha enseñado mucho en este sentido. Las medidas que dejan abiertas las vías de comunicación, que ofrecen una cierta transparencia y contribuyen a calmar las tensiones en tiempos de crisis, podrían ayudar a cumplir el objetivo deseado. Las iniciativas bilaterales y regionales, como los trabajos de la OSCE sobre la confianza en el ciberespacio y las medidas de reforzamiento de la seguridad,

avanzan en la buena dirección, pero también expresan la dificultad de llegar a un acuerdo, aunque sean modestas y de aplicación estrictamente voluntaria.

Esto no significa que sea prematuro considerar desde ahora negociaciones y una cooperación internacional. Además de las medidas de fomento de la confianza que pueden crear las condiciones necesarias para la elaboración de medidas más estrictas, en ciertas esferas las actividades podrían llevarse a cabo con relativa facilidad. Según propone Joe Nye: "Los ámbitos más prometedores para la cooperación internacional no son los conflictos bilaterales sino los problemas planteados por terceros, como los delincuentes y los terroristas"[42]. Con el tiempo, es probable que los intereses de los países avanzados (y por ello también más vulnerables) converjan para limitar los daños causados por grupos delictivos y terroristas, lo que facilitará una mejor cooperación en materia de técnicas forenses y controles. "En primer lugar, los Estados podrían aceptar ser considerados responsables de los ataques perpetrados en su territorio y comprometerse a cooperar en cuanto a técnicas forenses, información y medidas paliativas[43]."

En lo que respecta a las normas internacionales, el próximo paso consiste sin duda en aceptar como punto de partida los instrumentos jurídicos, tanto para el *jus ad bellum* (derecho relativo al uso de la fuerza) como para el *jus in bello* (derecho que regula la conducta durante los conflictos armados) y aplicarlos también en el ciberespacio. De esa forma, se podría progresar y evaluar una a una las disposiciones de esos instrumentos que exigen una interpretación común y las que necesitan un complemento.

En estos dos últimos años se llevaron a cabo dos tentativas importantes a escala internacional para promover una interpretación común del aspecto central de esta cuestión, es decir, los ciberataques. Tanto el Manual de Tallinn, redactado por un grupo de juristas internacionales independientes, con el patrocinio del Centro de Excelencia para la Cooperación en la Defensa del Ciberespacio de la OTAN, como las recomendaciones elaboradas por un Grupo de Expertos Gubernamentales de las Naciones Unidas en el campo de las tecnologías de la información afirman que el derecho internacional en vigor se aplica también al ciberespacio. En consecuencia, no se trata de saber si las leyes actuales se aplican, sino cómo se aplican. Desde luego, las conclusiones de ambos grupos no son vinculantes ni han sido refrendadas por los

---

42 Joseph S. Nye: "Nuclear Lessons for Cyber Security" in *Strategic Studies Quarterly*, invierno de 2011.

43 Eneken Tikk: "Ten Rules of Security", *Survival*, junio-julio de 2011.

Estados, al menos hasta ahora. No obstante, se podría calificar de histórico el acuerdo alcanzado por los expertos.

En el Manual de Tallinn[44], un estudio sumamente profundo y ambicioso elaborado gracias a la invitación del Centro de Excelencia para la Cooperación en la defensa del Ciberespacio de la OTAN situado en Tallinn, se examina exhaustivamente la aplicabilidad de las normas jurídicas a la ciberguerra. Ese Manual contempla únicamente las opiniones de expertos independientes que participaron en los trabajos del Grupo. Puede ser considerado un verdadero intento de iniciar una reflexión sobre una serie de cuestiones importantes y muy delicadas. En otras palabras, es una invitación a participar en esta reflexión y marca el comienzo, y no el fin, de los esfuerzos desplegados para llegar a una interpretación común.

¿Qué se entiende por "uso de la fuerza" o "ataque armado" en el ciberespacio?

Sabemos bastante bien a qué se parece un acto de guerra, pero ¿cómo definir, desde el punto de vista jurídico, el "uso de la fuerza" o el "ataque armado" en el ciberespacio? ¿Un acto no cinético – como un ciberataque – puede calificarse de "ataque armado" o sólo si forma parte de una operación de mayor envergadura? ¿Qué tipo de respuesta a un ciberataque puede considerarse legítima? Esa respuesta, ¿incluye el derecho al uso de la fuerza militar?

No hay una definición universalmente aceptada del término "ciberguerra", que se suele utilizar para describir las hostilidades en el ciberespacio "[...] que tienen repercusiones equivalentes a una violencia física importante, o incluso más graves"[45]. No es pues el simple despliegue de cibermedios ofensivos, sino más bien las consecuencias de su utilización que pueden ayudarnos a determinar si se trata de una ciberguerra. Hasta este momento, nadie ha visto una ciberguerra en el sentido más estricto del término. Se han observado ataques masivos por denegación de servicio dirigidos a un país o a sus infraestructuras esenciales en forma aislada o en el marco de una vasta ofensiva cinética, o ataques puntuales a sistemas de control de empresas del sector privado. "Pero como no se han tenido que afrontar repercusiones imprevistas ni efectos en cascada, puede decirse que no se ha experimentado aún toda la gama de ataques y respuestas de una ciberguerra entre Estados"[46].

---

44 Manual de Tallinn sobre la Aplicabilidad del derecho internacional a los ciberconflictos.

45 Joseph S. Nye, Ibid.

46 Ibid.

La Carta de las Naciones Unidas prevé sólo dos excepciones a la prohibición general del uso de la fuerza: en primer lugar, en el Capítulo VII, cuando el Consejo de Seguridad determine la existencia de una amenaza a la paz, está autorizado a adoptar las medidas que estime necesarias para restablecerla; en segundo lugar, en el Artículo 51, cuando un país ejerce su derecho de legítima defensa, individual o colectiva, que supone reconocer su derecho inmanente de hacer uso de la fuerza contra su agresor.

Es necesario en este punto formular ciertas observaciones. Resulta por lo general difícil llegar a acuerdo en el Consejo de Seguridad de las Naciones Unidas con respecto a la autorización al uso de la fuerza dado que se debe contar con la unanimidad de las "grandes potencias" o, en otras palabras, el derecho de veto de los Miembros Permanentes del Consejo de Seguridad. Es a veces difícil lograr la unanimidad, especialmente en los casos en que uno o más Miembros Permanentes son partes en el conflicto en cuestión. Aparte del menoscabo que supone al carácter democrático del proceso, también se corre el riesgo de que los países opten por considerar ataque armado un caso de uso de la fuerza, lo que, a su vez, justifica el uso de la fuerza contra el agresor. Otro elemento que aboga por una aplicación más amplia del Artículo 51 es el derecho de los Estados a la legítima defensa en caso de ataque terrorista.

¿Qué sucede cuando el atacante no es un Estado sino un agente no estatal, o aparenta serlo? Los redactores de la Carta de las Naciones Unidas han dejado el concepto de "ataque armado" deliberadamente abierto a la interpretación de sus órganos y de los Estados Miembros. Por otra parte, el texto del Artículo 51 es suficientemente vago para autorizar a los Estados que han sufrido un ataque a ejercer su derecho de legítima defensa, aunque ese ataque haya sido cometido por un agente no estatal. La respuesta a los ataques del 11 de septiembre es en ese sentido un ejemplo importante, tanto con respecto a la decisión adoptada por el Consejo de Seguridad de las Naciones Unidas como a las decisiones operativas de la OTAN.

Las operaciones no cinéticas en el ciberespacio, ¿constituyen un "uso de la fuerza", incluso un "ataque armado" o, según la lógica de los redactores de la Carta de las Naciones Unidas, se aplican únicamente al uso de la fuerza militar? En estos últimos años se ha intentado establecer en numerosas ocasiones si la coerción política y económica equivalía al uso de la fuerza. La mayoría de los intentos han fracasado por miedo a abrir una verdadera caja de Pandora si se reconocía que actos no cinéticos podrían desencadenar el uso de la fuerza. Ahora bien, ¿se justifica verdaderamente tener sólo en cuenta los instrumentos utilizados o habría que prestar mayor importancia y atención a las consecuencias?

Preocupan seguramente menos a los gobiernos los instrumentos concretos utilizados en un determinado ataque que las consecuencias de su utilización. Recordemos los ataques del 11 de septiembre: fueron utilizados aviones civiles para provocar deliberadamente daños de gran magnitud y causar víctimas. La regla general podría ser la siguiente: si entraña daños devastadores comparables a los causados por un ataque cinético, un ciberataque debería considerarse un caso de uso de la fuerza, incluso un ataque armado, del mismo modo que una ofensiva militar. En este sentido, poco importa que ese ataque sea aéreo, terrestre, marítimo o que tenga lugar en el ciberespacio; sus consecuencias son las que determinan la manera en que será percibido y otorga al país atacado el derecho de legítima defensa. El caso de Siria es otro ejemplo. La emisión de sustancias químicas mortales se considera generalmente un acto no cinético. Pero la utilización de esas sustancias en Siria contra las poblaciones locales, que ha causado un gran número de muertos y heridos, podría calificarse de uso de la fuerza.

Lo ocurrido con la empresa petrolera Saudi Aramco en 2012 presenta un problema más complejo. Es indudable que la desaparición completa de todos los datos almacenados en más de 30 000 computadoras de la empresa ha sido extremadamente perjudicial, dando origen a una grave situación financiera, resuelta al menos en parte, pero numerosos expertos prefirieron no referirse en este caso a un ataque armado, con todas las consecuencias correspondientes.

¿Cómo determinar entonces si un evento ha cruzado el umbral que autoriza el "uso de la fuerza", pudiendo ser de esa forma equivalente a un "ataque armado"? ¿Cómo evaluar los daños, los sufrimientos y el miedo causados antes de llegar a la conclusión de que es necesaria una respuesta?

Lamentablemente, no hay una respuesta clara a esa pregunta. Con todo, lo que indicamos más arriba sigue siendo cierto, es decir, si las consecuencias de un ataque son tan graves como las de un ataque convencional, puede ser considerado un caso de uso de la fuerza[47]. Hay por tanto una neta correlación entre la gravedad de los daños y el número de víctimas del ataque. Los eventos que causan un gran número de víctimas corresponden a esta categoría, del mismo modo que, probablemente, los ataques que paralizan sectores esenciales de la vida de un país. Pero, ¿se puede establecer un umbral? Evidentemente, no. La decisión de clasificar un evento "uso de la fuerza" o "ataque armado" siempre será puntual y tendrá en cuenta diversos factores.

---

47 Ver los "criterios de Schmitt", una serie de reglas que pueden ayudar a un Estado a determinar si un ciberataque es o no un acto de guerra.

Desde ese punto de vista, la decisión con respecto a qué se considera un acto de guerra tiene un carácter más político que militar o jurídico. Ni siquiera al hablar de terrorismo, después del horror del 11 de septiembre, se podía ser más preciso. ¿Se podría concluir, por ejemplo, que si un ataque terrorista tiene por objetivo civiles inocentes y causa más de 3 000 víctimas, se trata incontestablemente de un ataque armado? ¿Podemos deducir que no es así si el número de víctimas es inferior a un umbral de 3 000? Al margen de otras consideraciones, ¿es el tipo de mensaje que queremos transmitir a criminales en potencia? Me parece que no.

Las operaciones en el ciberespacio se pueden clasificar según diversos criterios. Un modelo generalmente aceptado es el de la CIA, basado en tres elementos (confidencialidad, integridad y disponibilidad) y que ha sido elaborado para identificar problemas y soluciones en materia de tecnologías de la información[48]. Los ataques a la integridad, concebidos específicamente para sabotear el funcionamiento normal de los sistemas de control (por ejemplo, el virus Stuxnet), o los ataques a la disponibilidad (interrupción de sistemas de control del tráfico aéreo o de redes militares, como en Georgia) pueden ocasionar víctimas y su repercusión puede ser comparable a la de un ataque cinético. Por tanto, pueden ser calificados de uso de la fuerza con relativa facilidad. En cambio, los ataques a la confidencialidad (ciberespionaje) pueden dar lugar a pérdidas enormes (sólo para los Estados Unidos, el robo de propiedad intelectual costaría, según estimaciones, unos 250 000 millones USD por año), pero corresponderían a otra categoría y la respuesta es principalmente diplomática.

El espionaje, o segunda profesión más antigua del mundo, se practica a gran escala, y en ocasiones incluso entre aliados muy cercanos. "Globalmente, cada Estado debe conciliar objetivos a veces irreconciliables: acordar la mayor libertad de acción posible y reducir al mínimo los daños. La vigilancia de comportamientos malintencionados tiene precisamente por finalidad general reducir al mínimo los daños, es decir, descubrir cuanto antes las amenazas para que no haya perturbaciones"[49]. En una época en que la prevención y la detección anticipada de intenciones delictivas y actividades malintencionadas son cada vez más importantes para evitar incidentes antes que poner remedio a sus consecuencias, los servicios de inteligencia adquieren mayor protagonismo. No sería pues realista, en el marco de las relaciones internacionales, prohibir las actividades de los servicios de inteligencia en el ciberespacio. Es no obstante "[...] plausible imaginar un intercambio de

---

48 Ver Darril Gibson's "Understanding The Security Triad", *Pearson*, 27 de mayo de 2011.

49 Entrevista con Kah-Kin Ho, Jefe de la ciberseguridad en CISCO.

procedimientos que permita elaborar un "código de ruta" que logre limitar los daños en la práctica".[50]

La utilidad de bajar el umbral del uso de la fuerza para contener la expansión del espionaje está muy presente en el espíritu de numerosos países, en particular de los países menos adelantados. La cuestión tiene más matices en el caso de los países desarrollados, que son a menudo las primeras víctimas de ese espionaje. Al mismo tiempo, suelen ser también los más interesados en mantener un gran margen de maniobra y no son favorables en general a la disminución de ese umbral. Puesto que esos países desean más libertad de acción para adoptar medidas de retorsión y tienen los medios para hacerlo, son también los que tiene más interés en reducir la brecha entre los umbrales del "uso de la fuerza" y el "ataque armado".

Respuesta a un ciberataque

Si un país es víctima de un ciberataque grave, su principal objetivo es, de inmediato, detenerlo y ponerle fin, así como restablecer cuanto antes el funcionamiento de los sistemas dañados. La protección de la población y la recuperación de las redes digitales esenciales son prioritarias. En la mayoría de los casos, se hace todo lo posible para evitar una nueva escalada del conflicto, a menos que se considere necesario el uso de la fuerza para impedir y prevenir nuevos ataques.

Un ciberataque grave perpetrado, por ejemplo, con softwares perniciosos que paralizan el control del tráfico aéreo y pueden causar accidentes de avión y numerosas víctimas, será probablemente considerado un ataque armado que exige una respuesta adecuada. Incluso en ese caso, en virtud del derecho humanitario internacional, la respuesta debe respetar ciertos criterios importantes. Debe ser proporcionada, justificada y necesaria y, además, ajustarse a los principios de distinción y precaución. En cuanto a su contenido, la respuesta puede adquirir varias formas. Puede ser militar, en línea, o consistir en denunciar públicamente al atacante ante las Naciones Unidas. Se puede dar una respuesta por vía diplomática o imponer sanciones. Y se puede también no dar ninguna respuesta.

---

[50] Joseph S. Nye, Ibid.

Los ejercicios que simulan situaciones de la vida real demuestran claramente que los ciberataques masivos y concentrados, lanzados por adversarios capaces e ingeniosos, determinados a infligir daños importantes, no pueden ser frenados únicamente por cibermedios, y mucho menos si esos ataques forman parte de una vasta ofensiva. Si bien las cibermedidas defensivas pueden contribuir a restablecer las redes dañadas y a detectar los ataques, no pueden hacer desaparecer las amenazas. Para ello, un país debe tener en reserva otras medidas.

Acción preventiva

Otra dimensión interesante del problema está vinculada a las especificidades del ciberespacio, en particular el hecho de que los factores tiempo y espacio no tienen importancia: los plazos de advertencia no existen o son muy breves. El tiempo transcurrido entre el momento en que una computadora detecta que va a ser atacada por un software malintencionado y la aplicación de las medidas para detener ese ataque puede ser de apenas unos milisegundos. Para asegurar una defensa eficaz, hacen falta pues respuestas automáticas, lo cual en sí plantea problemas. Dada la velocidad del ataque, la cuestión es saber si un Estado debe esperar que se produzca un ciberataque masivo – similar a un ataque armado (acto puntual dirigido a infraestructuras esenciales o que forma parte de una operación cinética cuya finalidad es destruir centros vitales de mando y control) – o puede ser autorizado a responder de manera preventiva. En este caso, ¿en qué momento los gobiernos pueden intervenir para impedir ciberataques destructivos? ¿Cuáles son las condiciones de un acto de legítima defensa preventivo?

Al parecer, numerosos expertos jurídicos han establecido una norma conocida como "última posibilidad de actuar", en virtud de la cual la inacción en un determinado momento pondría gravemente en peligro la eficacia de la defensa. En el Manual de Tallinn se llega a la conclusión de que un Estado puede actuar en legítima defensa "[...] cuando el atacante está claramente determinado a lanzar un ataque armado y el Estado víctima de ese ataque perderá la ocasión de defenderse eficazmente, a menos que actúe"[51].

La utilización de cibermedios se considera a veces preferible a una solución que podría ser peor. Los países avanzados y poderosos podrían estar tentados a intensificar la utilización estratégica de ciberarmas para convencer a sus adversarios de cambiar su comportamiento o de poner fin a ciertas actividades peligrosas. Esta iniciativa podría

---

51 Manual de Tallinn sobre la Aplicabilidad del derecho internacional a los ciberconflictos.

ser buena si sirviera para evitar una guerra. En cambio, podría hacer más vulnerables a algunos países, poniéndolos a merced de otros agentes más avanzados. El miedo de desencadenar una carrera armamentista generalizada en el ciberespacio, con países que tratan de competir o recurren a mercenarios del ciberespacio no es totalmente infundado. Otro motivo de inquietud es que el código utilizado para ciberataques sofisticados es con frecuencia accesible por Internet a agentes no estatales.

¿Cuál es el nivel de prueba necesario para imputar un ciberataque?

Imputar un ciberataque a un autor con la suficiente certeza suele considerarse a menudo un problema importante que, de hecho, hace prácticamente imposible calificar de "ataque armado" una operación llevada a cabo en el ciberespacio. Sin duda, no hay que ignorar este problema, que es real, pero tampoco habría que sobrestimarlo. Una mayor cooperación internacional y el reforzamiento de las relaciones entre los servicios de inteligencia y los expertos técnicos del ciberespacio, y ante todo la evolución de la tecnología, podrían contribuir a mejorar esta situación.

Si el objetivo es presentar ante los tribunales pruebas claras y convincentes de un vínculo entre el ataque y su autor, la imputación plantea un problema sumamente difícil. Pero este concepto es relativo. En la eventualidad de un ciberataque, habría que aceptar que es prácticamente imposible hallar una prueba irrefutable. Resulta difícil tener una certeza completa y absoluta incluso semanas después del ataque, en el mejor de los casos. Es más realista confiar en la acumulación de pruebas provenientes de diversas fuentes (servicios de inteligencia, técnicos, etc.) que constituirán "pruebas circunstanciales". La imputación es además un concepto relativo en la *Realpolitik*. Las preocupaciones asociadas a las dificultades que plantea la imputación de un ataque a un autor son proporcionales al número de víctimas. En otras palabras, cuanto más elevado sea el número de muertos, más fuerte será la presión ejercida en los Estados para que den una respuesta enérgica al ataque.

Es importante señalar también que la imputación no alcanza para calificar de ataque armado un acto. Recordemos la respuesta de la OTAN a los acontecimientos del 11 de septiembre. En el plazo de 24 horas la Alianza, por primera vez en su historia, invocó los mecanismos de defensa colectiva del Artículo 5. En su formulación, la OTAN no hizo referencia a la posibilidad de imputar el acto terrorista a un Estado, sino que se preguntó simplemente si el ataque a los Estados Unidos estaba dirigido desde el exterior, condición que aseguraba que la cláusula relativa al mecanismo de defensa colectiva no era utilizada contra ciudadanos de países miembros. Se concluye con frecuencia que la disuasión no funciona en el ciberespacio debido a los problemas que plantea la imputación. Es cierto en parte, pero no en el sentido tradicional cuando basta mostrar la fuerza para disuadir a un posible agresor. No obstante, la disuasión

funciona en situaciones que permiten negar las ventajas de un ataque en vez de intentar imponer un castigo mediante represalias, del mismo modo que la defensa antimisil balística vuelve ineficaz o demasiado oneroso el ataque. "Si los cortafuegos son sólidos, o si la perspectiva de una respuesta autoejecutable parece posible, los ataques pierden interés"[52].

Agentes no estatales

En el cibermundo, la mayor parte de las evaluaciones de los servicios de inteligencia coinciden en afirmar que sólo un pequeño número de Estados naciones tienen en la actualidad la capacidad de llevar a cabo ataques complejos y sostenidos que pueden causar daños graves. Al mismo tiempo, como ha declarado W.J. Lynn, Secretario Adjunto de Defensa, [...] "si bien los Estados tienen las capacidades más importantes, es más probable que un ataque con consecuencias catastróficas sea perpetrado por agentes no estatales"[53].

Desearía detenerme en este punto y establecer una neta distinción entre el espionaje, por una parte, y las perturbaciones y destrucciones devastadoras, por la otra, incluso si ambas, técnicamente, están muy próximas. Es indudable que hay que hacer todo lo posible para entorpecer el espionaje y el robo de informaciones de gran valor sobre el Estado y las empresas, pero la prioridad absoluta es eliminar el riesgo de ataques que tengan consecuencias devastadoras.

La buena noticia es que, en lo que concierne a la posición en materia nuclear, la mayoría de los Estados naciones piensan de manera racional e intentarán probablemente no cruzar las líneas rojas para no provocar reacciones violentas. Para que los países comprendan esta situación, deben saber en primer lugar que existe una línea roja. El mensaje debe ser transmitido sin ambages: un ataque devastador podría desencadenar medidas de retorsión nacionales o colectivas que podrían utilizar todo medio a disposición[54]. En segundo lugar, es posible poner progresivamente en marcha medidas de fomento de la confianza y de reducción de las tensiones, así como ciertas reglas básicas, como ya se indicó anteriormente, aprovechando una vez más la experiencia adquirida en el campo nuclear.

---

52 Joseph S. Nye, Ibid.

53 W.J.Lynn, Secretario Adjunto de Defensa, Observaciones pronunciadas en el *28º Taller internacional anual sobre seguridad mundial, París, 16 de junio de* 2011.

54 Discurso de Gabor Iklody ante el Global Intelligence Forum de AFCEA, Bruselas, 10-11 de diciembre de 2013.

Resulta más difícil esperar un comportamiento racional de algunos "Estados irresponsables" cuya ambición es poner en práctica cibercapacidades ofensivas que adquieren gracias a grandes inversiones. No es fácil disuadir a esos Estados y, como lo recuerdan algunos analistas de regiones cuya situación es explosiva, para ciertos países y ciertas culturas, un contexto en el que todos pierden puede ser una opción perfectamente aceptable.

Con todo, lo más inquietante es el potencial de agentes no estatales. La pesadilla absoluta sería que la capacidad de hacer daño se asocie a la intención de hacerlo, a todo precio. No hemos llegado aún a eso, pero el miedo de que los terroristas utilicen ciberarmas no pertenece al reino de lo imposible. En Internet se encuentra una serie de herramientas "listas para usar", que pueden ser mejoradas. Hay mercados negros del "día cero" y cibermercenarios o piratas muy capaces que alquilan sus servicios para robar dinero o secretos industriales, e incluso, utilizando prácticamente las mismas herramientas y técnicas, para causar perturbaciones masivas.

1.4 La ciberseguridad según las Naciones Unidas

por Hamadoun I. Touré

En la presente sección se describe la visión de las Naciones Unidas sobre ciberseguridad. En la actualidad, las TIC cumplen un papel fundamental y la seguridad de esos sistemas tiene una importancia decisiva. Las economías de los países desarrollados dependen en gran medida de las TIC, incluso para sus infraestructuras esenciales, y la ciberseguridad adquiere por tanto una prioridad absoluta, de lo cual son plenamente conscientes numerosos países. A los países en desarrollo se les ofrece una oportunidad única de crear una infraestructura de la comunicación esencialmente segura y, por tanto, de dar un paso de gigante en su desarrollo.

Sin embargo, la ciberseguridad está lejos de ser una prioridad para todos los países y, con frecuencia, las estrategias nacionales en materia de TIC y desarrollo ni siquiera la mencionan. Al incorporar la ciberseguridad en los programas de desarrollo y al considerarla "un medio al servicio de un fin" y no un fin en sí, las Naciones Unidas intentan cambiar la situación. El presente artículo aborda las necesidades actuales en el mundo en materia de ciberseguridad, la visión de las Naciones Unidas con respecto a su evolución y los mecanismos existentes, y describe en forma sucinta las iniciativas en curso o previstas en el ámbito de la ciberseguridad.

La ciberseguridad: un imperativo en todo el mundo

Las TIC tienen un "poder de transformación"[55] que ha alcanzado prácticamente cada sector de actividad en los países desarrollados y dado lugar a rápidas transformaciones en los países en desarrollo. No obstante, la omnipresencia de las redes informáticas tiene un costo: la vulnerabilidad creciente de sectores económicos enteros a los ciberataques. Esas amenazas son diversas: pequeños delitos, robos de números de tarjetas de crédito o ataques coordinados de alcance mundial, como el virus informático Conficker. Sus autores actúan por lo general en el anonimato[56], haciendo todavía más difícil una acción judicial. Por otra parte, los servicios tradicionalmente encargados de hacer cumplir la ley disponen de pocos recursos en la esfera de la ciberseguridad y los ataques son a menudo lanzados desde otros países. Esos factores se combinan y crean una situación compleja que plantea problemas técnicos y políticos a todos los países: es imperativo proteger la integridad, la confidencialidad y la disponibilidad de las informaciones fundamentales y los datos personales.

Varios países desarrollados han hecho de la ciberseguridad una prioridad nacional[57]. Ante una red concebida con un espíritu de apertura, y no de seguridad, los países gastan enormes recursos para proteger sus redes (según estimaciones, más de 70 000 millones USD en 2014)[58]. Aunque esos gastos corresponden en su inmensa mayoría a países de altos ingresos, resultan al parecer insuficientes teniendo en cuenta los ataques constantes a nuevos sectores de la economía[59].

Por motivos tan diversos como el afán de ganancia o el activismo político, las ciberamenazas pueden proceder de casi todos los países y afectar vastos sectores de la economía. Ninguna entidad ni ningún Estado pueden afrontarlas por sí solos de manera eficaz. Es pues urgente desplegar en el mundo entero esfuerzos concertados en busca de la ciberseguridad.

---

55 Discurso del Secretario General de la UIT, Hamadoun I. Touré – Cumbre Transformar África, Unión Internacional de Telecomunicaciones, 28 de octubre de 2013, Web, 24 de julio de 2014.

56 Nazli Choucri, Stuart Madnick & Jeremy Ferwerda, Information Technology for Development (2013): "Institutions for Cyber Security: International Responses and Global Imperatives, Information Technology for Development," DOI: 10.1080/02681102.2013.836699.

57 "Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet economy." *Organización para la Cooperación y el Desarrollo Económicos,* 2012.

58 "Defending the Digital Frontier." *The Economist*, 12 de julio de 2014.

59 "Hackers Inc." *The Economist*, 12 de julio de 2014.

Con todo, la ciberseguridad no se limita simplemente a las "ciberarmas" o los "ciberataques". Una estrategia general consistiría en proteger tanto el derecho a la información como el derecho al respeto de la vida privada en el ciberespacio, dos derechos humanos fundamentales reconocidos en tratados internacionales. La protección del ciberespacio fomentaría pues el desarrollo económico y la confianza, permitiendo así crear un entorno más seguro que proteja a los particulares de toda intrusión en sus datos. Por este motivo, la comunidad internacional debe acelerar sus acciones para que la ciberseguridad constituya una prioridad absoluta en el mundo entero.

Para las Naciones Unidas, la ciberseguridad se funda en cuatro pilares: 1) protección de las redes de cada organización; 2) prestación de asistencia (coordinada) a los Estados Miembros[60] para la elaboración y aplicación de políticas nacionales en materia de ciberseguridad; 3) integración de la ciberseguridad en los programas de desarrollo; y 4) impulso a la cooperación internacional para cuestiones relativas a la ciberseguridad, el ciberdelito y la protección de los derechos humanos en línea, en particular el respeto de la vida privada y el acceso a la información. El presente artículo hace referencia a los tres últimos pilares, los más pertinentes para el estudio del tema "La búsqueda de la confianza en el ciberespacio", que serán examinados uno a uno.

Según las Naciones Unidas, esas tres prioridades se basan en principios comunes. En primer lugar, para una seguridad eficaz de las tecnologías de la información, las Naciones Unidas preconizan un enfoque global, "con el conjunto de los gobiernos" y numerosos interesados. En sus trabajos internos, las Naciones Unidas deberían seguir esta doctrina y pasar a una estrategia "interorganismos" en la cual las entidades correspondientes coordinen sus actividades para ser más eficaces y evitar la duplicación de tareas. En segundo lugar, dado el carácter dinámico de las tecnologías de la información, las Naciones Unidas recomiendan la adopción de políticas poco estrictas, que serán examinadas con frecuencia, y, en la medida de lo posible, independientes de la tecnología. Por último, la elaboración de políticas debe prestar una atención prioritaria a las consecuencias de las medidas de seguridad en otras prioridades definidas a escala mundial, como la protección de la vida privada.

---

60 En el marco del mandato de cada organismo y en el respeto de la soberanía nacional.

Asistencia a los Estados Miembros

Los organismos de las Naciones Unidas ayudan desde hace tiempo a los Estados Miembros a elaborar políticas vinculadas a las TIC. Sin embargo, la ciberseguridad es considerada una prioridad desde hace muy poco. Con la elaboración de un Marco sobre ciberseguridad y ciberdelito para todo el sistema de las Naciones Unidas, aprobado en 2013, la Junta de los Jefes Ejecutivos (JJE) del Sistema de las Naciones Unidas para la Coordinación[61] ha llegado a un acuerdo sobre ciertos principios comunes que deberían seguirse al prestar asistencia a los Estados Miembros. Ese marco, que representa una primera etapa en la armonización de las actividades internas realizadas por las Naciones Unidas en materia de ciberseguridad, se examinará más adelante[62].

Integración de la ciberseguridad en los programas de desarrollo

El desarrollo de las TIC (de la cual forma parte la ciberseguridad) es considerado por lo general una prioridad distinta de otras esferas de desarrollo tradicionales, que se estiman que exigen más atención y son más urgentes. Sin embargo, no hay ninguna contradicción entre el desarrollo de las TIC y los temas generales del desarrollo sostenible: la evolución técnica no es un fin en sí misma sino un medio que permite a los países, en particular a los países en desarrollo y a los países menos adelantados (PMA), reforzar sus capacidades en diversos sectores de la economía, mejorando de esa forma el bienestar social y las condiciones de vida generales. No faltan ejemplos en los que la tecnología ha permitido mejorar el acceso a aguas salubres, a la educación y a una atención de la salud asequible, además de impulsar el crecimiento económico y estimular o facilitar el comercio internacional.

Es pues imperativo incluir la ciberseguridad en las prioridades de desarrollo *existentes*: sistemas seguros y fiables aumentan la probabilidad de su adopción. Al respecto, los países en desarrollo y los PMA disponen de circunstancias excepcionalmente favorables: al desarrollar redes informáticas intrínsecamente seguras, pueden quemar etapas y evitar sistemas que ya son objeto de ataques. Las inversiones en ciberseguridad pueden contribuir a reducir aún más la "brecha digital". Las organizaciones del sistema de las Naciones Unidas pueden desempeñar un papel fundamental en la materia aprovechando mecanismos internacionales en vigor para integrar los programas de ciberseguridad.

---

61 Ver el punto 85 del Informe de la Segunda Sesión Ordinaria de la JJE para 2013 (noviembre de 2013).

62 Ver la sección relativa a "Mecanismos de las Naciones Unidas para la ciberseguridad".

Otra prioridad a escala mundial es evitar la aparición y escalada de ciberconflictos. Aunque hasta ahora los países han sido bastante reticentes a responder a los ciberataques[63], no está claro que siga siendo así a mediano o largo plazo. La finalidad de las actividades de investigación y educación del Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) es contribuir a prevenir la escalada de conflictos, dado que este Instituto "[...] sirve de puente para crear las sinergias necesarias para atenuar y luchar contra las consecuencias de la inseguridad a nivel internacional, regional y local."

Impulso a la cooperación internacional en materia de ciberseguridad

Aunque las actividades en línea estén sujetas a diversas reglamentaciones de un país a otro, Internet sigue siendo en lo esencial una red mundial. Es particularmente cierto en lo que concierne a la ciberseguridad, ámbito en el cual los ataques y las amenazas trascienden cada día las fronteras nacionales. Fue lo que ocurrió, por ejemplo, con el virus informático Conficker, que causó daños en más de 180 países[64]. Ningún país puede por sí solo resolver los problemas de la ciberseguridad, y para las Naciones Unidas es prioritario, a escala mundial, alentar la cooperación internacional en esa esfera.

Una de las prioridades de las Naciones Unidas para garantizar la confianza en el ciberespacio es considerar este asunto en el marco de la protección de los derechos humanos en línea. Como prioridades más destacadas se pueden citar el derecho a la vida privada y el derecho a la información. Este último está amenazado por diversos comportamientos, entre ellos la violación de datos y una inversión insuficiente en la protección de los datos. El derecho a la información depende de un acceso seguro a las TIC que permita la libertad de expresión y el acceso libre a contenidos públicos. Los programas de seguridad de las TIC deben tener en cuenta estos intereses divergentes, como lo muestran las políticas nacionales de numerosos países[65], principalmente los países desarrollados. Los principios R-O-A-M, según los cuales Internet debe fundarse en los derechos humanos, ser abierta y accesible a todos, y permitir la participación de numerosos actores, constituyen una base firme para proseguir los trabajos. La Organización de las Naciones Unidas para la Educación, la Ciencia y la

---

63 Valeriano, B., & Maness, R. C. (2014). "The dynamics of cyber conflict between rival antagonists, 2001-11." *Journal of Peace Research*. doi:10.1177/0022343313518940.

64 "Conficker." ShadowServer. Shadowserver Foundation, n.d. Web. 4 de noviembre de 2013.

65 Ver *supra*, § 2.

Cultura (UNESCO), que tiene una importante experiencia en la protección de los derechos humanos en todo el mundo, ha considerado esta visión de la ciberseguridad en sentido amplio como una de las prioridades del desarrollo sostenible.

Dado el predominio de los actores del sector privado en la economía de Internet, e incluso en la gestión de la red propiamente dicha, los esfuerzos desplegados para lograr esa protección deben ser coordinados con otros interesados además de los gobiernos, por ejemplo, el sector privado, la comunidad técnica y la sociedad civil. El reforzamiento de esta cooperación cumple una función particularmente determinante en las encuestas judiciales, en el marco de las cuales una asistencia mutua puede ser útil a todos los interesados.

Directrices básicas en materia de ciberseguridad

El surgimiento del ciberespacio como un espacio global de las comunicaciones internacionales ha supuesto – junto con los incontables beneficios que aporta un mundo más interconectado – una amenaza importante para la seguridad y la estabilidad de los Estados Miembros de las Naciones Unidas. La confidencialidad de la información, los sistemas informáticos, las infraestructuras esenciales y los servicios en red son todos vulnerables a los ataques por Internet, lanzados periódicamente en todo el mundo. Garantizar la seguridad del ciberespacio en esas circunstancias[66] requiere una estrategia:

- global (o "del conjunto de los gobiernos") puesto que la prevención[67] y la detección de los ciberataques, la atenuación de sus efectos y la persecución de sus autores supone una infinidad de gobiernos y de entidades del sector privado;
- que incluya a los interesados en el sector de las TIC, comprendidos los encargados de adoptar políticas, los proveedores de servicios Internet y de telecomunicaciones, las organizaciones técnicas y las organizaciones no gubernamentales de protección de los derechos humanos (o "sociedad civil");
- favorable a políticas flexibles y dinámicas que puedan adaptarse a la evolución constante de las tecnologías y que permitan responder a amenazas y vulnerabilidades, manteniendo a su vez una innovación sin restricciones; y

---

66 Esta sección no constituye un censo completo de las directrices de las Naciones Unidas en materia de ciberseguridad; en su lugar, presenta un resumen sucinto de las tendencias comunes descritas en las obras consultadas.

67 Incluida la creación de capacidades a nivel del usuario.

- respetuosa de los derechos humanos, en particular el derecho al respeto de la vida privada y al acceso a la información.

Mecanismos de las Naciones Unidas para la ciberseguridad

Ya se han puesto en marcha en las Naciones Unidas destacados marcos sobre ciberseguridad, por ejemplo el Marco sobre ciberseguridad y ciberdelito para todo el sistema de las Naciones Unidas; la Línea de Acción C5 de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), "Creación de confianza y seguridad en la utilización de las TIC"; y la Red de Tecnologías de la Información y la Comunicación (Red TIC). Cada uno de ellos será descrito en las subsecciones siguientes. En esta sección se presentan igualmente ciertos mecanismos de ciberseguridad en curso de elaboración en el sistema de las Naciones Unidas.

Marco sobre ciberseguridad para todo el sistema de las Naciones Unidas

Como parte de los esfuerzos desplegados para afrontar las amenazas en el ciberespacio, las Naciones Unidas han creado, a nivel de todo ese sistema, un Marco sobre ciberseguridad y cibederlito que propone a todas sus entidades miembros directrices destinadas a dar respuesta a las preocupaciones de los Estados Miembros en la materia y a reforzar la coordinación entre ellos para mejorar la confianza y la seguridad en el ciberespacio.

Las actividades delictivas en Internet tienen un alcance y una frecuencia muy variables. El Marco pretende abordar una parte importante de esas amenazas estableciendo principios básicos que deben seguir todas las entidades de las Naciones Unidas, de acuerdo con sus mandatos respectivos. Los trabajos se centran en la prevención de los delitos y en la alerta temprana, el reforzamiento de capacidades a escala nacional, la eficacia de la disuasión y la importancia de la justicia en la lucha contra el ciberdelito. Ese Marco incluye aspectos técnicos y de capacitación para ayudar a los Estados Miembros y utiliza una estrategia global de sensibilización y mayor conocimiento de las capacidades de respuesta ante las ciberamenazas.

Como se define en el Marco[68], la ciberseguridad se refiere al conjunto de documentos, prácticas, políticas y tecnologías utilizadas para "[…] garantizar que se alcancen y mantengan las propiedades de seguridad" de las organizaciones, la información, los sistemas y los activos correspondientes. Pero, ¿contra qué la ciberseguridad asegura

---

[68] El Marco utiliza la definición de la Unión Internacional de las Telecomunicaciones, que figura en la "Recomendación UIT-T X.1205".

una protección? Además de reforzar la confianza en las tecnologías de la información, combate las actividades delictivas relacionadas con la informática o, en otras palabras, el ciberdelito[69]: conjunto de "[…] temas [que] comprenden las violaciones de la confidencialidad, la integridad y la disponibilidad de datos informáticos" y de infraestructuras; y conjunto de "… actos [delictivos] relacionados con la informática", así como con los datos.

Principios relacionados con la ciberseguridad y el ciberdelito

Con objeto de delimitar el alcance de ese Marco en todo el sistema de las Naciones Unidas, el documento está organizado en torno a siete grandes principios que pueden hallar sin dificultad una traducción política. Se pueden resumir de la siguiente manera:

1. Las entidades de las Naciones Unidas deberían ayudar a los Estados Miembros a afrontar los ciberincidentes de forma global, incluida la prestación de apoyo técnico a la justicia penal y el reforzamiento de la cooperación internacional.
2. Habría que tener en cuenta los mandatos de esas entidades al examinar las necesidades de los Estados Miembros, buscando la cooperación con otras organizaciones pertinentes de la Naciones Unidas.
3. Todos los programas de las Naciones Unidas en materia de ciberseguridad y ciberdelito deberían respetar los derechos humanos y el estado de derecho.
4. La planificación de las Naciones Unidas debería, siempre que sea posible, ayudar a los Estados Miembros a adoptar una estrategia basada en los hechos cuando efectúen la evaluación de los delitos y riesgos.
5. En la medida de lo posible, habría que adoptar un modelo de respuesta "del conjunto de los gobiernos" que implique a todos los interesados en el plano nacional, así como a actores no estatales, como las ONG, las instituciones académicas y la comunidad técnica.
6. El apoyo prestado a los Estados Miembros debería apuntar a reforzar mecanismos formales e informales de cooperación internacional en materia de ciberseguridad y de ciberdelito
7. Para dar una respuesta eficaz a las ciberamenazas, habría que alentar la cooperación entre entidades públicas y privadas en los Estados Miembros, así como la armonización y la adopción de normas técnicas y directrices en materia de políticas y seguridad a escala regional e internacional.

---

69 Como se define en el Marco.

La asistencia a los Estados Miembros se encuentra por tanto en el núcleo del Marco: su finalidad es mejorar la ciberseguridad y reforzar la seguridad y fiabilidad de Internet. En ese Marco se presentan recomendaciones destinadas a aplicar los principios mencionados y a ofrecer esa asistencia con eficacia. Las directrices enunciadas se pueden clasificar en tres categorías: medidas de carácter jurídico y político, asistencia técnica y mecanismos de implantación.

Asistencia técnica

En un entorno de naturaleza tan técnica como el ciberespacio, el fomento de capacidades y la formación en conocimientos básicos sobre ciberseguridad se consideran fundamentales para los Estados Miembros. En el Marco se recomienda realizar en los países evaluaciones detalladas de las capacidades técnicas como punto de partida indispensable, además de elaborar políticas nacionales de ciberseguridad. Concretamente, la asistencia técnica prestada por entidades de las Naciones Unidas podría incluir: publicaciones técnicas sobre el ciberdelito y su economía; mecanismos de intercambio de información (prácticas óptimas y otras formas de conocimientos generales); formación en técnicas de investigación digital y otras técnicas de investigación sobre ciberdelito, incluida la formación del usuario final en la utilización segura de las computadoras y las redes; cooperación con los proveedores privados de servicios Internet y con otros interesados en la recopilación y análisis de los datos; respuestas en caso de incidentes informáticos, incluida la creación de instituciones permanentes encargadas de gestionar esos incidentes (como los equipos nacionales de intervención en caso de incidente informático, CIRT) y "puntos centrales de contacto para responder a las demandas formuladas desde el extranjero".

Línea de Acción C5 de la CMSI

Como se indicó en los documentos establecidos en la fase de 2003[70] de la Cumbre de la CMSI y reexaminados durante el Evento de Alto Nivel CMSI+10 en 2014, la Línea de Acción C5 de la CMSI se centra en la creación de confianza y seguridad en la utilización de las TIC, cuya labor fue confiada a la UIT en calidad de entidad facilitadora. En 2007, la UIT lanzó la Agenda sobre Ciberseguridad Global (GCA) "[…] con el fin de ofrecer un marco dentro del cual la respuesta internacional a los recientes desafíos suscitados por la ciberseguridad pueda coordinarse y abordarse" con los Estados Miembros y otros interesados pertinentes. A este respecto, la UIT ha concluido acuerdos de

---

70 Cumbre Mundial sobre la Sociedad de la Información http://www.itu.int/wsis/index.html, última actualización el 13.10.2014.

asociación con todos los interesados del mundo entero para hacer avanzar la ciberseguridad, que guardan relación, entre otras cosas, con la publicación de directrices para la formulación de políticas nacionales en la materia[71], la prestación de asistencia técnica a los Estados Miembros para ayudarlos a reforzar sus competencias y el impulso de debates sobre las normas técnicas necesarias para mejorar la seguridad.

Red TIC

La Red TIC es un mecanismo de la Junta de los jefes ejecutivos del sistema de las Naciones Unidas para la coordinación. Esa red, que reagrupa las capacidades TIC de numerosas entidades de las Naciones Unidas con respecto a la toma de decisiones, coordina actividades y sirve de foro para la elaboración y puesta en práctica de políticas relativas a las TIC. En lo que concierne a la presente publicación, lo que más nos interesa es su Grupo de interés para la seguridad de la información, que analiza cuestiones vinculadas a la ciberseguridad "[…] mediante presentaciones de expertos y de estudios de casos, [y el examen de] ámbitos en que las instituciones tienen una acción común, por ejemplo las respuestas en caso de incidentes, la seguridad y las políticas de la información y la sensibilización en la seguridad de la información"[72].

Trabajos en curso

Como han reconocido tanto los Estados Miembros de las Naciones Unidas como la JJE[73], es preciso coordinar los trabajos, en el sistema de las Naciones Unidas, relativos a la ciberseguridad y el cibederlito. Tras la aprobación en 2013 del Marco sobre ciberseguridad y ciberdelito para todo el sistema de las Naciones Unidas, el Secretario General de las Naciones Unidas, Ban Ki-Moon, hizo un llamamiento para que la UIT, junto con la UNESCO, la UNODC, el PNUD y la UNCTAD, y en estrecha colaboración con el Comité de Alto Nivel sobre Gestión (HLCM) y el Grupo de las Naciones Unidas para el Desarrollo (GNUD), elaboraran, para todo el sistema, una estrategia completa y coherente que permitiera resolver las cuestiones con el fin de

---

71 ITU National Cybersecurity Strategy Guide (Guía de la UIT sobre Estrategias nacionales en materia de ciberseguridad), septiembre de 2011.

72 Grupo de intereses especiales sobre seguridad de la información, Naciones Unidas – Junta de los Jefes Ejecutivos (JJE) del Sistema de las Naciones Unidas para la Coordinación, 2014. Web. 22 de julio de 2014.

73 "Action on Cybersecurity/Cybercrime and Policies on Information", JJE de las Naciones Unidas, 21 de noviembre de 2011. Web. 22 de julio de 2014.

debatirla durante la segunda reunión ordinaria de la JJE en noviembre de 2014[74], trabajos que están en curso de elaboración.

Conclusión

Todos los países coinciden en la necesidad de dar una respuesta universal y concertada a los problemas de la ciberseguridad. Las Naciones Unidas tratan estas cuestiones en su globalidad, con la participación de numerosos interesados, en el respeto de los derechos humanos y siguiendo un modelo flexible y dinámico. Aunque todavía no se ha alcanzado ningún acuerdo sobre una visión de la ciberseguridad, se observan, en los trabajos de las entidades de las Naciones Unidas, algunos elementos y tendencias comunes que ponen de relieve la prioridad acordada desde hace poco a la ciberseguridad. Se admite actualmente que la seguridad del ciberespacio es una necesidad universal que tiene claras repercusiones en el desarrollo económico y social, en tanto que resulta fundamental conciliar intereses divergentes y respetar la soberanía nacional. Las perspectivas de la ciberseguridad parecen prometedoras, como ha sido reconocido por Choucri y otros[75]: "Aunque el sistema actual de acuerdos institucionales [internacionales] [sobre ciberseguridad] muestra signos de debilidad, también es cierto que ha aumentado paulatinamente la concertación y la cooperación."

Esta tendencia positiva es un incentivo adicional a la cooperación internacional en materia de ciberseguridad. Dado que Internet, por su naturaleza, es una red mundial, sólo los esfuerzos de alcance mundial (o casi mundial) pueden lograr la seguridad del ciberespacio. Los costos de las perturbaciones causadas en los servicios por los ciberataques pueden ser bastante elevados, en particular en sectores decisivos como la distribución de energía eléctrica o las finanzas, pero se compensan con creces debido a las ventajas que supone invertir en ciberseguridad. Esto resulta aún más evidente para los países desarrollados con infraestructuras sumamente interconectadas. Por otra parte, los países en desarrollo tienen la ocasión histórica de quemar una etapa de su desarrollo y el hecho de dar prioridad a la ciberseguridad puede indudablemente mejorar sus perspectivas.

---

74 Ver el apartado 85 del Informe de la segunda reunión ordinaria de la JJE, noviembre de 2013.

75 Ver *supra, §* 2.

Estos cambios sólo se harán realidad cuando la ciberseguridad sea realmente una prioridad mundial. Las Naciones Unidas, con su gran experiencia en el desarrollo de nuevas iniciativas, se encuentran en una posición inmejorable para cumplir la función de entidad facilitadora de las actividades de ciberseguridad en el mundo; los Estados, el sector privado y la sociedad se beneficiarán en gran medida de contribuir a llevarlas a cabo.

Capítulo II: Ciberresiliencia

Introducción

En febrero de 2005, el Comité Asesor en Tecnologías de la Información del Presidente de los Estados Unidos hizo un llamamiento a la acción[76] para reforzar la seguridad en el ciberespacio[77] en un Informe histórico titulado "Cyber Security: A Crisis of Prioritization". La Academia Nacional de Ingeniería de los Estados Unidos publicó en 2008 una lista de los "14 grandes retos para el siglo XXI". En los últimos años muchas otras fuentes han abordado este reto de la instauración de la confianza en el ciberespacio en el futuro mundo digital.

Desde entonces, nuestra dependencia de las ventajas que nos ofrece la era digital ha seguido aumentando de manera exponencial a medida que los equipos y sistemas informáticos y de la comunicación son cada vez más omnipresentes y esenciales en prácticamente todos los aspectos de nuestra vida cotidiana.

De ahí la crucial importancia de mantener un ciberespacio seguro y de instaurar la resiliencia para afrontar la amenaza creciente de los ciberataques, que pueden causar estragos y tener efectos destructores a gran escala.

---

76 Comité Asesor en Tecnologías de la Información del Presidente de los Estados Unidos, "Cyber Security: A Crisis of Prioritization" (febrero de 2005).

77 Academia Nacional de Ingeniería: "Grand Challenges for Engineering"; http://www.engineeringchallenges.org/cms/challenges.aspx

La utilización creciente de las tecnologías de sensores, sistemas ciberfísicos, servicios en la nube, *Big Data* o sistemas autoadaptativos inteligentes[78] ampliará en gran medida las capacidades de las TIC e influirá en nuestra vida, mientras se avanza inexorablemente hacia la Internet de las Cosas.

Esta tendencia se debe no sólo a los adelantos tecnológicos sino también a la incesante demanda de nuevos mercados y productos. La mejora de ciberinfraestructuras y ciberservicios ofrecerá mayores posibilidades y beneficios, pero también dará lugar a nuevos puntos vulnerables y a nuevas amenazas que corren el riesgo de socavar la protección y la seguridad privadas y públicas de nuestras sociedades.

Los retos son considerables, en particular porque la confianza en la era digital y también nuestro bienestar general dependen en gran medida de nuestra capacidad para identificar y gestionar una amplia gama de ciberamenazas. Tras un análisis y una evaluación rigurosa de las vulnerabilidades y los riesgos, es preciso definir medidas adecuadas para garantizar la ciberseguridad – o por lo menos una ciberresiliencia adecuada – en particular para las infraestructuras esenciales como la energía, el agua, el transporte, la salud y los sistemas financieros[79].

Entre las fuentes de posibles riesgos para la estabilidad y la seguridad en el ciberespacio se encuentran la creciente complejidad y la utilización progresiva de las infraestructuras y servicios TIC. Incluso más graves son las amenazas que representan acontecimientos externos, como las catástrofes ambientales o los ataques por gobiernos, organizaciones delictivas o particulares. Las investigaciones han mostrado que los diseñadores de sistemas, los operadores o los usuarios pueden ser una fuente importante de vulnerabilidad para las TIC, de forma intencionada o no. Al respecto, los problemas científicos y técnicos de base que deben resolverse guardan relación con las cuestiones de "complejidad-emergencia-resiliencia" en el ciberespacio.

---

78 Markus Luckey Gregor Engels: "High-Quality Specification of Self-Adaptive Software Systems", en: Proceedings of the 8th International Symposium on Software Engineering for Adaptive and Self-Managing Systems. ACM (Nueva York, NY, USA), SEAMS '13, pp. 143-152; (2013).

79 US Executive Order 13636: "Improving Critical Infrastructure Cybersecurity"; (febrero de 2013): http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

En primer lugar, el presente capítulo explica la terminología con respecto a la complejidad de la TIC, los riesgos en el ciberespacio y los comportamientos inesperados, así como el motivo por el cual es cada vez más necesario elaborar estrategias para asegurar la ciberresiliencia. Destaca además las numerosas fuentes potenciales de ciberriesgos – errores y fallos físicos, técnicos o medioambientales, y también causas orgánicas, institucionales o legislativas – y trata la identificación de ciberriesgos, su análisis y estrategias de resiliencia hasta el nivel de información desde el punto de vista informático y técnico. Los capítulos siguientes abordarán los problemas de la resiliencia para aplicaciones de "*Big Data*" y de la "computación en la nube", así como para la demanda de sistemas de cibercontrol resilientes. Por último, el presente capítulo contiene contribuciones relativas a la ciberresiliencia desde la perspectiva del sector privado, y en el Capítulo 2.4 se trata un ciberriesgo no técnico importante y se propone un marco jurídico internacional requerido con urgencia para luchar contra otros riesgos existentes no vinculados a la simple protección de los datos.

2.1 Fundamentos de la ciberresiliencia

por Axel Lehmann

Terminología

Como ya se ha indicado, la creciente complejidad del mundo digital que influye tanto en nuestra vida pública como privada, plantea un verdadero problema desde el punto de vista de las medidas de fomento de la confianza. En general, **la complejidad de un sistema (digital)** depende del número y las funcionalidades de sus componentes que determinan el espacio de estado del sistema.

Las supercomputadoras son los equipos de mayor potencia, y su capacidad máxima debería permitir el tratamiento de unos 1 000 PetaFLOPS – 1 000 billones de operaciones de coma flotante por segundo – en la próxima década[80]. Los sistemas ciberfísicos (en su mayoría, microdispositivos de cálculo invisibles e integrados) ofrecen únicamente capacidades de cálculo muy especializadas y limitadas.

---

80 Calculador Exascale, ver: http://en.wikipedia.org/wiki/Exascale_computing

Una conectividad mayor entre diversos sistemas permite crear el llamado "sistema de sistemas" (utilizado por ejemplo para regular los sistemas de alimentación de energía, de comunicaciones o de control del tráfico)[81]. El almacenamiento de información es otro importante servicio global que debe tenerse en cuenta en lo que respecta a la ciberconfianza; las tecnologías de almacenamiento están evolucionando incluso más deprisa que las tecnologías informáticas (la capacidad de almacenamiento crece permanentemente con una disminución considerable de los costos).

La complejidad general de los sistemas que hay que gestionar aumenta también de forma exponencial debido al aumento del número de componentes y de capacidades de un sistema, así como del número de sistemas interconectados en el "sistema de sistemas" redimensionable.

Estos adelantos tecnológicos en curso necesitan métodos de diseño, desarrollo y de control de la calidad particularmente robustos para garantizar la estabilidad del sistema, su disponibilidad – sin olvidar las estrategias de resiliencia en caso de situaciones no deseadas[82] – y la ciberconfianza. La aplicación más frecuente de métodos bien definidos para la especificación y el diseño de los sistemas puede asegurar que se detecten y eviten ciertos estados del sistema (inseguros o críticos) si se ponen en marcha medidas adecuadas de identificación y prevención. Sin embargo, eventos o peligros que no fue posible prever durante el diseño pueden provocar un comportamiento del sistema inesperado que podría resultar difícil o incluso imposible de controlar o corregir. En el caso más desfavorable, el sistema podría colapsar y no se podría volver a su estado operativo. Por todos estos motivos, es preciso elaborar y aplicar métodos adecuados para asegurar la ciberresiliencia.

Es imprescindible identificar, analizar y evaluar esas amenazas, vulnerabilidades y riesgos, y definir las contramedidas correspondientes. El diseño de sistemas digitales según los métodos probados de diseño y tolerancia a los fallos mejorará significativamente su robustez y su facilidad de control, pero no evitará totalmente los comportamientos emergentes, en particular en el caso de un sistema de sistemas. Por tanto, es preciso examinar y poner en práctica métodos y procedimientos de ajuste para aumentar **la resiliencia de sistemas y procesos**, etapa importante para establecer la confianza en ellos y en el ciberespacio en general.

---

81 Mo Jamshidi: "System-of-systems engineering: a definition"; en: IEEE SMC; (2005).

82 "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; publicado por Ashgate Publishing Limited; (2006).

Según la definición de Wreathall[83], "[…] la resiliencia es la capacidad de una organización (o de un sistema) de mantener, o de recuperar con rapidez, un estado estable que le permita seguir funcionando durante y después de un incidente importante o ante presiones importantes y continuas." En el Foro Económico Mundial de 2012 se creó la iniciativa "Asociaciones para la ciberresiliencia" y se formularon algunos "Principios y directrices en materia de riesgos y responsabilidades en un mundo hiperconectado"[84]. Dada la amplia variedad de usuarios humanos, diseñadores, operadores, dispositivos digitales y sistemas que constituyen este mundo digital complejo, y puesto que los estudios han mostrado que los seres humanos son los más vulnerables, las medidas de fomento de la confianza deben tener particularmente en cuenta sus actividades.

Identificación y clasificación de los ciberriesgos

En un mundo en el que los seres humanos dependen considerablemente de los recursos cibernéticos, el análisis de los ciberriesgos y de la resiliencia en el ciberespacio deben tener en cuenta una gran diversidad de perspectivas que comprendan tanto los actores humanos como la variedad y complejidad de la era digital. El espectro de recursos en el ciberespacio va desde las infraestructuras y los servicios digitales internacionales que se pueden utilizar en todo el mundo hasta los dispositivos informáticos o ciberfísicos independientes.

Por otra parte, en relación con las actividades humanas en el ciberespacio – por ejemplo, en tanto que diseñadores, fabricantes o usuarios – hay que distinguir sus funciones y capacidades según se utilicen sistemas digitales desde el interior o desde el exterior de esos sistemas. Con respecto a la jerarquía, y también a la clasificación de la identificación, el análisis y la prevención de ciberriesgos, se pueden distinguir los niveles de abstracción o capas enumerados a continuación. Puesto que las interrupciones y las deficiencias que se producen a niveles inferiores pueden tener una gran incidencia en el comportamiento y el funcionamiento del sistema a niveles superiores, un análisis y una evaluación globales de los riesgos deben tener en cuenta

---

83 John Wreathall: "Properties of Resilient Organizations: An Intitial View"; en: Resilience Engineering – Concepts and Precepts, Ashgate Publishing Limited; (2006).

84 Foro Económico Mundial: "Partnering for Cyber Resilience"; Boletín de febrero de 2013 – Davor Edición especial http://www3.weforum.org/docs/WEF_RRHW_PartneringCyberResilience_NewsletteFebruary_2013.pdf; (2013).

todos los factores siguientes como requisito previo para la elaboración de estrategias de resiliencia del sistema[85, 86]:

- nivel global;
- capa empresa/nivel institucional/privado;
- nivel de información;
- nivel técnico;
- nivel físico.

Análisis de los ciberriesgos y la ciberresiliencia desde la perspectiva de la informática y la técnica

Con el fin de efectuar un análisis profundo de los ciberriesgos y de definir estrategias de ciberresiliencia, se deben identificar en primer lugar las principales fuentes de ciberriesgos en cada uno de los niveles indicados. En una segunda etapa, hay que analizar y evaluar detalladamente cualesquiera efectos secundarios (dependencias), puesto que los errores, fallos, averías o intrusiones en un nivel inferior pueden afectar las funcionalidades, la fiabilidad o la confidencialidad y la seguridad en niveles superiores. Con ese fin, se utilizan gráficos de dependencia[87] para detectar las dependencias mutuas siguiendo, en un sentido u otro, los trayectos entre los niveles, lo cual permite detectar las causas del disfuncionamiento, de los fallos, de las averías, de la pérdida o de la corrupción de los datos.

Como se muestra en la Figura 1, cada nivel proporciona ciertas capacidades, ciertas funcionalidades o ciertos servicios (cx), que incorporan o utilizan atributos de niveles inferiores, como lo indican las flechas. Las flechas de trazo discontinuo indican que la implantación de cada capacidad (cx) requiere cumplir determinadas normas, reglamentos o reglas. En la Figura 1 se identifica una deficiencia a nivel de la empresa, causada probablemente por un error, un fallo o una intrusión en ese nodo o en un

---

85 "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; publicado por Ashgate Publishing Limited; (2006).

86 Lorenzo Strigini: "Fault tolerance and resilience: meanings, measures and assessment"; en: K. Wolter y otros. (eds.), Resilience Assessment and Evaluation of Computing Systems, Springer-Verlag, Berlin Heidelberg; (2012).

87 Algirdas Avizienis, Jean-Claude Laprie, Brian Carl: "Basic Concepts and Taxonomy of Dependable and Secure Computing"; IEEE Transactions on Dependable and Secure Computing; (2004).

nodo de nivel inferior. Siguiendo la estructura del gráfico (hacia adelante o hacia atrás), se pueden localizar las posibles fuentes de un error, un fallo o una avería.

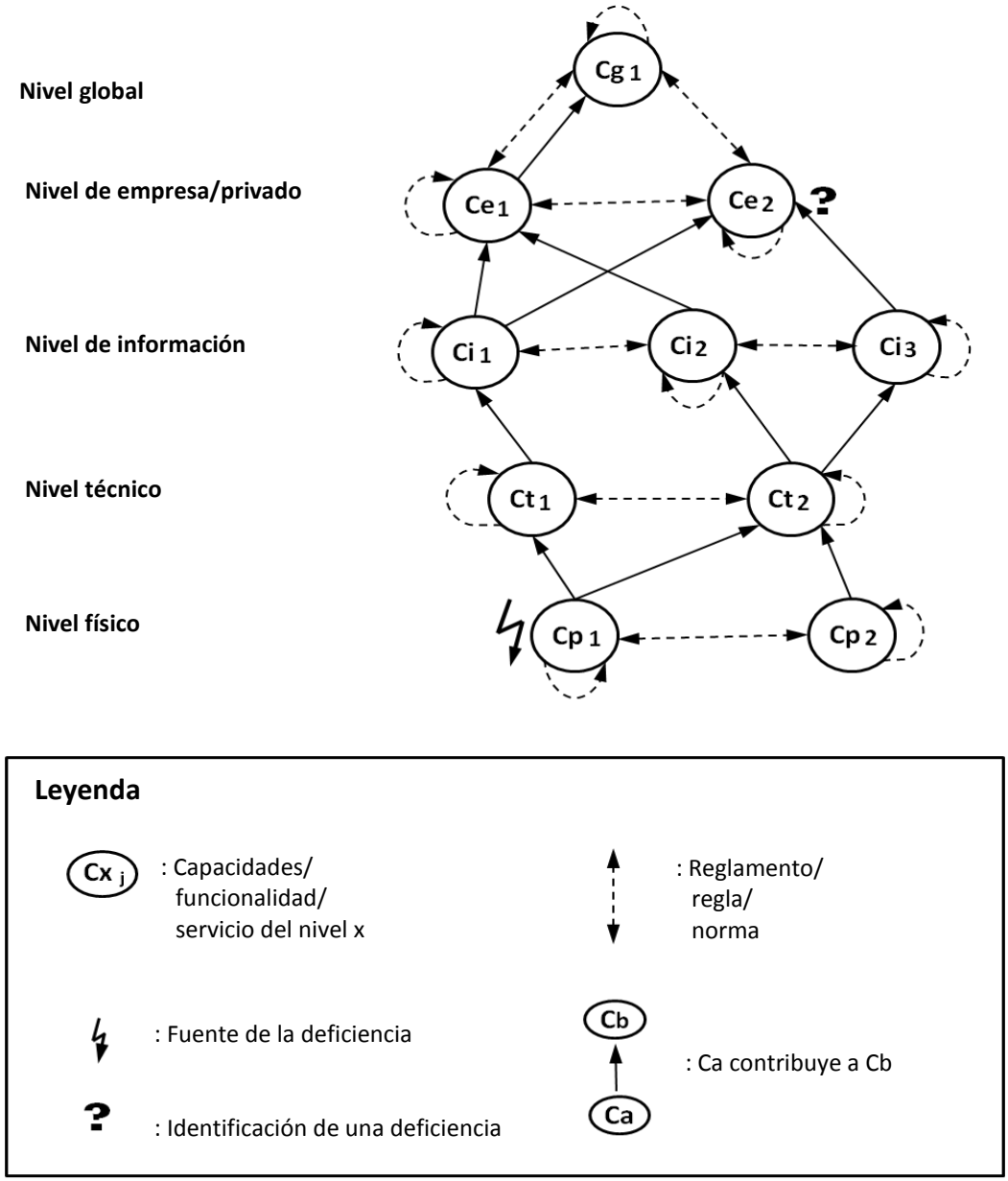

Figura 1: Ejemplo de gráfico de dependencia

Como ya hemos visto, la rápida evolución de las TIC permite avances técnicos importantes pero al mismo tiempo aporta nuevas fuentes y causas de ciberriesgos, que afectan a la estabilidad y la seguridad en el ciberespacio. Además de las deficiencias técnicas y físicas, las principales fuentes de riesgos en el ciberespacio provienen de la tendencia a la virtualización de los recursos de cálculo, de comunicación y de almacenamiento generada por la demanda de una mejor calidad de funcionamiento, de la fiabilidad y de la relación costo-eficacia para la comunidad de usuarios. La rápida evolución de las tecnologías, como los *Big Data*, la computación en la nube y los recursos de software como servicio (SaaS) que utilizan la nube[88], los sistemas de sistemas[89] y las "hiperredes"[90] ponen en evidencia esta tendencia.

Esos adelantos tecnológicos también dan lugar a nuevos problemas de ciberseguridad en relación con la vida privada, la confidencialidad y la autenticidad. Además de la utilización abusiva, la manipulación y la corrupción de los datos y de las infraestructuras TIC, esas tecnologías suponen nuevos riesgos para la recopilación, la utilización y el reagrupamiento no autorizados de datos personales o de otros datos confidenciales. El peligro, ya comprobado en ciertos casos, radica en que diferentes tipos de datos protegidos que pertenecen a personas, organizaciones o incluso Estados se vuelven "visibles", lo que socava la confianza en el ciberespacio.

En general, los riesgos se pueden calcular de la siguiente forma:

Riesgo = Probabilidad * Impacto

Desde un punto de vista técnico, los ciberriesgos pueden deberse a errores de diseño, a fallos o a averías de los componentes digitales durante el funcionamiento, a disfunciones o a comportamientos imprevistos del sistema, en particular en el caso de sistemas "hiperconectados". También pueden ser causados por una utilización errónea o prácticas indebidas de un sistema digital, por un ataque proveniente del interior del sistema o de un usuario, por un accidente inesperado o por un evento medioambiental. Para reducir al mínimo esos riesgos vinculados a las TIC, hay que tener en cuenta una relación más precisa de análisis de los riesgos: Riesgo-TIC: = f (amenaza, vulnerabilidad, activo).

---

88 Nicolas Gold, Andrew Mohan; Clair Knight, Malcolm Munro: "Understanding Software-Oriented Software"; en: IEEE Software; (2004).

89 Mo Jamshidi: "System-of-systems engineering: a definition"; en: IEEE SMC; (2005).

90 "Resilience Engineering"; Eds. Erik Hollnagel, David Woods, Nancy Leveson; publicado por Ashgate Publishing Limited; (2006).

En el contexto de las TIC, la vulnerabilidad de un sistema TIC está relacionada con los puntos débiles o las deficiencias de diseño o de ejecución, o de aplicaciones erróneas, que pueden causar averías, una reducción de capacidades, un disfuncionamiento de los componentes del sistema o incluso el colapso del sistema. Es preciso en primer lugar identificar y clasificar esas vulnerabilidades antes de pensar en las posibles soluciones. Al respecto, se debe realizar una evaluación de los riesgos relacionados con las TIC, luego clasificar las vulnerabilidades de la infraestructura y los servicios y las contramedidas correspondientes por orden de prioridad. Seguidamente, se podrá realizar un análisis cuantitativo de los riesgos, por ejemplo de la manera siguiente:

Riesgo-TIC = (Vulnerabilidad * Amenaza / Nota de la contramedida) * Valor del activo

Como requisito previo para la elaboración de una estrategia de resiliencia para las TIC, hay que llevar a cabo un análisis de fiabilidad (o de seguridad de funcionamiento) y de disponibilidad que deberían tener en cuenta los siguientes métodos genéricos para mejorar la fiabilidad y la disponibilidad del sistema[91]:

- *Prevención de fallos* – evitar que se produzcan errores o fallos mediante un diseño y una fabricación minuciosos.
- *Supresión de fallos* – detectar los errores que podrían dar lugar a fallos o averías aplicando métodos de prueba, de verificación y de validación.
- *Tolerancia a los fallos* – prever un sistema redundante (por ejemplo, duplicar recursos y/o diversificar implantaciones) que solucione o permita un ajuste en caso de avería.
- *Previsión de fallos/averías* – analizar y evaluar las consecuencias de las averías que pueden causar un fallo del sistema, así como las consecuencias en el funcionamiento del sistema[92].

Desde un punto de vista analítico, los gráficos de dependencia (como el de la Figura 1) o los diagramas funcionales de fiabilidad son métodos sencillos para analizar los efectos directos e indirectos de los errores, fallos o averías, así como de las contramedidas concretas indicadas *supra*[93].

---

91 Algirdas Avizienis, Jean-Claude Laprie, Brian Carl: "Basic Concepts and Taxonomy of Dependable and Secure Computing"; IEEE Transactions on Dependable and Secure Computing; (2004).

92 Ibid.

93 Ibid.

Además de esas vulnerabilidades relacionadas con las TIC, se deben tener en cuenta, con respecto a la confianza en el ciberespacio, otras amenazas causadas por deficiencias. "Una amenaza es un peligro potencial que podría aprovechar una vulnerabilidad para violar la seguridad y, de esa manera, causar daños. Por lo tanto, se deben examinar y evaluar otras amenazas debidas a las actividades de los usuarios humanos que afectan los recursos del sistema, a accidentes, a catástrofes naturales o a otros eventos externos inesperados."[94]

Las actividades humanas que constituyen una amenaza pueden llevarse a cabo de manera intencional (por ejemplo, por usuarios internos, piratas informáticos) o ser el resultado no intencional de una operación o de un comportamiento del usuario. Para el análisis de los riesgos, se deben determinar las actividades humanas que más daño pueden causar y analizar las vulnerabilidades correspondientes. Además de las vulnerabilidades y las amenazas, los análisis de los ciberriesgos deben tener en cuenta su incidencia en las capacidades, los activos y el valor de los diferentes componentes de un sistema.

Para fomentar la ciberresiliencia convendría considerar los siguientes enfoques[95]:

- Prevención de deficiencias – evitar que se produzcan deficiencias como errores, fallos y averías a niveles físico y técnico concibiendo, poniendo en práctica y explotando de manera minuciosa el sistema y los procedimientos de funcionamiento; a niveles superiores, se puede conseguir aplicando a cada nivel normas, reglamentos y reglas de comportamiento aceptadas.
- Supresión de deficiencias – detectar las deficiencias que podrían dar lugar a fallos, averías, disfunciones o a una utilización indebida aplicando métodos de prueba, de verificación y de validación.
- Tolerancia a las deficiencias – prever un sistema redundante (por ejemplo, duplicar recursos y servicios y/o diversificar implantaciones) que solucione o permita un ajuste en caso de deficiencia.
- Previsión de deficiencias – estudiar las vulnerabilidades en casos plausibles efectuando numerosas simulaciones, analizando los riesgos correspondientes

---

94 Lorenzo Strigini: "Fault tolerance and resilience: meanings, measures and assessment"; In: K. Wolter et al. (eds.), Resilience Assessment and Evaluation of Computing Systems, Springer-Verlag, Berlin Heidelberg; (2012).

95 Ibid.

y evaluando las consecuencias de la puesta en marcha de estrategias de resiliencia en ese contexto.

La elaboración de una estrategia global de resiliencia que se basa en esos análisis de los riesgos y de la fiabilidad requiere además mecanismos de ajuste y de recuperación que permitan a un sistema recuperarse totalmente por sí mismo a partir de un estado de indisponibilidad, de estados de calidad de funcionamiento degradada o después de una intrusión. La mayoría de los sistemas naturales o biológicos han desarrollado mecanismos de autorregeneración o de autorreconfiguración. En el caso de los sistemas técnicos, por ejemplo en procesos u organizaciones que funcionan como organismos biológicos – denominadas capacidades informáticas orgánicas – los correspondientes métodos de cobertura, de ajuste y de recuperación deben examinarse y utilizarse como hipótesis en la etapa de concepción del sistema. Los estudios científicos relativos a la informática y la comunicación orgánicas se centran en este tipo de métodos biológicos que pueden mejorar la resiliencia de sistemas TIC y ciberfísicos, conceptos que deben utilizarse para la implantación de sistemas digitales de auto-x (x se puede sustituir, por ejemplo, por protección, regeneración, optimización o configuración)[96]. A partir de los resultados de los trabajos de investigación en ámbitos como la ingeniería del conocimiento o la exploración de datos, los principios de diseño de sistemas inteligentes han evolucionado y se pueden aplicar para la identificación y evaluación de riesgos permanentes, así como para tomar medidas preventivas que permitan la resiliencia del sistema.

Las medidas enunciadas a continuación, que se presentan del nivel inferior al superior del sistema, son ejemplos de medidas que pueden tomarse en cada nivel para evitar fallos, disfunciones, averías o interrupciones, o para asegurar su recuperación cuando se producen esas situaciones, y también para mejorar la ciberresiliencia desde el punto de vista de la ingeniería informática[97, 98, 99]:

---

96 "Organic Computing"; Ed. Rolf Würtz; In: Springer series Understanding Complex Systems; Springer (2008).

97 Yue Yu, Michael fry, Alberto Schaeffer-Filho et.al.: "An Adaptive Approach to Network Resilience: Evolving Challenge Detection and Mitigation"; en: 8th IEEE Internat. Workshop on the Design of Reliable Communication Networks; (2011).

98 Dorothy Reed, Kailash Kapur, Richard Christie: "Metzhodology for Assessing the Resilience of Networked Infrastructure"; en: IEEE Systems Journal, Vol. 3 No. 2; (2009).

99 Piotr Cholda, Anders Mykkeltveit et. al.: "A Survey of Resilience Differentiation Frameworks in Communication Networks"; en: IEEE Communications, Surveys, Vol.9 No.4; (2007).

- a nivel físico – restricciones sobre la utilización de materiales y dispositivos únicamente en determinadas condiciones ambientales predefinidas (por ejemplo, con respeto a las temperaturas, la radiación). Además, se puede asegurar una cierta redundancia utilizando otros materiales, procesos de explotación opcionales, etc., o diversificando la utilización de un componente;
- a nivel técnico – dispositivos de cálculo (n de m), conceptos de transmisión y codificación de datos redundantes o la utilización de protocolos de transmisión seguros diferentes pero normalizados con soluciones no sólo para evitar la propagación de fallos sino también para permitir el autoajuste. Por otra parte, la diversificación mediante, por ejemplo, la creación de algoritmos de cálculo diferentes, de diversos nodos de cálculo o la utilización de diferentes conceptos de almacenamiento, son otras medidas para evitar la propagación de fallos, para reforzar la fiabilidad de un sistema y para permitir la resiliencia a nivel técnico[100];
- a nivel de la información – el objetivo es "preservar la confidencialidad, la integridad y la disponibilidad de la información. Además, también se pueden considerar otras propiedades, como la autenticidad, la imputabilidad, el no repudio y la fiabilidad. " (ISO/IEC 27000)[101]. Las medidas son, por ejemplo, la codificación redundante o la utilización de algoritmos de encripción y descifrado robustos, o de protocolos de transmisión de datos protegidos para evitar fallos, la utilización indebida o la corrupción; en lo que respecta a las herramientas, se pueden instalar a nivel de la empresa/privado sistemas y redes SCADA (control de supervisión y adquisición de datos)[102] con objeto de respetar las buenas prácticas, los procesos comerciales, las secuencias de tareas y las normas, reglas y restricciones en materia de seguridad establecidas, y de aplicar códigos de conducta internos[103];

---

100 Departamento de Energía de los Estados Unidos: "21 Steps to Improve Security of SCADA Networks"; (2011); http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

101 Norma ISO/CEI 27000: Tecnologías de la información - Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Visión General y Vocabulario; (2014).

102 Departamento de Energía de los Estados Unidos: "21 Steps to Improve Security of SCADA Networks"; (2011); http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

103 Amy Lee, John Vargo, Erica Seville: "Developing a Tool to Measure and Compare Organizations Resilience"; en: Nattural Hazards Review; ASCE, febrero (2013).

- a nivel de la empresa/institucional/privado – un marco de leyes y reglas de funcionamiento; códigos de conducta institucionales, regionales y culturales; enseñanza adecuada; difusión de la información y capacitación para dar mejor a conocer las cuestiones de ciberseguridad;
- a nivel global – respetar acuerdos de política aceptados en todo el mundo y, siempre que sea posible, códigos de conducta internacionales; en concreto, establecer un marco de leyes y reglas de funcionamiento internacionales, crear y aplicar códigos de conducta regionales y culturales; asegurar una enseñanza adecuada; difundir el material didáctico y proponer la capacitación para para dar mejor a conocer las cuestiones de ciberseguridad.

Esta lista de medidas y métodos destinados a reforzar la ciberseguridad y, por lo tanto, la confianza en el ciberespacio, no es exhaustiva.

2.2 Aumentar la resiliencia de los sistemas de computación en la nube y de los *Big Data*

por Vladimir Britkov

Los *Big Data* y la computación en la nube son las principales novedades en la esfera de las TIC. Según las estimaciones de la empresa Gartner, el 64% de las organizaciones del mundo entero han invertido en *Big Data* o prevén hacerlo. Se trata de cantidades enormes de información digital sobre los seres humanos y nuestro entorno, cuyo volumen está previsto que se duplique cada dos años. La tecnología de los *Big Data* comprende el nuevo ámbito de la "inteligencia empresarial", que permite una mayor ciberresiliencia en materia de *Big Data* y computación en la nube.

Las infraestructuras en la nube a gran escala, el volumen y la diversidad de las fuentes y los formatos de datos, el carácter ininterrumpido de la adquisición de datos así como la circulación de un volumen importante de datos de una nube a otra generan numerosas vulnerabilidades de seguridad particulares. Por lo tanto, los mecanismos de seguridad tradicionales, adaptados para proteger datos estáticos (y no transmitidos de forma continua), son inadecuados. En el presente artículo ponemos de relieve los diez principales factores que permitirán proteger la seguridad y la confidencialidad de los *Big Data*, los cuales, esperamos, contribuirán a dar mayor prioridad al reforzamiento de las infraestructuras de los *Big Data*.

La confianza, factor "ineludible" de una relación comercial fructífera entre un proveedor de servicios en la nube y un cliente, es una de las principales cuestiones que guardan relación con la seguridad. Sin embargo, no existe ningún vínculo de confianza particular que garantice que ningún ataque proveniente del interior del sistema o algún otro incidente de seguridad amenacen las informaciones almacenadas en la nube. Como es natural, las empresas consideran que ése es un factor esencial cuando deciden recurrir a un proveedor de servicios en la nube. Los clientes pueden no obstante concertar un acuerdo de nivel de servicio (SLA) con el proveedor que estipule las condiciones de la relación contractual entre el cliente y el proveedor de servicios en la nube. Esos acuerdos tienen especial importancia en lo que respecta a la protección de los datos del cliente almacenados en la nube pero, dado que la nube es por naturaleza internacional, se extiende generalmente a numerosas jurisdicciones, cuyas prescripciones jurídicas aplicables son con frecuencia diferentes.

Tradicionalmente, las infraestructuras de los *Big Data* eran oficialmente privadas y estaban aisladas de las redes generales. Cuando se combinan con la adopción de metodologías de explotación de datos, los *Big Data* son ahora accesibles con facilidad y a bajo precio para las organizaciones, grandes o pequeñas, gracias a la infraestructura pública en la nube. Las infraestructuras de los programas informáticos permiten a los diseñadores aprovechar fácilmente millares de nodos de cálculo para el tratamiento paralelo de datos. Para proteger la infraestructura de los sistemas de *Big Data*, se debe garantizar la seguridad de la computación distribuida y los almacenes de datos. Para asegurar la seguridad de los datos, la difusión de la información debe preservar la confidencialidad y los datos sensibles deben ser protegidos mediante la utilización de la criptografía y un control de acceso granular.

La gestión del volumen enorme de datos necesita soluciones redimensionables y distribuidas tanto para proteger la seguridad del almacenamiento de datos como para permitir auditorias eficaces y conocer la procedencia de los datos. Por último, el flujo ininterrumpido de datos que proviene de diferentes puntos extremos debe ser verificado desde el punto de vista de la integridad y puede utilizarse para analizar en tiempo real los incidentes de seguridad con la intención de garantizar la integridad de la infraestructura.

Se enumeran a continuación los diez factores que permitirán asegurar la seguridad y la confidencialidad de los *Big Data*:

1. Seguridad de las operaciones de cálculo en los marcos de programación distribuida.
2. Aplicación de prácticas óptimas de seguridad para las memorias de datos no relacionales.

3. Seguridad de las memorias de datos y de catálogos de transacciones.
4. Validación/filtrado en la entrada de puntos extremos.
5. Verificación de la seguridad en tiempo real.
6. Exploración y análisis de los datos preservando la confidencialidad, redimensionable y acomodable.
7. Seguridad centrada en los datos reforzada por elementos criptográficos.
8. Control de acceso granular.
9. Auditorias detalladas.
10. Proveniencia de los datos.

Creación de una infraestructura de *Big Data* segura

Para resolver los problemas que plantean la seguridad y la confidencialidad, hay que abordar por lo general tres cuestiones diferentes:

1. Modelización: establecer un modelo de amenaza que abarque la mayoría de los casos de ciberataque o de pérdida de datos.
2. Análisis: encontrar soluciones fáciles de utilizar basadas en el modelo de amenaza.
3. Aplicación: poner en marcha la solución en las infraestructuras existentes.

Hacia una computación segura en marcos de programación distribuida

Caso de utilización: Modelización

El modelo de amenaza para los *mappers* consta de tres casos principales:

1. Disfuncionamiento de los nodos de cálculo subordinados – Los nodos subordinados asignados a los *mappers* en una operación de computación distribuida podrían funcionar indebidamente a causa de una configuración incorrecta o de un nodo defectuoso.
2. Ataques a la infraestructura – Los nodos subordinados comprometidos pueden interceptar la comunicación entre otros nodos subordinados y el nodo maestro con objeto de lanzar un ataque por repetición, un ataque por intermediario (*Man-In-The-Middle*) o un ataque por denegación de servicio en las operaciones de computación efectuadas según el marco MapReduce.
3. Nodos de datos fraudulentos – Se pueden añadir nodos de datos fraudulentos a un grupo y, seguidamente, recibir datos replicados o entregar un código MapReduce alterado.

Análisis

Sobre la base del modelo de amenaza indicado antes, hay dos dimensiones de análisis: garantizar la credibilidad de los *mappers* y dar seguridad a los datos a pesar de *mappers* no fiables. Dos técnicas permiten garantizar la credibilidad de los *mappers*: la instauración de la confianza y el control de acceso obligatorio (MAC).

Puesta en marcha

Se pone en marcha el MAC modificando el marco MapReduce, el sistema de archivos distribuidos y la máquina virtual Java que utiliza SELinux como sistema de explotación subyacente.

Conclusión

Los *Big Data* han venido para quedarse. Resulta prácticamente imposible imaginar que la próxima generación de aplicaciones no consuma datos, no genere nuevas formas de datos ni contenga algoritmos basados en datos.

Debido a la reducción del costo de los entornos informáticos, a la conexión de los entornos de aplicaciones y a la utilización común de los entornos de sistemas y analíticas en la nube, la seguridad, el control de acceso, la compresión, la encripción y la conformidad generan riesgos que deben ser tratados de forma sistemática. Los retos correspondientes figuran en la lista de los diez principales problemas de seguridad y de confidencialidad enunciados *supra*, que deben resolverse para que la infraestructura informática y del tratamiento de *Big Data* sea más segura y resiliente.

Los elementos comunes propios de los *Big Data* surgen a partir de la utilización de numerosas categorías de infraestructuras (tanto de almacenamiento como de cálculo) para su tratamiento; de la utilización de nuevas infraestructuras de cálculo, como las bases de datos NoSQL (para el elevado caudal que exigen los enormes volúmenes de *Big Data*), que no han sido objeto de un examen de seguridad suficientemente exhaustivo; de la imposibilidad de modular la encripción de grandes volúmenes de datos; la imposibilidad de modular las técnicas de control en tiempo real que podrían ser aplicadas para volúmenes de datos menos importantes; de la heterogeneidad de los dispositivos que producen los datos y de la poca claridad con respecto a las diversas restricciones jurídicas y políticas que dan lugar a la aplicación de estrategias ad hoc para garantizar la seguridad y la confidencialidad.

2.3 Creación de sistemas de cibercontrol resilientes

por Stefan Lüders

La vida en nuestro mundo actual "occidentalizado" se rige por sistemas de control que regulan prácticamente todos los aspectos de nuestra cotidianeidad. Nuestra vida está en simbiosis[104] con esos sistemas de control, de los que depende inextricablemente. Sin ellos, volveríamos rápidamente a condiciones de vida similares a las de la Edad Media[105]. Dada nuestra dependencia de esos sistemas de control, es esencial garantizar su estabilidad y su resiliencia.

Sin embargo, esos sistemas de control son hoy vulnerables a los fallos de los sistemas informáticos estándar que los hacen funcionar. Utilizan las mismas técnicas que los centros informáticos modernos: el protocolo Ethernet, TICP/IP, la World Wide Web y el correo electrónico han reemplazado las comunicaciones por bus de terreno patentadas; con las computadoras ya no es necesario disponer de pantallas, indicadores y monitores; el sistema de explotación Microsoft Windows sustituye los terminales con líneas de mando personalizadas.

Por otra parte, es raro que los software sean de gran calidad; por lo general, contienen defectos, fallas y errores. Para responder a las demandas del mercado, los software se comercializan en su versión beta, es decir, en estado de funcionamiento, pero con fallas y puntos vulnerables que son detectados (y eliminados) posteriormente. Los usuarios y las empresas no piden necesariamente que los mejoren debido a los costos que entrañaría.

Como si eso no bastara, las tecnologías de la información estándar han dado lugar a un mercado de la delincuencia verdaderamente nuevo, una "red oscura" donde los atacantes se asocian para infiltrar y explotar los sistemas de esas tecnologías, poniendo así en riesgo la confianza de los usuarios. Hoy, personas malintencionadas buscan permanentemente los puntos vulnerables y las fallas de cada aplicación Internet, de cada sitio web, de cada sistema de explotación y de cada aplicación informática de gran difusión para utilizarlos en su propio beneficio o para venderlas en

---

104 Ver también el artículo de Stefan Lüders "Our Life in Symbiosis", Boletín del CERN, 2014.

105 Todo ello está bien descrito en la novela de Marc Elsberg "Blackout: Morgen ist es zu spät" Blanvalet, marzo de 2012.

ese mercado "oscuro". Y puesto que la prevención o el fortalecimiento de la resiliencia ante esos ataques son operaciones infinitamente más complejas que la explotación de esas vulnerabilidades, los atacantes se benefician de una verdadera ventaja.

Sin embargo, las tecnologías de la información en general han mostrado ser suficientemente resilientes para que esos ataques no tengan grandes repercusiones en nuestra vida cotidiana y, pese a que la economía "oscura" sigue prosperando y a que el sistema jurídico internacional hace lo posible para ir al compás de esa evolución, es raro que las consecuencias sean graves para el público en general[106].

El desarrollo exponencial de los sistemas de control y su incorporación en las tecnologías de la información estándar han cambiado la situación. Aunque esos sistemas sacan partido de las tecnologías de la información, han heredado también sus puntos vulnerables y sus fallas. Por ese motivo, procesos de control sólidos, patentados y personalizados se fragilizan y quedan expuestos, siendo cada vez más por otra parte el objetivo de personas malintencionadas, como lo indican los siguientes titulares de los medios: "Rusia en la mira de los *hackers*" (The Register, 2000), "*Hackers* atacan el sistema de gestión del agua de Pensilvania" (InTech, 2006), "Las plantas eléctricas de la TVA vulnerables a los ciberataques" (The Washington Post, 2008), "Un empleado acusado por haber pirateado el sistema de control del canal de California" (Computerworld, 2009), "El tráfico aéreo en los Estados Unidos expuesto a un "grave riesgo" de ciberataques" (Flightglobal, 2009), "La red eléctrica de los Estados Unidos infiltrada por espías" (The Wall Street Journal, 2009), "Informe: Se han introducido *hackers* en los sistemas de control del tráfico aéreo de la FAA" (CNET, 2009), "Informe: Ciberataques causan cortes de electricidad en Brasil" (Wired, 2009), "DHS: Los servicios de agua y electricidad estadounidenses víctimas de ciberataques cotidianos" (Computerworld, 2012), "Protección insuficiente de represas, estaciones de bombeo y puentes" (Radio Netherlands Worldwide, 2012), "La red eléctrica de los Estados Unidos vulnerable a casi todo" (OilPrice.com, 2012). El sabotaje de instalaciones de enriquecimiento de uranio de Nantax en Irán, que habría sido realizado por los servicios secretos israelíes y estadounidenses, es otra noticia publicada recientemente: "El virus Stuxnet marca el inicio de una nueva era en la ciberguerra" (Spiegel Online, 2010). Computadoras infectadas por el virus "Stuxnet" han falsificado las pantallas que observan los operadores de las instalaciones, se descargaron ellas mismas en el sistema de control y modificaron la velocidad de

---

106 Excepto tal vez en el caso de ataques llevados a cabo por organismos gubernamentales a servidores mundiales de nombres de dominio, a las principales vías de Internet y, más generalmente, a la vida privada de los ciudadanos.

rotación de centenares de centrifugadores, impidiendo de esa manera el enriquecimiento de uranio.

En tanto que "Stuxnet" es considerado el primer cibersabotaje demostrado, pone también en evidencia el dilema que representan los ciberataques lanzados con la ayuda del Estado. Richard A. Clarke, antiguo Coordinador nacional para la seguridad y el contraterrorismo en la Casa Blanca, declaró que los Estados Unidos estarían en condiciones de hacer saltar una central nuclear o un campo de entrenamiento terrorista en cualquier parte del mundo, pero un cierto número de países podrían responder con un ciberataque y "las represalias podrían lograr el derrumbamiento de todo el sistema económico del país (...) porque no podemos defenderlo hoy".

De hecho, actualmente es imposible proteger los sistemas de control con técnicas similares a las utilizadas para proteger instalaciones como los centros informáticos, por ejemplo con "correctivos", es decir, eliminar los puntos vulnerables poniendo al día el sistema de explotación.

Los centros informáticos modernos responden a sistemas de gestión de la configuración. Por lo general, es posible poner al día e incluso reinstalar un gran número de servidores en un plazo de tiempo muy breve. Las redundancias y la virtualización facilitan ese proceso, debido al mantenimiento de los subgrupos de torres de servidores mientras el servidor principal sigue funcionando. En cambio, es actualmente imposible utilizar correctivos flexibles para los sistemas de control porque las ventanas de mantenimiento son raras y las exigencias en materia de conformidad estrictas, en particular con respecto a los procesos de seguridad pertinentes. Se considera que únicamente son seguros los sistemas plenamente conformes y certificados (por ejemplo, recertificación a un nivel de seguridad integrada, SIL), pero efectuar pruebas completas lleva tiempo y entraña costos suplementarios. Además, no siempre está garantizado que los nuevos correctivos para sistemas de explotación sean compatibles con los softwares utilizados por los sistemas de control, y los fabricantes tardan en hacer la declaración de conformidad, si la hacen. Por último, aunque con frecuencia los equipos de los centros de computación se reciclan cada tres o cinco años, los antiguos equipos se conservan para el proceso de control tanto tiempo como sea posible, incluso mucho después de la duración de vida oficial de su sistema de explotación[107].

---

107 La reciente interrupción progresiva de la utilización del sistema de explotación Microsoft Windows XP plantea pues otro problema para los proveedores de servicios.

Los diferentes métodos utilizados para el control de acceso es otro ejemplo. Los servicios de centros informáticos dan generalmente prioridad a la confidencialidad, la integridad y la disponibilidad. El control de acceso es por tanto de importancia primordial y las técnicas de autenticación y autorización están bien integradas y centralizadas gracias a una firma única con o sin implantaciones multifactores, la gestión de certificados X.509 y directorios LDAP/AD de gestión centralizada. Los sistemas de control dan prioridad a la disponibilidad por encima de la confidencialidad y la integridad. Por tanto, el acceso del hombre al proceso debe estar siempre asegurado.

Para facilitar la transferencia de las operaciones, los operadores comparten las contraseñas. Por otra parte, debido a que a menudo están patentados o son antiguos, los equipos y softwares tienen puertas traseras no señaladas, funcionan con contraseñas por defecto que no se han modificado, impidiendo bloquear conexiones no autorizadas mediante cortafuegos internos o listas de control de acceso, y son difíciles de integrar en las soluciones de gestión de identidad centralizada. Se considera que la encripción consume numerosos recursos. Generalmente, los sistemas de control exigen o utilizan dispositivos de protección suplementarios que procuren su seguridad y controlen el acceso. Una buena protección de la red adquiere aún más importancia, aunque es imposible de asegurar, puesto que un modelo eficaz de "defensa a fondo" supone medios de protección para cada capa del equipo del sistema de explotación y de las aplicaciones de la red.

Por otra parte, la robustez tiene una importancia esencial. Como ya se ha indicado, los atacantes tratan permanentemente de descubrir fallas en los sistemas de las tecnologías de la información estándar instalados en los centros informáticos, en particular cuando son directamente accesibles desde Internet. Es posible responder a esos intentos de intrusión o explotación de puntos vulnerables mediante una gestión correcta de los centros, manteniéndolos al día de todos los aspectos de ese fenómeno, sumada a la creación de sistemas adaptados de detección de intrusiones y su control. Gracias a la experiencia y los conocimientos acumulados durante varios decenios con respecto a diferentes tipos de ataques y las fallas posibles, así como a medios aceptados de intercambio de informaciones entre los interesados, resulta más fácil protegerse contra los incidentes, detectarlos y afrontarlos. En cambio, no se puede considerar que los sistemas de control sean ciberrobustos. Aunque los equipos físicos en los que están instalados podrían serlo, se ha observado muchas veces que su implantación en los softwares no respetaba las normas comunes en materia de tecnologías de la información, no pasaba las pruebas de seguridad básica ni disponía

de medios esenciales para rechazar los ataques[108]. Los sistemas de control responden a casos de utilización bien definidos, pero no lo hacen cuando esos casos están menos bien definidos. Contrariamente a lo que ocurre con los equipos de las tecnologías de la información estándar, la "seguridad" no forma parte de los dispositivos utilizados por los sistemas de control. Aunque lo fuera, puesto que la implantación de la seguridad es propia de cada empresa y opaca, los proveedores de servicios tienen dificultades para determinar si la seguridad es verdaderamente apropiada o apenas una ilusión.

Por último, aunque no menos importante, la comunidad encargada de los sistemas de control se esfuerza actualmente por hallar un consenso sobre la manera de llevar a cabo una "revelación responsable", es decir, de qué manera anunciar y presentar, al distribuidor correspondiente y, seguidamente a los proveedores de servicios, puntos vulnerables que se acaban de descubrir. En el mundo de las tecnologías de la información estándar se acepta que transcurra un plazo de tres a nueve meses entre el momento en que el proveedor de software recibe la información y el momento en que todas las informaciones se comunican al público, pero algunos estiman que ese plazo es muy corto dado que la fase de control en el ciclo de desarrollo de un software es mucho más prolongada y la aplicación de correctivos por un proveedor de servicios debe estar bien coordinada y programada. En realidad, el proceso completo lleva normalmente un año.

Ese problema debe resolverse para que los sistemas de control sean resilientes en el ciberespacio. Estos sistemas deben procurar que la seguridad forme parte del conjunto de funciones, de la disponibilidad, de las posibilidades de utilización, del mantenimiento y de la protección. Los expertos en sistemas de control deben recibir una formación adaptada en tecnologías de la información y, ante todo, en la seguridad de esas tecnologías. La formación debe comenzar en establecimientos de educación secundaria y universidades, y la seguridad debe ser incorporada en los programas educativos y no considerarse una opción. Mejor aún, convendría que todos los aspectos que guardan relación con las tecnologías de la información fueran confiados a especialistas competentes de esas tecnologías, capaces de distinguir entre las diferentes necesidades vinculadas a la explotación de los sistemas de control y los centros informáticos. Habrá tal vez que hallar nuevos compromisos para conciliar la necesidad de asegurar una disponibilidad permanente, la aplicación rápida de correctivos, un acceso fácil y un control de acceso riguroso. Paralelamente, las técnicas de virtualización de las tecnologías de la información podrían ofrecer la solución ideal

---

108 "CERN tests reveal security flaws within industrial networked devices", *The Industrial Ethernet Book*, 2006.

para resolver ese tipo de problemas y servir de nuevas bases para la aplicación de correctivos entre las fases de puesta a prueba, producción previa y explotación de sistemas. La gestión completa de softwares, los sistemas de gestión de versiones, los ciclos de desarrollo de softwares que comprenden también su actualización, pruebas de regresión completas y las compilaciones automáticas nocturnas deben convertirse también en norma para los sistemas de control. La integración en inventarios sumamente completos y puestos al día constantemente es igualmente indispensable. Es obligatorio disponer de una documentación muy completa sobre la base de la instalación, todos los dispositivos, las cuentas y las aplicaciones, así como sobre sus interdependencias, para comprender los riesgos e implantar medidas de protección. Las pruebas de intrusión deben ser efectuadas por defecto. Lo ideal sería recurrir automáticamente a fórmulas y procedimientos acordados y plenamente abiertos para evaluar los puntos vulnerables, de modo que los distribuidores y fabricantes, los proveedores de servicios y los encargados de la integración, pero también los gobiernos, las instituciones académicas y las autoridades de certificación, puedan evaluar de manera independiente la seguridad de un determinado dispositivo, equipo o software de control. Esos procedimientos deberán obligatoriamente aumentar la robustez de los sistemas de control actuales para, en última instancia, mejorar su resiliencia en caso de actividades malintencionadas y, es de esperar, despejar el camino a un mecanismo de certificación ISO9001.

Ninguna de estas etapas es trivial o fácil de realizar. Para la generación actual de sistemas de control y de expertos en esos sistemas, podría incluso ser demasiado tarde. En consecuencia, debemos mirar al futuro y fijarnos como objetivo vincular aún más las tecnologías de la información utilizadas por los sistemas de control y los centros informáticos. El grado de éxito que logremos será decisivo para determinar nuestro futuro.

2.4 La ciberresiliencia desde la perspectiva del sector privado

por Danil Kerimi

Vivimos en un mundo sumamente complejo e hiperconectado. Nos ofrece posibilidades sin precedentes, pero nos confronta a riesgos que eran inimaginables unos pocos años atrás. Empezamos recién ahora a comprender los cambios sociales, políticos y económicos que entraña ajustando las normas, las políticas y los modelos comerciales a la metafísica de la red.

Todos esos cambios redefinen profundamente la manera en que las personas, las empresas y los gobiernos se conectan entre sí. Los métodos tradicionales de creación de la riqueza económica y de consumo son puestos en tela de juicio por nuevos modelos comerciales e interacciones sociales producto de la hiperconectividad. Ya hoy, las empresas del sector dependen cada vez más de medios digitales para su funcionamiento interno, así como para las interacciones con sus asociados. Entidades que no han sido jamás consideradas grandes actores tecnológicos están en la actualidad confrontadas a cuestiones que no corresponden a su ámbito de competencia o de confort.

El comportamiento de los consumidores también ha cambiado: más autonomía, flujos de información más eficaces y mayor número de opciones. Las empresas conocen mejor el comportamiento de los consumidores, lo que permite un grado de personalización sin precedente. Tienen por otra parte que adaptarse a un entorno que cambia rápidamente, para lograr dar respuesta a las nuevas expectativas de los consumidores, como la creación conjunta de productos y la elaboración rápida de prototipos.

La hiperconectividad es un catalizador que a menudo logra reducir los obstáculos a la entrada en los mercados, desarrollar los intercambios comerciales y reforzar la competencia en cada uno de los sectores y también entre ellos, redefiniendo constantemente el entorno en que evolucionan las empresas y cuestionando la rigidez de las políticas. La automatización ininterrumpida de diferentes tareas y procesos, que forman parte de una evolución más amplia hacia economías del conocimiento, ejercen una presión considerable en los mercados de trabajo tradicionales.

El ritmo de la innovación no sólo ha causado la destrucción de empleos manuales sino también un declive estructural a largo plazo de empleos más fundados en el conocimiento. Por otra parte, nuestro sistema educativo actual no permite responder a la demanda de personal dotado de nuevas competencias (por ejemplo, especialistas de datos) que sustituya al que ocupa empleos más tradicionales.

Las tecnologías de la información y la comunicación son el motor de esas transformaciones. La hiperconectividad es el producto de empresas tecnológicas del mundo entero y pone a prueba la propia definición de empresa tecnológica. Al escuchar a los dirigentes de la industria automotriz hablar de los automóviles de hoy se tiene la impresión de que esos automóviles son terminales sobre ruedas. Las empresas de atención de la salud hablan de datos y los bancos, de ciberseguridad. Del sector bancario a los consumidores y a las empresas del sector de la energía, el mundo entero apuesta al universo digital.

Mientras que en el pasado las empresas tecnológicas afectaban los diferentes modelos comerciales y transformaban otros sectores, hemos llegado hoy a una situación en que otros sectores afectan modelos comerciales digitales más elaborados.

Esta evolución se plasma en nuestro espíritu de consumidor. Según el Informe más reciente de Interbrand[109], ocho de las diez grandes marcas son empresas TIC. La mitad de las marcas situadas entre el 10º y 20º lugar de esa clasificación son empresas conocidas que han contribuido a definir el panorama tecnológico actual. El valor total de esas marcas tecnológicas que figuran en los primeros 20 lugares supera 1 billón USD. Si correspondiera a un país, éste tendría su lugar en el G20.

En 2014, tres empresas que cotizan en bolsa entre las más importantes en cuanto a la capitalización bursátil son asimismo grandes empresas TIC. Según la última lista publicada en la revista Fortune, seis de las veinte personas de mayor influencia en el mundo proceden del sector de la tecnología; once son dirigentes políticos o religiosos y las tres restantes, directores del sector de las finanzas, el comercio y la energía[110]. Resultará interesante ver cuál será la clasificación para 2015.

Nuestra dependencia total en el ciberespacio para nuestras actividades cotidianas se ha afianzado. Por eso nos inquietan los riesgos a que está expuesto y tememos que pueda llegar a ser inaccesible. La ciberresiliencia, un concepto que nos resultaba extraño hace pocos años, es hoy un tema habitual en las reuniones de los consejos de administración, en los debates políticos y en las conversaciones en los cafés y hogares del mundo entero. El mundo está aprendiendo que todo objeto conectado puede ser pirateado y que el problema no es que esos objetos estén protegidos permanentemente, sino que sean flexibles y resilientes para funcionar en circunstancias desfavorables.

La velocidad, la movilidad y la colaboración son características fundamentales para una empresa próspera en la era digital. Para seguir aprovechando las ventajas que ofrece la hiperconectividad, se necesita con urgencia crear un ecosistema internacional ciberresiliente. En los dos últimos años, el Foro Económico Mundial ha reunido a un grupo de altos directivos y responsables políticos con objeto de estudiar la manera de lograr que el entorno digital sea más resiliente. El denominador común de los diferentes representantes de gobiernos y del sector privado era la inquietud por el aumento espectacular del número de ciberincidentes en el mundo. Para utilizar un

---

109 http://www.interbrand.com/en/best-global-brands/2013/Best-Global-Brands-2013.aspx

110 http://www.forbes.com/powerful-people/list/

concepto que pertenece al derecho del medio ambiente, se admite que los interesados tienen responsabilidades comunes aunque diferenciadas con respecto al ciberespacio, pero la ciberresiliencia exige un nivel elevado de colaboración multipartita. Como ocurre en otras esferas de la gobernanza mundial, los países en desarrollo, que por lo general no conocen muy bien las ciberamenazas ni tienen los medios adecuados para afrontarlas, están tan preocupados por los nuevos riesgos como los países desarrollados. A medida que aumenta la dependencia de nuestras economías en la conectividad digital, la ciberresiliencia deviene poco a poco una capacidad esencial para todos los dirigentes del sector privado y del ámbito político.

Para responder a esas inquietudes, el Foro Económico Mundial se concentró en la cuestión de la ciberresiliencia y pidió a los dirigentes empresariales (y no a los encargados de la seguridad de la información, de las tecnologías, etc.) y a los altos funcionarios gubernamentales que reconocieran la interdependencia de todas las partes que deben cumplir una función en la promoción de un espacio digital común resiliente. Al hacerlo, quisimos poner de relieve el papel de los dirigentes alentando la toma de conciencia de los altos responsables y una gestión integrada de los riesgos. Alentamos además la adopción de un enfoque sistémico global de la ciberresiliencia dado que las actividades de una empresa no se limitan a su entorno institucional sino que se inscriben en la cadena de valores completa, de los proveedores a los clientes.

La opinión pública y también un gran número de personas atribuyen gran importancia a la ciberresiliencia. Es probable que en los próximos años los gastos anuales en ese concepto aumenten, para pasar de 69 000 millones USD en 2013 a 123 000 millones USD en 2020[111]. Esas estimaciones dependen naturalmente de los análisis de mercado, que tendrán a su vez en cuenta ciberamenazas existentes y previstas. Por ejemplo, según una hipótesis, se prevé un aumento del 13% de las inversiones en materia de ciberresiliencia, que alcanzarían 139 000 millones USD por año, con una mayor colaboración entre el sector público y el sector privado teniendo en cuenta sus medios de defensa. Según otra hipótesis, se podría esperar un aumento del 28% en los gastos, que alcanzarían entonces 157 000 millones USD por año, si las capacidades de ataque superan las capacidades de defensa y si las respuestas son aisladas y no el fruto de la cooperación.

Con frecuencia, los debates sobre los ciberriesgos hacen referencia a situaciones de catástrofe o a una "ciberapocalipsis" temida y dan lugar a numerosas afirmaciones, como "ya no hay vida privada" o "el eslabón más débil". No obstante, quizás habría

111 http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

que preocuparse también de las ocasiones perdidas en caso de rechazo general o de fragmentación del ecosistema digital actual. Una sola gran "ciberapocalipsis" o una degradación progresiva ("muerte a fuego lento") podrían ocasionar un rechazo.

La fragmentación podría tener lugar a nivel de las regiones, los países o las empresas y son numerosos los motivos que podrían llevar a un gran número de actores a optar por ella. Este fenómeno ocurriría si se pidiera a los gobiernos preocupados de la falta de fiabilidad del entorno que aseguraran la seguridad en el ciberespacio. También podría guardar relación con las políticas industriales o en materia de reglamentación de diferentes países.

Mckinsey estima que las pérdidas para el posible crecimiento económico mundial podrían representar unos 3 billones USD si la incesante sofisticación de las capacidades de ataque desembocara en una disminución de las inversiones[112]. Un panorama político complejo podría complicar aún más la toma de decisiones económicas.

Podemos preguntarnos entonces a qué se parece la ciberresiliencia desde la perspectiva de una empresa. Para empezar, supone aceptar un criterio interdependiente y fundado en los riesgos que admite que la atenuación parcial de los riesgos es una característica esencial de todo sistema complejo y que la resiliencia de una organización contribuye a la resiliencia del sistema en general.

Las empresas, como otras organizaciones, atribuyen gran importancia a las prioridades establecidas por sus dirigentes. Por ese motivo, para elaborar un programa eficaz de gestión de los riesgos y supervisar su aplicación, es importante hacer participar a los equipos de dirección y poner en práctica estructuras de supervisión, por ejemplo comités.

Sería conveniente que el equipo de dirección definiera una serie de responsabilidades diferenciadas y objetivos comunes y previera los recursos, la gobernanza y los fondos necesarios para alcanzarlos, sin olvidar de dar a conocer las medidas adoptadas al respecto. Con respecto a la continuidad de las actividades, las pruebas de resistencia de los sistemas y la simulación de situaciones de crisis del tipo "juego de guerra", que exigen una coordinación entre los diferentes departamentos, de tecnologías de la información a asuntos públicos, podrían ser sumamente útiles si la empresa se viera confrontada a una situación real en que los actores no habrían tenido tiempo de

---

112 Ibid.

examinar en detalle las responsabilidades de cada uno y las posibilidades de respuesta.

También se podría considerar la ciberresiliencia un componente básico e integrarla en la gestión en sentido amplio de la continuidad de las actividades y de los riesgos para la empresa. Podría ser razonable comenzar por identificar los activos de información que son decisivos para la misión de la organización. La defensa del perímetro era quizá una buena estrategia en el pasado, pero dado el nivel actual de los ataques, los intentos de intrusión, las amenazas internas y el panorama moderno en materia de riesgos, hay que establecer un orden de prioridad claro entre los activos para asignar los recursos suficientes para protegerlos.

Para hacerlo, todos los aspectos de las actividades, así como el riesgo en el plano de la reputación tendrían que estar sujetos a evaluaciones regulares de sus efectos. Además, habría que poner en marcha procesos que permitan reducir el tiempo necesario de restablecimiento completo o parcial en caso de fallo grave. Es fundamental que el conjunto de la empresa colabore y que no se considere que esa cuestión corresponde únicamente al departamento de tecnologías de la información.

Todos los departamentos, comprendidos los que se encargan del marketing, de cuestiones gubernamentales y públicas, así como de las relaciones con los consumidores, dirigidos por un equipo de gestión de alto nivel, deberán estar preparados para actuar simultáneamente en el restablecimiento de las actividades afectadas, atenuado las posibles repercusiones negativas para la marca y una eventual reacción de rechazo de los clientes, y también las posibles consecuencias reglamentarias.

Numerosas grandes empresas tienen un director encargado de la seguridad de la información. Otras han separado claramente esa función de las atribuciones del director técnico/director informático. Asimismo, ciertas empresas han procurado que, aunque no sean del mismo nivel, los cargos estén asociados a entidades jerárquicas diferenciadas, puesto que los objetivos estratégicos de las diferentes funciones pueden necesitar prioridades diferentes con respecto, ante todo, a la arquitectura técnica y la adquisición.

Únicamente gracias a una apreciación exhaustiva de los diferentes activos de información y de la importancia de una respuesta adecuada e inmediata en caso de ataque a su seguridad, una empresa puede contribuir verdaderamente a su propia ciberresiliencia sistémica. Las empresas que ponen en práctica estructuras de ciberresiliencia/gestión de riesgos deben tener en cuenta la conformidad, un elemento importante en la medida en que los gobiernos comienzan a hacer frente a una inseguridad en aumento instaurando diferentes mecanismos reglamentarios, por

ejemplo, códigos de conducta y buenas prácticas de aplicación voluntaria, indicación obligatoria de los incidentes y elaboración de normas.

El papel que cumplen los proveedores, los contratistas y los clientes en la cibercadena completa de suministros es otro elemento igualmente importante. Una empresa debería hacer todo lo posible para mejorar su rendimiento en el ecosistema en sentido amplio, ampliando de esa forma el perímetro de seguridad y asegurando que se crea una coalición.

La defensa anticipatoria es una de las esferas más delicadas para las actividades internacionales de los últimos años. Dado que se ha vuelto muy difícil definir el perímetro de seguridad, la empresa aprovechará las fuentes de datos internas y externas existentes para seguir de cerca la evolución de las amenazas que podrían concluir en un ataque. Con todo, resulta muy difícil comprender en qué momento el nivel de las amenazas internas y el de las amenazas externas confluyen, sin mencionar la posibilidad de aplicar medidas preventivas y la cuestión de su legitimidad incluso cuando el peligro es claro e inminente.

Las dificultades con respecto a la atribución son citadas a menudo como uno de los más grandes obstáculos, del mismo modo que la legalidad y la legitimidad de una posible acción. Esa «zona gris» se vuelve más transparente cuando existe una ciberestrategia completa a nivel del país y de la empresa, que no siempre está fácilmente a disposición. Esa estrategia debería comprender elementos nacionales y también internacionales claros y transparentes.

La manera de aceptar ese problema ha cambiado radicalmente y los dirigentes de empresa comprenden mejor ahora todos los matices de los elementos y las técnicas de atenuación posibles. Se ha abierto el diálogo entre numerosos interesados a escala nacional e internacional, puesto que las amenazas siguen evolucionando rápidamente.

La hiperconectividad ya ha modificado nuestra manera de conectarnos unos a otros: incide en las decisiones que tomamos y en cómo organizamos nuestras vidas. El efecto perturbador de las tecnologías de la información supone transformaciones sociales y económicas cada vez más frecuentes. Tenemos tendencia a sobrestimar las repercusiones de las tecnologías a corto plazo y a subestimar sus repercusiones a largo plazo en todos los aspectos de nuestras vidas. La reflexión sobre la ciberresiliencia puede ser el punto de partida para comprender y elaborar soluciones que nos ayuden a tomar decisiones con miras a obtener los resultados positivos que todos deseamos.

2.5 Asegurar la ciberseguridad en su totalidad para reforzar la ciberresiliencia

por Solange Ghernaouti

Las diferentes dimensiones de la ciberresiliencia

Los ciberriesgos son una realidad para cada uno de nosotros. Cualquiera que esté al tanto de la actualidad se habrá convencido. El ciberdelito es una plaga mundial y los ciberataques forman parte ahora de las doctrinas militares. En ocasión de su Cumbre, celebrada en septiembre de 2014[113], la OTAN definió los ciberataques masivos como actos de guerra que podrían provocar una respuesta militar y, si un miembro de esa organización fuera la víctima, se considerarían un ataque a la OTAN en su conjunto. Hay que admitir que los conflictos también tienen lugar en el ciberespacio, por lo general a través de ciberataques dirigidos a las infraestructuras de la información civiles y militares, así como de la manipulación de la información. Por Internet, la promoción de la guerra y el terrorismo coexiste con la promoción de actividades legítimas e ilegales, en tanto que el mercado negro del ciberdelito prospera. Por otra parte, Internet es en la actualidad el medio de comunicación más utilizado para las actividades delictivas y la propaganda. Los ataques a sistemas de información pueden interrumpir el funcionamiento de las infraestructuras vitales de un país, permitir que se pongan en práctica estrategias criminales, causar pérdidas de productividad y de competitividad o contribuir a la toma de poder en un país. Asimismo, con Internet es más fácil llevar a cabo actividades destinadas a desacelerar o impedir el desarrollo económico de un país, a menoscabar el buen funcionamiento del Estado o a desestabilizarlo. Un gran número de sistemas de información son el blanco de ciberactividades cuya finalidad es desestabilizar un país o dañar su economía, sus instituciones o su reputación. Esas actividades se realizan en un contexto más amplio de hipercompetitividad económica mundial.

Las ciberamenazas y sus numerosas facetas evolucionan constantemente y es importante interpretarlas de manera interdisciplinaria y global para combatirlas sin cesar, reforzar la seguridad y la resiliencia de las infraestructuras civiles y militares, así como para proteger a cada agente económico, comprendidas las pequeñas y medianas empresas y los particulares. El proceso ininterrumpido de asegurar la ciberseguridad

---

113 http://www.nato.int/cps/en/natohq/news_112107.htm?selectedLocale=en (Guía de la Cumbre de la OTAN en el País de Gales – Newport, 4-5 de septiembre de 2014).

de personas y bienes, garantizando al mismo tiempo la seguridad pública, debe formar parte de un proyecto político que respalde una estrategia de desarrollo sostenible para la sociedad, que tenga ella misma en cuenta la cultura y las particularidades del país. Ello exige la participación de todos los actores, privados y públicos, a escala nacional e internacional[114].

Hemos creado un mundo de conectividad permanente gracias a las comunicaciones móviles, inalámbricas y sin contacto[115], un mundo donde los objetos devienen inteligentes y capaces de comunicar: es lo que llamamos la Internet de las Cosas y de casi todo lo que contribuye a crear hogares y ciudades inteligentes. Objetos tan habituales como coches y semáforos tendrán componentes informáticos y de tecnologías Internet. Podrán lograr así una cierta autonomía y tomar decisiones, gracias a la inteligencia integrada en su sistema de programación. Esos objetos ya han comenzado a invadir los lugares públicos y son automáticamente las posibles víctimas de ciberactividades malintencionadas, puesto que cada entidad conectada a Internet puede ser pirateada e integrada en una red robot que atacará otros sistemas. Las fallas de seguridad de esos objetos podrían tener graves consecuencias en nuestra seguridad física. Para facilitar la vida de las personas y sus actividades de cada día, robots más o menos sofisticados comienzan a compartir nuestra vida cotidiana. Dado que los robots son capaces de influir en nuestro comportamiento y nuestro entorno, su control por entidades malintencionadas o indeseables podría tener graves consecuencias en nuestra sociedad. El siglo XXI es el de los circuitos integrados RFID y de las nanotecnologías, la idea del polvo inteligente. La convergencia de los universos de la electrónica y la biología es cada vez más real, en particular con respecto al cuerpo humano y los diversos sensores, prótesis y otros elementos de electrónica biomédica que pueden implantarse en el cuerpo humano para corregir ciertas anomalías (por ejemplo, bombas de insulina o marcapasos). Ya se han creado interfaces neuronales que permiten interactuar con computadoras mediante el pensamiento. Naturalmente, todo esto puede contribuir al bienestar a medida que la utilización de esas tecnologías y la convergencia de la electrónica y la biología avanzan y alcanzan mayor complejidad, pero su utilización para fines distintos a los que guiaron su creación podría conducir a casos de piratería, incluso del pensamiento humano. Esos nuevos riesgos nos obligan a reinventar la seguridad para gestionarlos mejor y proteger nuestros valores amenazados por las repercusiones incesantes de las tecnologías en la sociedad.

---

114 "Cyberpower: crime, conflict and security in cyberspace"; S. Ghernaouti, EPFL Press 2013.

115 Las tecnologías sin contacto aluden a las tecnologías de comunicación de campo cercano.

El ciberespacio ha pasado a ser un elemento de civilización del que dependemos considerablemente. Por eso es importante que sus infraestructuras sean sólidas y resilientes ante todo tipo de incidentes. El concepto de ciberresiliencia abarca varias dimensiones que pueden necesitar la adopción de medidas operacionales como, por ejemplo, la lucha contra el ciberdelito, las actividades complementarias vinculadas a la ciberseguridad y la ciberdefensa, la gestión eficaz de los riesgos en materia de energía y medio ambiente, así como la educación y el mantenimiento de las competencias humanas necesarias para la sociedad de la información del futuro.

Luchar contra el ciberdelito

Es urgente que la comunidad internacional esté mejor preparada para luchar contra el ciberdelito. Ningún Estado, ninguna organización ni ningún usuario de Internet está protegido contra las cibermolestias, sean criminales o simplemente irritantes.

Estar mejor preparado para luchar contra el ciberdelito supone estar ya preparado, aunque sea a un nivel bajo e inadecuado. Para las instituciones, eso podría significar:

- Disponer de los medios (estrategias, medidas, recursos, capacidades) necesarios para resolver el problema, pero a niveles cuantitativos y cualitativos insuficientes.
- Disponer de medios de protección, pero que no son suficientemente eficaces o convenientes.

Si bien son dos situaciones corrientes, no hay que olvidar que para numerosos actores, como las pequeñas y medianas empresas y los particulares, y para un gran número de infraestructuras y objetos conectados a Internet, no existe ninguna estructura de control ni ninguna medida de seguridad.

En el caso de un Estado, luchar contra el ciberdelito entraña varios factores:

- Disponer de un marco jurídico aplicable a escala nacional compatible con las estructuras internacionales.
- Disponer de estructuras judiciales y de fuerzas de policía con recursos y competencias que les permitan funcionar a escala nacional y cooperar con una red internacional para luchar contra el ciberdelito transnacional.

En el plano internacional, eso supone que la comunidad internacional se une para defender una causa común, la lucha contra el ciberdelito, y que no hay "paraísos digitales" donde las personas deshonestas pueden actuar con total impunidad.

La existencia de esos paraísos beneficiaría a los delincuentes puesto que:

- verían en Internet un medio de cometer delitos económicos y un instrumento para perpetrar actos criminales (tráfico de personas, tráfico de drogas, blanqueo de dinero …);
- considerarían el ciberespacio como una instancia protectora y un terreno de juego mundial.

La lucha contra el delito ha sido siempre un asunto complejo. El ciberdelito ha acentuado esa complejidad y hecho aún más difícil esa lucha, tanto a escala nacional como internacional.

Al mismo tiempo, las proezas de los ciberdelincuentes son descritas con regularidad en los medios, pero no parece que entrañen la adopción de medidas suficientemente eficaces para limitar la progresión de esos ataques o para reducir el número de víctimas. De hecho, hay muy pocos arrestos o procesos penales en relación con la proliferación de actividades malintencionadas, lo que despierta un cierto sentimiento de injusticia en las víctimas.

Pese a ello, la acción que llevan a cabo los Estados para luchar contra el ciberdelito ha logrado dos avances importantes:

- en primer lugar, a nivel europeo con la creación en 2013 del Centro Europeo de Lucha contra el Ciberdelito de Europol (EC3) situado en La Haya[116];
- en segundo lugar, a nivel internacional con la inauguración en 2014 del Complejo Mundial para la Innovación, instalado en Singapur[117].

Para luchar eficazmente contra el ciberdelito se debe adoptar un criterio de prevención que vuelva el ciberespacio, como medio de cometer delitos, menos atractivo y reduzca las posibilidades de realizar actividades delictivas. En consecuencia, es necesario poner trabas al lanzamiento de ciberataques, lo cual incrementará los costos en concepto de competencias y recursos, reduciéndose así las ventajas previstas y aumentando los riesgos de identificación, localización y procesos penales para los delincuentes. De manera general, la resiliencia puede asegurase gracias a las siguientes medidas:

---

116 https://www.europol.europa.eu/ec3

117 http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation

- Reducir el número de vulnerabilidades técnicas, orgánicas, jurídicas y humanas.
- Reforzar la solidez y resiliencia de las infraestructuras de la información aplicando medidas en materia de tecnología, procedimiento y gestión que sean coherentes y complementarias.
- Crear una verdadera capacidad que permita adaptar los medios de ciberseguridad y ciberdefensa a una situación en constante evolución.
- Dotarse de medios de gestión de las cibercrisis.
- Luchar contra los circuitos de monetización del ciberdelito.

El nuevo universo del ciberespacio está inundado de todo tipo de actividades. Es un instrumento al servicio de la rentabilidad económica y un lugar de ejercicio del poder: se trata, en realidad, de un territorio estratégico. Por ese motivo, debe ser protegido y defendido, tanto desde el punto de vista económico como de la seguridad nacional.

Garantizar la defensa de la seguridad en su totalidad para asegurar un cierto nivel de estabilidad

La vigilancia de los ciberriesgos se inscribe en un contexto de competencia económica feroz y constante (casi de guerra económica), búsqueda de rendimiento inmediato, crisis monetaria internacional, inestabilidad generalizada, injusticia social, riesgos ecológicos y una cierta deficiencia en materia de gobernanza mundial. No habría que considerar la ciberseguridad únicamente en un contexto de reacción lógica que apunta a "sobrevivir" a un ciberincidente, haya sido premeditado o accidental. Si bien es fundamental y absolutamente necesaria, esta capacidad de resistencia no puede reemplazar la ausencia de un enfoque global con la participación de numerosos actores a nivel nacional e internacional o una verdadera comprensión del fenómeno del ciberdelito o el ciberconflicto en su conjunto. Un enfoque global, interdisciplinario e integrado de la ciberseguridad y la ciberdefensa favorecerá la adopción de medidas adecuadas en materia de prevención y de acción inmediata, cuya eficacidad dependerá de su exhaustividad y coherencia desde un punto de vista civil y militar. Sería utópico pensar que podemos resolver los problemas vinculados al ciberespacio sin varios niveles de cooperación entre numerosos actores, tanto al interior como al exterior de las fronteras nacionales, con el objetivo de respaldar estrategias a favor de la paz en el ciberespacio y en el mundo real.

En ciertos casos, será quizá necesario replantear la cooperación y el diálogo entre fuerzas civiles y militares con objeto de procurar un modelo coherente de protección de la seguridad para la sociedad en sentido amplio. La ciberseguridad sólo puede entenderse de manera interdisciplinaria y global. A escala nacional, eso significa una visión común y transversal del problema, una cooperación interministerial reforzada y la capacidad de trabajar juntos.

Cualquiera sea la finalidad principal de un ciberataque, cualquiera sea su víctima (una persona, una organización, un Estado), los instrumentos utilizados son los mismos. La naturaleza y la magnitud de las consecuencias varían en función de las víctimas y las motivaciones de los atacantes, pero los métodos e instrumentos a que recurren no cambian. Para un país, el mantenimiento de la seguridad pública, la seguridad económica y la seguridad nacional se sitúa en cierta forma entre la seguridad civil y la seguridad militar. Por eso es importante que las estrategias nacionales de ciberseguridad y de ciberdefensa lo tengan en cuenta para optimizar la eficacia y eficiencia de las medidas adoptadas con la intención de responder de la mejor forma posible a las necesidades de la población, en tiempos de paz y en tiempos de guerra. Al mismo tiempo, la protección de infraestructuras esenciales no puede quedar en manos del sector privado ni del sector público únicamente, lo que justifica igualmente la necesidad de prever un conjunto de medidas para proteger la seguridad.

Es importante proteger y defender a la vez los activos digitales y el patrimonio digital de las personas, las organizaciones y los Estados, así como las infraestructuras que dan soporte a esos activos y funciones esenciales. Esto exige adoptar medidas de protección complementarias, en especial actividades de protección, en el sentido civil y militar del término, encaminadas a salvaguardar las infraestructuras y activos que son vulnerables a las ciberamenazas.

La creación de una cultura de la ciberseguridad y la ciberdefensa, al tiempo que promueve el diálogo internacional sobre esas cuestiones, debería contribuir, en el mundo complejo e incierto en el que vivimos, a lograr un cierto grado de confianza y estabilidad, a condición de que cada interesado se comporte con honestidad y sentido de la responsabilidad colectiva, teniendo en cuenta que es necesario gestionar los riesgos en las esferas de la energía y el medio ambiente.

Entre los riesgos indirectos creados por sociedades digitales y la utilización intensiva de sistemas de información que tienen grandes repercusiones en nuestro planeta, no deberíamos olvidar, al encarar la ciberresiliencia a largo plazo, la elaboración de medidas que garantizarán nuestra durabilidad en términos de disponibilidad de energía y preservación de recursos naturales y del medio ambiente ecológico para las futuras generaciones.

Por lo tanto, tendríamos que privilegiar en particular los riesgos relativos:

- a la eliminación y el reciclado de desechos electrónicos;
- al consumo de energía (necesidades de electricidad crecientes y constantes);
- al calentamiento del planeta (escape de calor y necesidad de enfriar las computadoras y las torres de servidores);
- a la explotación de tierras y metales raros necesarios para la construcción de equipos electrónicos;
- a las consecuencias ambientales de los ciberataques contra sistemas de control de sitios de purificación, la producción y distribución de productos tóxicos, las alarmas de incendio, etc.

Las actividades llevadas a cabo para asegurar la ciberresiliencia deberán además cumplir las exigencias de protección de la infraestructura esencial, en especial con respecto a elementos vitales vinculados a la energía y el medio ambiente.

Desde un punto de vista ecológico, nos incumbe a todos adoptar pautas de prevención para anticipar mejor las amenazas, gestionar los ciberriesgos, detectar anomalías para limitar sus consecuencias y asegurar la ciberresiliencia. Se debe asimismo garantizar la educación y el fomento de capacidades humanas.

Las personas formadas en cuestiones de ciberseguridad en diversas disciplinas de las ciencias sociales o técnicas determinan los principios teóricos y la posición adoptada en la materia, una indicación de que los ámbitos de formación correspondientes existen. Sin aptitudes ni facultades en la esfera de la ciberseguridad en todo el mundo, y sin transferencia de conocimientos ni cooperación para reforzar las capacidades humanas, será difícil adoptar comportamientos compatibles con la ciberconfianza. Es importante adoptar buenas prácticas en el campo de las tecnologías de la información y capacitarse para tener conciencia de los ciberriesgos, pero no es suficiente si el concepto de ciberseguridad no está integrado en los productos y servicios desde su primera fase de concepción, si la policía y el aparato judicial no están en condiciones de cumplir su función por incompetencia o si los actores políticos y económicos, del mismo modo que los usuarios de Internet, de los más jóvenes a los de más edad, no poseen los conocimientos, las competencias o la experiencia que necesitan. No basta con sensibilizar a la población respecto de los peligros inherentes a Internet y de las precauciones elementales que deberían adoptarse o determinar que es la única responsable de una situación que, en la mayoría de los casos, escapa a su control. En realidad, sería injusto pedir al usuario final y al ciudadano que se haga cargo del costo de los riesgos que quienes los han creado no han sido capaces de eliminar y, por tanto,

atribuir un problema de sociedad a personas que no tienen los conocimientos ni los medios necesarios para hallar una solución.

La ciberresiliencia, un nuevo dilema de la ciberseguridad

La resiliencia a los delitos forma parte de una visión general de la ciberseguridad y contribuye a instaurar la ciberconfianza. Es urgente aumentar la robustez y resiliencia de nuestras infraestructuras adoptando medidas adecuadas en el ámbito tecnológico, judicial, orgánico y de procedimiento. Como para todas las actividades vinculadas a la seguridad, la lucha contra el ciberdelito, el ciberabuso y la ciberutilización abusiva es una tarea complicada. Ese combate debe situarse en una perspectiva de protección de las personas y los activos tangibles e intangibles, y de defensa de valores democráticos comunes de amplia aceptación. Conviene por tanto adoptar un enfoque claro y eficaz en materia de ciberseguridad y ciberresiliencia.

Para evitar que la sociedad de la información sea sinónimo de desconfianza y vigilancia, se deben aportar respuestas convincentes a la necesidad de instaurar la confianza y la resiliencia en el ciberespacio y proponer soluciones prácticas para proteger los activos y las infraestructuras digitales. Todo intento de obstruir el ciberespacio exigirá poner en práctica una voluntad política en el plano nacional e internacional, recursos y conocimientos, estructuras y procedimientos orgánicos así como una coordinación adaptada. Se trate tanto de actores legítimos como dudosos, el nuevo factor de estabilidad de las sociedades forma parte de la seguridad de las mismas y depende de su capacidad para controlar los ciberriesgos y mantener las cibermolestias a niveles aceptables. La ciberseguridad no debería ser un instrumento de dominación ni de ejercicio de poder de los Estados, sino un instrumento de estabilidad y de fomento de la paz[118].

---

118 Asegurar la ciberconfianza a escala mundial contribuirá a resolver los principales problemas relativos a la paz en el ciberespacio, como los formulados en "La búsqueda de la paz en el ciberespacio" – UIT 2011 (http://www.itu.int/pub/S-GEN-WFS.01-1-2011)

Capítulo III: Ciberlibertad

Introducción

Mientras que en el capítulo anterior se destaca la importancia crucial de la ciberresiliencia para instaurar la confianza en el ciberespacio, en este último capítulo se presenta un panorama general de los retos de la ciberlibertad y de las nuevas amenazas provenientes tanto del sector público como del sector privado que entraña y que desalientan la esperanza de una Internet libre.

La libertad de opinión y de expresión, el libre acceso a la información y el derecho al respeto de la vida privada han sido siempre elementos esenciales de la sociedad civil puesto que constituyen derechos humanos y libertades civiles esenciales, que son los cimientos de principios y valores democráticos. La creación de Internet y las tecnologías de la información y la comunicación ha dado a miles de millones de personas en todo el mundo la posibilidad de acceder a cantidades de información y de medios de comunicación hasta ese momento inimaginables. Sin embargo, esas herramientas esenciales de la era digital, aunque representan enormes plataformas para el intercambio de opiniones, datos e ideas innovadoras, son al mismo tiempo explotadas para poner en peligro el progreso, los derechos políticos y el respeto de la vida privada, socavando la confianza en su utilización.

Como ha indicado en varias ocasiones el Tribunal Europeo de Derechos Humanos, "… el derecho a la libertad de expresión protegerá no sólo la «información» o las «ideas» que se reciben favorablemente o se consideran inofensivas o indiferentes, sino también aquéllas que ofenden, conmocionan o perturban al Estado o a cualquier sector de la población."[119]

Si bien los blogs y los medios sociales han abierto nuevas posibilidades para el intercambio de ideas, ciertos Estados han recurrido en los últimos años a bloquear Internet para aumentar la censura y de esa forma controlar la opinión pública y poner freno a la libertad de información y de expresión.

---

119 Tribunal Europeo de Derechos Humanos; asunto de *Handyside contra Reino Unido* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"dmdocnumber":["695376"],"itemid":["001-57499"]} última consulta el 17/10/2014.

Esa censura pone en tela de juicio las ventajas de Internet, es decir, su capacidad de propagación ilimitada y su accesibilidad en todo el mundo, y forma parte del debate actual sobre la neutralidad de la red, insistiéndose en que se debe garantizar la igualdad de derechos con respecto al acceso de ese medio esencial de nuestra época.

Las cantidades masivas de datos altamente disponibles son una característica de la sociedad de la información actual y acentúan las nuevas amenazas de espionaje provenientes a la vez del sector público y el sector privado, poniendo en peligro el respeto de la vida privada y la utilización segura de los instrumentos digitales. De hecho, la vigilancia justificada que ponen en marcha los gobiernos para garantizar la seguridad nacional puede conducir rápidamente a la recopilación de datos y al almacenamiento de informaciones personales de forma generalizada, lo que hace difícil hacer una distinción entre prácticas aceptables y prácticas inaceptables que dan la impresión de cruzar la línea roja.

Al mismo tiempo, para sacar partido del régimen de protección de datos más conveniente y procurarse ventajas financieras y en términos de competencia, el sector privado recoge y transfiere enormes cantidades de datos personales más allá de las fronteras, con lo cual se crean nuevos riesgos para los datos personales.

Dado que, por su naturaleza, Internet no tiene fronteras, las legislaciones nacionales no pueden garantizar la libertad de Internet. Por ese motivo, es imprescindible elaborar y adoptar un marco internacional para la instauración de la ciberconfianza.

El presente capítulo se divide en cinco secciones. En primer lugar, se hace hincapié en la ausencia de un marco jurídico adecuado con respecto a la protección de las libertades civiles en el ciberespacio y de la libertad de Internet, como se observa en la situación actual de numerosas regiones del mundo árabe. Seguidamente, se pone de relieve el debate sobre los *Big Data* y el problema de la protección de los datos, cuya finalidad es destacar la necesidad de contar con un marco reglamentario internacional para preservar la libertad de Internet y el derecho al respeto de la vida privada. En la tercera sección se examina el tema de la vigilancia estatal y la recogida de información en el ciberespacio, así como su incidencia en la instauración de la ciberconfianza.

En la cuarta sección se aborda, desde la perspectiva europea, el problema de la violación por parte de los gobiernos de la confidencialidad digital y de la protección de los datos, y también la importancia de la creación de una política armonizada al respecto en la Unión Europea, no sólo para facilitar la cooperación entre sus Estados Miembros sino también para que sirva de modelo fuera de sus fronteras. En la quinta y última sección se trata de establecer criterios para la gestión de la ciberlibertad en tanto que derecho humano fundamental y poderoso motor de la confianza en el ciberespacio.

3.1 Ciberlibertad: Progresos y retos

por Mona Al-Achkar

Introducción

El poder de las nuevas tecnologías ha marcado una era en la que se superan cada vez más problemas técnicos que limitan las posibles realizaciones a numerosos niveles, una era digital en que los individuos y los Estados naciones disponen de medios de acción sin precedentes no sólo para desarrollarse sino también para planificar actos de abuso y violencia de gran envergadura.

Esta paradoja se pone de manifiesto en la oposición entre las ventajas innegables de la era digital y los numerosos peligros que afrontan las personas, el mundo de los negocios y los Estados naciones debido a la utilización incesante de las TIC y al aumento de las actividades delictivas, cada vez más sofisticadas, en el ciberespacio. Las amenazas a la seguridad nacional se han agravado, y las infraestructuras esenciales están de más en más expuestas a numerosos riesgos, en especial a ataques a partir de Internet.

Con el ciberdelito, la incompatibilidad y la ausencia o insuficiencia de un marco jurídico siguen siendo los principales factores que socavan la confianza en la utilización de plataformas del ciberespacio, dado que permiten la instauración de una inseguridad jurídica e impiden el pleno ejercicio de las libertades civiles. En consecuencia, el control ejercido sobre Internet representa una verdadera amenaza para numerosas libertades civiles, como el respeto de la vida privada, la libertad de expresión, la protección contra la autoincriminación, los registros e incautaciones injustificadas y el derecho a la debida aplicación de la ley. El nivel de protección de esas libertades civiles depende en gran medida de la legislación, las prácticas jurídicas y el sistema político en vigor en un país o región determinados.

Para garantizar un ciberentorno económico digno de confianza es indispensable proteger esas libertades civiles e instaurar de esa manera la confianza en el ciberespacio. Así lo ilustra con claridad el caso PRISM, que ha revelado que la Agencia de Seguridad Nacional de los Estados Unidos (NSA) había recopilados datos personales y llevado a cabo operaciones de espionaje de forma clandestina. A raíz de esas revelaciones, Cisco anunció una disminución del 8 al 10 por ciento de sus ingresos, y previó una disminución suplementaria de sus actividades y de sus ingresos para 2013-2014, debido a la situación económica mundial y a las consecuencias del escándalo del caso PRISM.

Esta vigilancia masiva junto con nuevos conceptos como "ciberrepresión" y "Estado policial electrónico", tienden a señalar el empeoramiento de un gran número de las libertades civiles indicadas anteriormente, tanto en regímenes dictatoriales como en países democráticos.

Libertades civiles

El término "libertades civiles" viene del latín *ius civis*, que significa "derecho de los ciudadanos" y su fuente es la *Carta Magna* destinada a limitar el abuso de poder de las autoridades. Por ese motivo, las libertades civiles se consideran una protección contra las prácticas y las acciones ilegales de los gobiernos y contra la violación de los derechos jurídicos fundamentales que ellos ejercen.

En tanto que los derechos humanos son universales y se aplican en igual medida a todos los países, las libertades civiles guardan relación con la legislación nacional de cada país. Por consiguiente, cada país otorga a sus ciudadanos las libertades fundamentales concedidas en virtud de su sistema jurídico nacional. La particularidad más importante de las libertades civiles consiste en que limitan la intrusión del Estado en la vida de los ciudadanos, así como todas las formas de abuso de poder, y garantizan por tanto la capacidad de los ciudadanos para participar en la vida civil y política del país sin padecer discriminación ni represión.

Las libertades civiles comprenden derechos personales, políticos y económicos tales como el derecho a un proceso equitativo, el derecho a la debida aplicación de la ley, la libertad de asociación, el derecho de petición, el derecho de autodefensa, el derecho de voto, la protección contra la esclavitud y el trabajo forzado, la protección contra la tortura y la muerte, el derecho a la libertad y la seguridad, la libertado de conciencia, la libertad de religión, la libertad de expresión, la libertad de palabra, el derecho a la vida privada, el derecho de propiedad, el derecho al matrimonio, el derecho a defenderse, el derecho a la integridad física, el derecho a la utilización de equipos, el derecho a una educación igualitaria y el derecho de ejercer una función pública.

Las libertades civiles enunciadas en la legislación nacional pueden tener una base jurídica común, como el delito de agravio a las libertades civiles, que permite a los particulares pedir reparación – no sólo con respecto a otros particulares sino también al Estado – cuando han sido agraviados o sufrido daños corporales a raíz de una violación de sus derechos fundamentales. Esas infracciones pueden comprender, por ejemplo, la intrusión injustificada en el domicilio o la vida privada de una persona, la difamación o la apropiación ilícita.

Libertad de información: el derecho de acceso a la información

La libertad de información o derecho de acceso a la información ha surgido en calidad de nuevo derecho, distinto pero inseparable de la libertad de expresión. Puede definirse como derecho de acceso a la información en manos de los organismos públicos[120].

De acuerdo con el documento final establecido por una reunión de expertos organizada por la Secretaría del Commonwealth, en el que se tuvo en cuenta el Artículo 19, "La libertad de información debe ser garantizada en tanto que derecho legal y exigible que permite a todo individuo obtener documentos e informaciones en manos de los poderes ejecutivo, legislativo y judicial del Estado, así como de toda empresa pública o cualquier otro organismo que cumpla funciones públicas."

El principio fundamental que sustenta esta libertad reside en el derecho de los ciudadanos a saber, la obligación de los gobiernos a informar a sus ciudadanos y el hecho de que la carga de la prueba corresponde a la parte que recibe el pedido de información. Es por ello que numerosos gobiernos se inclinan a clasificar secreta la información que no desean divulgar o a no publicarla por razón de Estado.

El derecho de acceso a la información incluye el derecho de buscar, recibir y transmitir informaciones e ideas, y vale tanto para las personas que buscan activamente información como para las que esperan recibirla a través de medios de comunicación o canales oficiales. Este derecho concierne principalmente al acceso a la información pública. Hace hincapié en el principio de la publicación de los actos, así como en la transparencia de la administración pública, lo cual establece una relación directa entre su aplicación y la participación activa de los ciudadanos en la vida política y en los mecanismos de lucha contra la corrupción.

Con arreglo a la Resolución 59 (1) de la Asamblea General de las Naciones Unidas: "La libertad de información es un derecho humano fundamental y piedra de toque de todas las libertades a las cuales están consagradas las Naciones Unidas"[121]. Del mismo modo, como se enuncia en el preámbulo de los Principios de Lima o en la Declaración de Chapultepec: […] el derecho individual a la libertad de expresión y al acceso a la información son fundamentales para la existencia de todas las sociedades

---

120 http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-information/

121 Asamblea General de las Naciones Unidas, (1946) Resolución 59 (1), 65ª Sesión Plenaria. http://foishehri.wordpress.com/

democráticas y esenciales para el progreso, el bienestar y el goce de todos los demás derechos humanos".[122]

Asimismo, en el Compromiso de Túnez, la Cumbre Mundial sobre la Sociedad de la Información reafirmó la necesidad de que los Estados respeten los derechos humanos y las libertades fundamentales, y reconoció "[…] que la libertad de expresión y la libre circulación de la información, las ideas y los conocimientos son esenciales para la Sociedad de la Información y benéficos para el desarrollo".[123]

En consecuencia, el derecho de acceso a la información es considerado esencial, entre otras cosas, para el ejercicio de la libertad de expresión y la libertad de opinión. Supone la obligación para los gobiernos de garantizar la libre circulación de la información y las ideas. En 1995, Abid Hussain, entonces Relator Especial de las Naciones Unidas para la libertad de expresión y de opinión, afirmó en su informe a la Comisión de Derechos Humanos de las Naciones Unidas: "La libertad perderá toda su efectividad si la población no tiene acceso a la información. El acceso a la información es esencial para la vida democrática. Se debe por tanto frenar la tendencia a ocultar información al público en general."

El nivel de la libertad de acceso a la información varía de un país a otro. Merecen destacarse en particular ciertos sucesos en la materia ocurridos últimamente. Por ejemplo, una de las consecuencias de la reciente Primavera Árabe ha sido la inclusión en la Constitución[124] de ciertos países árabes de una disposición que garantiza el derecho a la información[125]. En cambio, los ciudadanos de los Estados Unidos tienen más dificultades para acceder a la información en manos de su gobierno después de la adopción de la *Patriot Act* (Ley Patriótica).

Aunque se ha solicitado a los Estados naciones reconocer y respetar el derecho a la información, conviene indicar que a menudo ese derecho ha sido objeto de restricciones por parte de las autoridades cuando estiman que obstaculiza o pone en peligro la protección de la seguridad nacional, la integridad territorial, la seguridad pública, la prevención de los delitos, la protección de salud y las costumbres, el

---

122 http://www.rjionline.org/MAS-Codes-Peru-Lima-Principles

123 http://www.itu.int/wsis/docs2/tunis/off/7.pdf

124 http://www.shorouknews.com/news/view.aspx?cdate=30092013&id=9bc20aff-06e7-4c44-8c45-fc197559616f

125 http://www.shorouknews.com/news/view.aspx?cdate=30092013&id=9bc20aff-06e7-4c44-8c45-fc197559616f

respeto de la vida privada, la reputación y otros derechos de los ciudadanos. No obstante, esas restricciones deben estar conformes a la legislación y responder a criterios de imparcialidad jurídica y de buen funcionamiento de la democracia.

En el ciberespacio, la libertad de información otorga a las personas y a las organizaciones la posibilidad de alcanzar un mayor grado de libertad de expresión y de intercambio social. Al mismo tiempo, plantea una nueva serie de dificultades que pueden limitar la utilización de los medios sociales. La Primavera Árabe y los documentos sustraídos por Wikileaks constituyen los ejemplos más recientes. Esos casos, aparte de los problemas que plantean para los intereses nacionales y el secreto de los datos clasificados, ponen de relieve las restricciones y prácticas policiales que los gobiernos y las entidades del sector privado aplican a Internet.

Tras los compromisos adoptados por el G8 en 2004 para promover un entorno propicio al diálogo informal, flexible, abierto e integrador, los países de Oriente Medio y de África del Norte lanzaron ese mismo año una iniciativa, *Forum for the Future*. Más adelante, en julio de 2008, organizaciones árabes de la sociedad civil procedentes de Bahréin, Egipto, Jordania y Marruecos crearon la Red árabe para la libertad de la información. Sin embargo, pese a las actividades de promoción concertadas en la región, la legislación relativa a la libertad de información no ha avanzado en la mayoría de los países árabes. Jordania y Túnez son los únicos Estados árabes que han adoptado una ley sobre la libertad de la información, aunque se han debatido proyectos de ley en la materia en Bahréin, Egipto, Kuwait, Líbano, Marruecos, Palestina y Yemen. En Líbano, en 2004, un grupo de abogados libaneses elaboró un proyecto de ley sobre la protección de los denunciadores de irregularidades, con la ayuda de la *American Bar Association*. Ese proyecto fue presentado al parlamento del país en 2010 por la Red nacional para el derecho de acceso a la información en Líbano.

Privacidad: protección contra la comunidad mundial de inteligencia

La privacidad es una libertad civil relativa a las libertades personales, a la dignidad y a la integridad. Consiste en el derecho de los ciudadanos a una protección contra todo tipo de intrusión injustificada del Estado en su vida, como los registros domiciliarios no autorizados y el espionaje de sus comunicaciones y su correspondencia. En la era digital, la privacidad es considerada en un nuevo contexto. Ya no se limita a la protección del entorno físico o material, como el domicilio, el correo o los documentos, sino que se aplica asimismo al enorme volumen de datos personales

presentes en el ciberespacio y al alto nivel de conectividad que hace de cada persona un "sensor de la comunidad mundial de inteligencia".[126]

No hay consenso mundial con respecto a lo que puede considerarse una protección adecuada de la vida privada. No obstante, existe un marco jurídico internacional básico para el derecho a la vida privada, que puede aplicarse al ciberespacio, y que da cuenta de las disposiciones de las legislaciones y declaraciones, así como de los convenios y tratados.

El Artículo 12 de la Declaración Universal de los Derechos Humanos reconoce que la vida privada es un derecho humano fundamental. Según esta Declaración, nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, y toda persona tiene derecho a la protección de la ley al respecto.

El Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos dispone que "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

Entre otras directrices, convenios y directivas pertinentes pueden indicarse:

- Las "Directrices sobre la protección de la vida privada y la transmisión transfronteriza de datos personales", publicadas en 1980 por la Organización de Cooperación y Desarrollo Económicos (OCDE).
- El "Convenio para la protección de las personas con respecto al tratamiento automático de los datos personales", publicado en 1981 por el Consejo de Europa.
- Las "Directrices sobre la utilización de los flujos de datos personales informatizados", publicadas en 1989 por el Consejo de Europa.
- Los "Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales", publicados en 1999 por las Naciones Unidas.

---

126 Philippe Langlois, fundador de la sociedad Priority One Security, con sede en París, a propósito de la capacidad de las agencias de recopilar los datos personales de los usuarios de teléfonos inteligentes (*smartphones*).

http://www.nytimes.com/2014/01/28/pageoneplus/quotation-of-the-day-for-tuesday-january-28-2014.html?_r=0

Esos instrumentos establecen principios que garantizan una protección mínima de la privacidad de las informaciones personales en todas las etapas de su tratamiento (recopilación, almacenamiento, difusión, utilización, transferencia, etc.). Reconocen asimismo el derecho de los particulares a acceder a sus datos personales, a ponerlos al día y a ser informados de los métodos y objetivos de las operaciones de recopilación de datos. Por otra parte, establecen el derecho de las personas a hacer destruir sus datos una vez alcanzado el objetivo de su recopilación y tratamiento, que corrobora el derecho al olvido en Internet. A escala regional, ciertos países ya han dispuesto medidas y niveles mínimos de protección con respecto a cuestiones sobre la privacidad.

La Directiva de la Unión Europea (UE) de 1995 sobre la protección de los datos autoriza la recogida de datos personales con fines precisos, explícitos y legítimos, y prohíbe la retención de datos que no estuvieran actualizados o no fueran pertinentes y exactos. Asimismo, los Estados Miembros de la UE deben impedir la transferencia de esos datos a terceros países[127] en ausencia de medidas equivalentes que aseguren la protección de los datos y el derecho de los ciudadanos a acceder a sus datos, a protegerlos y a modificarlos, y a negar a un tercero el derecho de utilizarlos.

Por ejemplo, para autorizar la circulación transfronteriza de datos hacia los Estados Unidos, donde no existe esa obligación de respetar un cierto nivel de protección, la UE ha concertado con ese país el "Acuerdo de inmunidad" (*Safe Harbour Agreement*), en virtud del cual se autoriza a ciertas empresas estadounidenses a recopilar datos sobre ciudadanos de la UE, con la condición de que den muestra de su determinación de garantizar la protección de esos datos con arreglo a las normas de la UE. Además, se solicita a esas empresas que mantengan informados a los ciudadanos de la UE con respecto a las modalidades de tratamiento y utilización de sus datos, y que reconozcan el derecho de esos ciudadanos a acceder a sus datos, a no divulgarlos y a modificarlos.

A nivel regional, la Directiva de la UE sobre la protección de los datos regula la libre circulación de datos personales entre sus Estados Miembros e impone la adopción de sus disposiciones en las legislaciones nacionales, autorizando al mismo tiempo a cada país de la UE a establecer sus propios criterios de aplicación. Se debe garantizar a las

---

127 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos – *Diario Oficial L 281 de 23/11/1995 p. 0031 - 0050*.

– (57) Considerando, por otra parte, que cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales;

personas su derecho a conocer el origen de los datos, a hacer corregir los datos inexactos, a presentar un recurso de apelación en caso de tratamiento ilícito de los datos, y a no autorizar su utilización en ciertas circunstancias.

A nivel nacional, casi todos los países reconocen un derecho constitucional a la vida privada. Ciertas nuevas constituciones (Sudáfrica) y numerosos países europeos, han aprobado leyes destinadas a reglamentar la vigilancia de los datos personales y a proteger la vida privada de los ciudadanos[128]. Las Naciones Unidas han respaldado la protección de la vida privada aprobando un proyecto de Resolución[129], elaborado por Brasil y Alemania, llamado "El derecho a la privacidad en la era digital".[130]

Libertad de expresión: sello distintivo de las sociedades democráticas

En las sociedades democráticas, la legislación, la libertad de palabra y la independencia de la sociedad civil son garantes de la libertad y las libertades civiles, en oposición a los rasgos característicos de los regímenes tiránicos, como la impunidad de la policía, los juicios sin las debidas garantías y la detención arbitraria.

En virtud del Artículo 19 de la Declaración Universal de los Derechos Humanos, así como del Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión." La libertad de expresión indica la capacidad de expresar libremente las ideas y opiniones sobre asuntos económicos, políticos, sociales y de otro tipo, mediante todos los medios de comunicación existentes como, por ejemplo, la escritura, la pintura, la radiodifusión o los blogs. Por tanto, la libertad de la prensa y la libertad de utilizar los medios sociales se inscriben en la libertad de expresión.

---

128 FISA Amendments Act of 2008, Communications Assistance for Law Enforcement Act, en los Estados Unidos - Data Protection Act 1998 y Regulation of Investigatory Powers Act (RIPA) en el Reino Unido – Ley informática y libertades (1978) en Francia – Convenio de la UE sobre la protección de los datos personales, Directiva sobre la conservación de datos de la UE.

129 La Asamblea General se pronuncia a favor del derecho a la vida privada en la era digital.

http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UwCw6ThWHZY

130 Sexagésimo octavo Periodo de Sesiones – Tercera Comisión – Tema 69 b) del programa – Promoción y protección de los derechos humanos: Cuestiones de derechos humanos, incluidos otros medios de mejorar el goce efectivo de los derechos humanos y las libertades fundamentales.

Del mismo modo, el Artículo 11 de la Carta de los Derechos Fundamentales de la UE, correspondiente al Artículo 10 del Convenio Europeo de Derechos Humanos, dispone que: "Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras." Estipula asimismo que: "El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial." Por otra parte, como para todas las restricciones de derechos y libertades, reconoce los principios de necesidad y proporcionalidad, así como la necesidad de impedir prácticas arbitrarias o discriminatorias.

En consecuencia, la libertad de expresión se considera esencial para la confianza de los ciudadanos en su gobierno y en el sistema político, dado que permite la aplicación de otros derechos humanos, una mejor comprensión de las políticas públicas, la creación de una opinión pública bien informada y la libertad de expresar sus preocupaciones a través de los medios. A nivel nacional, la libertad de expresión es reconocida en un gran número de constituciones como un sello distintivo de los regímenes democráticos. En este contexto, la Asamblea General de las Naciones Unidas estima que la vigilancia de las redes de telecomunicación amenaza los derechos humanos y las libertades civiles, desde la libertad de opinión y de expresión al derecho a la vida privada y al activismo político, y socava los cimientos de la sociedad democrática[131].

131 Asamblea General de las Naciones Unidas - 16 de mayo de 2011 A/HRC/17/27- Consejo de Derechos Humanos – Decimoséptimo Periodo de Sesiones – Tema 3 de la agenda – Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo – "La utilización incesante y cada vez más avanzada de la vigilancia digital ha privado a las sociedades de la aptitud para decidir su propia utilización en un marco legislativo, lo que da lugar a "prácticas ad hoc que escapan a la supervisión de toda autoridad independiente" y amenaza con reprimir la libertad de expresión."

La libertad de expresión en línea debe pues ser respetada y los gobiernos deben evitar ahogarla y suprimir todos los obstáculos en ese sentido. En particular, a los fines de nuestra presentación, no deben recurrir a la ciberrepresión para hacer callar las voces de la oposición, y han de evitar interceptar las comunicaciones, censurar los contenidos y bloquear los sitios web.

Sin embargo, en realidad, numerosos países no respetan la libertad de expresión. Algunos gobiernos evocan la protección de los valores religiosos y la decencia, además de la seguridad nacional y la lucha contra el terrorismo, para justificar las restricciones de la libertad de expresión en línea. Censuran contenidos que consideran sexualmente explícitos o que incitan al odio sobre la base de consideraciones raciales, religiosas o de otros factores culturales, o que alientan actividades terroristas. El peligro reside en la terminología jurídica utilizada para reprimir esos contenidos, que es generalmente ampliable y puede por tanto perder objetividad y afectar la estabilidad de la justicia, dando lugar a abusos de autoridad.

Redes sociales

Las discusiones, los intercambios de opiniones y objetivos comunes, así como los grupos de presión, son tradicionalmente las etapas preliminares de la organización de protestas que pueden conducir a una revolución. La abundancia de intercambios en las redes sociales con respecto a la libertad de Internet y la democracia, asociada a la capacidad incesante de los ciudadanos de influir en la vida política nacional, ha cumplido una función decisiva en la configuración del debate político durante la Primavera Árabe. Los ciudadanos han tenido a su alcance un nuevo espacio de expresión gracias a los blogs, los tweets y las telecargas en YouTube. Según un activista egipcio: "Internet merece la más elevada protección contra las intrusiones del Estado. Si quieres liberar a los pueblos, dales Internet".

Las redes sociales crean una capacidad sin precedentes de movilización de las personas y de intercambio de informaciones clandestinas. Ofrecen grandes posibilidades en materia de organización y difusión de información y pueden contribuir a crear y estructurar grupos de oposición, reclutar militantes, atraer simpatizantes, difundir ideologías y constituir redes de apoyo internas y externas. Durante la Primavera Árabe, los militantes han utilizado los medios sociales para obtener apoyo regional e internacional y para organizar campañas de propaganda.

Si bien las redes sociales no pueden sustituir las acciones físicas necesarias para impulsar con éxito una revolución, han ofrecido a los ciudadanos árabes la posibilidad de utilizar la información como un arma contra la represión. Los participantes de los movimientos de la Primavera Árabe utilizaron las redes sociales para mantenerse en contacto, intercambiar información, difundir noticias relativas a los últimos

acontecimientos, organizar sus actividades, difundir informaciones y noticias, enviar mensajes al mundo e influir en la opinión pública. Las imágenes y los videos enviados a través de teléfonos móviles han permitido obtener informaciones sobre las fuerzas gubernamentales y sus posiciones. Las acciones políticas fueron organizadas esencialmente por medio de las redes sociales. Antes y durante los cambios de régimen que tuvieron lugar en varios países árabes debido a la Primavera Árabe se observó una propagación viral de tweets de grupos de oposición que llegaron a millones de usuarios y de páginas Facebook. Los blogs aumentaron de forma espectacular generando en toda la región discusiones sobre la democracia, la libertad y la transparencia. Millones de ciudadanos participaban en los medios sociales y se crearon numerosas páginas y sitios para promover a la oposición a través de mensajes en línea y blogs. Algunos activistas filmaron con sus teléfonos móviles y publicaron secuencias en tiempo real de los acontecimientos en Facebook, Twitter y otras redes sociales. Hoy, muchos eslóganes de esos días son utilizados frecuentemente en diferentes países en ocasión de diversas protestas sociales, políticas y económicas.

En el curso del año pasado se han producido en Líbano ataques inquietantes contra la libertad de expresión. La reputación del país como bastión de la libertad de palabra ha sido empañada por una serie de arrestos, detenciones e intimidaciones de ciudadanos libaneses debido a sus actividades en línea, en particular en los medios sociales.

Las personalidades políticas libanesas adoptan al parecer una actitud cada vez más defensiva, cuestionada abiertamente en tweets de 140 caracteres u otros contenidos difundidos en las redes sociales. Por ejemplo, cuatro usuarios de Facebook fueron arrestados y un usuario de Twitter condenado a dos meses de prisión por haber insultado al Presidente de la República. En otro caso, un bloguero fue detenido durante más de ocho horas y amenazado de acción judicial si seguía firmando textos políticos en lugar de limitarse a la poesía. Las autoridades encargadas del ciberdelito interrogaron a varios blogueros y bloquearon algunos blogs, entre ellos una publicación referida al tratamiento injusto de trabajadores de una importante cadena de supermercados.

Esas decisiones, que se asemejan a sanciones impuestas en países autocráticos, son inhabituales en el Líbano, donde la expresión de opiniones ha sido relativamente poco reglamentada en el pasado.

Peligros: hechos y actores

El ciberespacio representa la nueva dimensión de la seguridad nacional y es una valiosa fuente para la recopilación de información de inteligencia. Sin embargo, ya no son adecuadas las formas tradicionales de supervisión y recopilación de información por parte de las agencias de seguridad.

Hoy en día, existe la necesidad de identificar y tener en el punto de mira a conspiradores y anticiparse a las acciones de redes que pueden ser de carácter malicioso y delictivo. A tal fin se han desplegado tecnologías sofisticadas para la vigilancia masiva de redes de computadoras y de usuarios para detectar, identificar y hacer un seguimiento de intrusos y preservar datos que puedan servir de prueba.

La recopilación de datos personales y el abuso asociado de las libertades civiles son titulares frecuentes en los medios de comunicación de todo el mundo; las revelaciones de los casos Snowden, WikiLeaks y Tempora[132], entre otros, han contribuido a incrementar la presión sobre la red a través de los sistemas SORM-2 y SORM-3[133], el "registro único"[134], y la censura de las redes sociales[135]. Recientemente algunos gobiernos han incrementado los controles sobre Internet con medidas que garantizan la identificación de los usuarios en línea[136].

---

132 Tempora, es un sistema de computación para la vigilancia electrónica con fines de seguridad y de carácter clandestino puesto a prueba en in 2008,[2] establecido en 2011 y operador desde el Cuartel General de Comunicaciones del Gobierno (GCHQ) del Reino Unido. Tempora permite interceptar las comunicaciones cursadas a través de los cables de fibra óptica que constituyen la red troncal de Internet para acceder a grandes volúmenes de datos personales de usuarios de Internet. http://en.wikipedia.org/wiki/Tempora

133 Esta ley está aparentemente en contradicción con el Artículo 23 de la Constitución de Rusia que establece lo siguiente:[32]

1. Las personas tienen el derecho a la inviolabilidad de su vida privada, secretos personales y familiares, a la protección del honor y del buen nombre.
2. Las personas tienen el derecho a la privacidad de su correspondencia, conversaciones telefónicas y mensajes postales, telegráficos y de otro tipo. Las limitaciones a este derecho en sólo serán posibles en virtud de una decisión judicial.

134 Véase "Ex-Soviet States, Russian Spy Tech Still Watches You" – de Andrei Soldatov e Irina Borogan – 12.21.12 6:30 AM.
http://www.wired.com/dangerroom/2012/12/russias-hand/all/

135 King, Gary, Jennifer Pan, y Margaret Roberts. 2014. Reverse Engineering Chinese Censorship through Randomized Experimentation and Participant Observation. Copia disponible en http://j.mp/16Nvzgehttp://gking.harvard.edu/publications/randomized-experimental-study-censorship-china

136 China obliga al registro del nombre real de quienes realizan telecargas de videos en línea. http://www.reuters.com/article/2014/01/21/us-china-internet-idUSBREA0K04T20140121

Las agencias de seguridad pueden acceder a datos personales que se contrastan con listas de objetivos de inteligencia. Las tecnologías de vigilancia les permiten determinar la ubicación de objetivos utilizando mapas de Google o sistemas GPS para el seguimiento de movimientos, o utilizar componentes incrustados en imágenes puestas en circulación en las redes sociales. Dichas tecnologías permiten obtener listas de direcciones y de números de teléfono de familiares y amigos mediante el registro y almacenamiento de correos electrónicos. Según reflejan documentos secretos de la inteligencia británica, los espías pueden incluso estar ocultos en aplicaciones de juegos populares a fin de obtener datos que revelen ubicación, edad, sexo y otras informaciones personales de los jugadores.

Este fenómeno debilita en gran medida la privacidad y muchas otras libertades civiles. Pero los retos a nuestra privacidad y a otras libertades civiles no sólo proceden de gobiernos. Actores públicos y privados realizan una vigilancia ilegal de individuos por considerarlo útil para recopilar información con fines de conocimiento e inteligencia del mercado. Empresas grandes y pequeñas realizan un seguimiento de lo que compramos, compilan datos personales para enviar publicidad personalizada a los teléfonos móviles de las personas, y almacenan y analizan datos con fines comerciales. En ocasiones recopilan datos especialmente sensibles etiquetados como opcionales y relativos, entre otros, a aspectos étnicos y de orientación sexual.

Los gobiernos aplican la censura mediante técnicas como el filtrado en Internet, el despliegue de herramientas maliciosas de supervisión como troyanos[137], y restricciones al anonimato en línea. Con estas medidas los Estados pretenden facilitar la vigilancia de las comunicaciones al simplificar la identificación de individuos que acceden o difunden contenidos prohibidos y recopilar información de inteligencia.

La escala de los datos que se recopilan y de la intrusión en las comunicaciones es muy notable, y desconcertante, y representa un serio riesgo para la privacidad y las libertades civiles.

No obstante, algunos aspectos positivos de esta vigilancia son evidentes. Por ejemplo, la vigilancia permitió frustrar un complot de Al Qaeda para la colocación de una bomba en Alemania en 2007 y la detención de traficantes de drogas[138] y responsables

---

137 La aplicación QQ de China se considera un troyano gigantesto.

138 Detección de Guzmán, el señor de la droga. http://news.yahoo.com/internet-crucial-venezuela-battleground-075124059.html

de redes de pornografía infantil[139]. En este contexto, puede mencionarse el proyecto europeo INDECT "sistema de información inteligente para la observación, búsqueda y detección con fines de seguridad de ciudadanos en entornos urbanos", que tiene por objetivo garantizar la seguridad de los ciudadanos, principalmente en relación con la violencia.

Foco en el mundo árabe[140]

La mayoría de los países árabes son miembros de las Naciones Unidas y todos ellos pertenecen a la Liga de los Estados Árabes, que se compone de Estados árabes soberanos del norte y noreste de África y del sudoeste de Asia. El objetivo de la Liga es fortalecer las relaciones entre los Estados Miembros para impulsar la cooperación entre ellos y salvaguardar su independencia y soberanía. Más en concreto, se pretende crear una estrecha cooperación en las esferas económica, financiera, de comunicaciones, de la salud, social y cultural así como en asuntos sobre nacionalidad, pasaportes, visados, ejecución de sentencias y extradición de delincuentes.

Los países árabes están comprometidos con el respeto a la libertad de expresión de conformidad con el Artículo 19 de la Declaración Universal de los Derechos Humanos y con el Artículo 32 de la Declaración Árabe de Derechos Humanos, cuyo enunciado es semejante al del mencionado Artículo 19.

Las costumbres y tradiciones sociales, así como la religión, son por lo general las razones declaradas de ciertas restricciones y de medidas represivas. En algunos países se han aprobado legislaciones de urgencia, que siempre están destinadas a reprimir opiniones disidentes a través de la persecución de quienes se atreven a expresas sus ideas libremente. Pueden ser víctimas de detenciones, tortura y encarcelamientos brutales, acusados de traición o de complot contra la seguridad e intereses nacionales. Algunos gobiernos establecen o imponen sus capacidades para restringir las libertades civiles a través de mecanismos intermediarios (proxy) de seguridad de tipo "*blue coat*" y otras tecnologías importadas para el seguimiento y bloqueo de las comunicaciones de disidentes.

---

139 Cómo la alta tecnología de la vigilancia de la NSA ha ayudado a la captura de terroristas en Europa. http://www.civilbeat.com/articles/2013/06/21/19341-how-the-nsas-high-tech-surveillance-helped-europe-catch-terrorists/.

140 En este documento se define el mundo árabe como el formado por los miembros de la Liga de los Estados Árabes: Argelia, Bahrein, Comoras, Djibouti, Egipto, Iraq, Jordania, Kuwait, Líbano, Libia, Mauritania, Marruecos, Omán, Territorios Palestinos, Qatar, Arabia Saudí, Somalia, Sudán, Siria (suspendido), Túnez, Emiratos Árabes Unidos y Yemen.

La censura en línea está muy extendida aunque los gobiernos señalan que sólo censuran sitios pornográficos. Los usuarios pueden ser dirigidos a un servidor intermediario (proxy) que mantiene una lista de sitios web prohibidos y bloquea el acceso a materiales considerados incompatibles con la religión, la cultura, la política y los valores morales locales. La mayoría de los periodistas y blogueros practican la autocensura, particularmente en relación con asuntos relacionados con la política, la cultura o la religión local o cualquier otro asunto que las autoridades puedan considerar política o culturalmente sensible. Por lo general se evita la crítica al Jefe del Estado u otros altos cargos, así como la publicación de información que pueda deteriorar la reputación del país, las relaciones internacionales o la economía nacional. La difamación es un delito.

En un caso que alcanzó gran resonancia en los Emiratos Árabes Unidos, el periodista independiente Mark Towsend, antiguo editor de la sección de negocios del periódico de Dubái de habla inglesa Khaleej Times, fue acusado de difamación y no pudo abandonar el país durante los casi dos años que duró la investigación. Fue acusado en virtud del Artículo 373 del código penal por haber publicado ilegalmente artículos en los que criticaba al Khaleej Times, en el que el gobierno tiene una participación del 30 por ciento, y se enfrentó a una condena máxima de dos años de prisión y una multa de 20 000 dirhams (5 400 dólares USA). Finalmente fue absuelto en mayo de 2011. En otro caso ocurrido también en 2011, cinco activistas y blogueros de los Emiratos fueron detenidos y acusados de insultar a los líderes de la EAU a través de artículos publicados en el foro de Internet Hewar de los EAU. Fueron condenados a sentencias de prisión.

En un sentido más positivo, Internet se ha convertido en un espacio útil para la organización de los activistas y en un mecanismo de influencia. Sin embargo, los países Árabes no dudan en cortar el acceso a Internet cuando se producen demostraciones civiles contra los gobiernos.

En el mundo árabe la privacidad se percibe esencialmente en términos físicos y materiales. Está centrada en factores como la inviolabilidad del domicilio, la correspondencia personal y las comunicaciones. Sin embargo, los sistemas jurídicos árabes no protegen adecuadamente el derecho a la privacidad, salvo casos excepcionales en los que la constitución o las leyes contemplan dicha protección.

En Líbano la privacidad no tiene un estatus jurídico bien definido, aunque los líderes políticos han debatido ampliamente sobre este asunto. Está protegida mediante una combinación de disposiciones constitucionales y legislativas. La constitución libanesa, a semejanza de las de los Estados Unidos de América, no define el derecho a la privacidad Sin embargo, salvaguarda la protección de las personas, su residencia y efectos personales.

Algunas disposiciones protegen la exposición de la vida personal en circunstancias específicas. El Artículo 17 establece que la residencia de la personas es inviolable y que nadie puede acceder a la misma salvo en circunstancias específicas y de conformidad con lo definido por ley. Además, una ley sobre escuchas determina que los ciudadanos tienen derecho a la privacidad de sus comunicaciones locales e internacionales, alámbricas e inalámbricas.

La constitución del Líbano reconoce el derecho de las personas a su seguridad, la de sus domicilios, documentos y efectos personales frente a registros e incautaciones no justificadas, que sólo pueden tener lugar si han sido autorizadas en las condiciones prescritas por la ley. Siguiendo el ejemplo de numerosos gobiernos de todo el mundo, la base jurídica utilizada en el Líbano para justificar una invasión de la privacidad que puede poner en riesgo las libertades civiles se nutre de pretextos como la seguridad nacional, el freno al terrorismo y la protección del bien público.

En el mundo árabe se utilizan pretextos similares para el bloqueo por parte de los gobiernos de redes sociales en Internet ocasionalmente utilizadas para promover u organizar protestas.

En marzo de 2013, Reporteros sin Fronteras declaró a algunos países árabes como "Estados enemigos de Internet"[141] debido a sus prácticas represivas contra blogueros, que constituyen violaciones graves de la libertad de información y de los derechos humanos.

La Liga de los Estados Árabes y las libertades civiles

La Liga de los Estados Árabes fue creada siete meses antes de la creación de las Naciones Unidas por seis países (Egipto, Iraq, Líbano, Arabia Saudí, Siria y Transjordania) y actualmente veintidós Estados árabes son miembros de la misma.

La Carta de constitución de la Liga en 1945 no hace alusión a los derechos humanos. Tampoco los documentos jurídicos de la Liga recogen disposición alguna sobre la protección de los defensores de los derechos humanos.

---

141 Reporteros sin Fronteras, marzo de 2013 – Informe especial sobre la vigilancia en Internet titulado "Enemigos de Internet", centrado en cinco gobiernos y en cinco empresas. http://en.rsf.org/special-report-on-internet-11-03-2013,44197.html

Por otro lado, la Liga creó un comité de trabajo para desarrollar un sistema jurídico más integrado y armonizado mediante la unificación de términos, estructuras y procesos jurídicos y judiciales. Para aplicar las recomendaciones de este comité la Liga estableció el Centro Árabe de Estudios Jurídicos y Judiciales en Beirut. Este Centro ha elaborado numerosos convenios de cooperación entre países árabes en aspectos jurídicos que preocupan a todos los miembros, tales como el modelo de legislación contra el ciberdelito. Colabora con numerosas organizaciones internacionales y regionales, así como con organismos de la sociedad civil en relación con la gobernanza de Internet. Por ejemplo, ha trabajado con la Comisión Económica y Social para Asia Occidental de las Naciones Unidas para establecer el Foro Árabe para la Gobernanza de Internet. También es miembro fundador del Observatorio Pan Árabe para la Ciberseguridad desde 2009 y ha iniciado la elaboración de un convenio árabe sobre ciberseguridad que se remitirá al Consejo de Ministros Árabes de Justicia. El proyecto menciona claramente la protección de las libertades civiles como un elemento esencial para la creación de confianza en el ciberespacio. Al mismo tiempo, el Centro ha celebrado numerosos foros y reuniones anuales para responsables de la toma de decisiones en el ámbito de las TIC sobre aspectos relacionados con los derechos humanos y las libertades civiles, en particular los derechos de privacidad, de acceso a la información y de libertad de expresión.

Conclusión

Es necesario realizar esfuerzos legislativos concertados para alcanzar un equilibrio adecuado entre la necesaria protección de las libertades civiles, la privacidad de los usuarios de Internet y, en primera instancia y más importante, la libertad de expresión y, por otro lado, la necesaria lucha contra las ciberamenazas a la seguridad nacional. El éxito en este asunto evitará que el ciberespacio se convierta en un nuevo dominio sujeto a vigilancia.

Los Estados deben perseguir los ciberdelitos como delitos al amparo de la legislación nacional, que debe combinar medidas proactivas y reactivas para la protección de las libertades civiles. Un tratado o un acuerdo internacional específico que proporcione un nivel mínimo razonable de protección aceptable por todas las partes concernidas contribuiría a salvaguardar la privacidad de los intercambios de información. Ello debería ser complementado con un marco de cooperación internacional eficaz de lucha contra el cibercrimen transnacional. A este respecto el Centro Árabe de Estudios Jurídicos y Judiciales me ha solicitado la elaboración de un proyecto de convenio árabe para la cooperación en la lucha contra el cibercrimen transfronterizo.

En este marco de cooperación las investigaciones, seguimientos, acusaciones de las fiscalías, asistencia jurídica mutua y procedimientos judiciales deberían realizarse de conformidad con las leyes nacionales. Igualmente, cualquier procedimiento jurídico internacional debe ser conforme con la legislación nacional y los tratados de asistencia jurídica mutua. Los Estados deben disponer de procedimientos y medidas especiales para proteger el intercambio internacional de información sensible y supervisar las redes de computadoras, así como la recopilación y procesamiento de datos. Se trata de una necesidad para países que carecen de una legislación insuficiente sobre privacidad.

Debe prestarse una atención especial a la protección frente a registros e incautaciones ilegales. La naturaleza técnica del ciberespacio, junto con el nivel de crecimiento del ciberdelito y la ausencia de un marco de derecho penal internacional pertinente complican la tarea de garantizar el respeto a las libertades civiles.

En la mayoría de los sistemas jurídicos nacionales, el comportamiento de la policía está regulado por la constitución, la legislación y los procedimientos que protegen a los ciudadanos de los poderes y actuaciones abusivas en aplicación de la ley, como registros e incautaciones injustificadas y la violación de las libertades civiles cuando se llevan a cabo dichas operaciones.

Dado que numerosos países carecen aún de legislación y procedimientos para el ciberespacio, y aplican el régimen jurídico penal general a los asuntos del mismo, sus gobiernos podrían adoptar directrices para prevenir el abuso de las libertades civiles en ese ámbito. Dichas directrices deberían definir claramente las garantías de registros e incautaciones legales con los límites justificados de excepciones a las libertades civiles. Los autores de dichas directrices podrían inspirarse en las excepciones jurídicas tradicionales relacionadas con la "doctrina de los hallazgos casuales" ("*plain view*") o de las "circunstancias apremiantes".

Dichas excepciones podrían ser equilibradas con medidas de protección: encriptación, servidores anónimos de reenvío de correo, comunicaciones anónimas seguras, cortafuegos y servidores de representación (proxy). Muchas de dichas tecnologías ofrecen protección frente al ciberdelito y refuerzan la privacidad.

3.2 Marcos jurídico, político y reglamentario de la libertad en Internet y el *Big Data*

por Pavan Duggal

Introducción

El crecimiento exponencial del ciberespacio ha supuesto una revolución en el dinámico mundo actual. Internet ha hecho que la geografía sea historia, aunque el medio sin fronteras que es el ciberespacio constituye una enorme preocupación para todos los gobiernos del mundo. Por ese motivo, establecer marcos políticos y reglamentarios adecuados se ha convertido en un asunto críticamente urgente.

Internet se construye sobre información y datos en formato electrónico. De hecho, ambos términos, "datos" e "información" se utilizan indistintamente y se refieren a los bloques constitutivos esenciales para la creación de la arquitectura de contenidos que constituye la base de los canales de comunicación sobre los que funciona Internet.

El desarrollo de Internet ha recorrido un largo camino, desde la red ARPANET (*Advanced Research Projects Agency Network*) a finales de la década de los 60, pasando por la *World Wide Web* y otros elementos posteriores, hasta la actual era de las redes sociales, las comunicaciones móviles, las analíticas de datos y las comunicaciones en la nube (SMAC, *Social, Mobile, Analytics and Cloud*). Internet ha sido una gran palanca que ofrece libertad de acceso a la información a todos los usuarios y les ayuda a realizar numerosas actividades diarias y abordar aspectos de la vida de formas muy diversas.

En Internet se crean ingentes volúmenes de datos. El anterior CEO de Google, Eric Schmidt, declaró en 2010 que cada dos días "[…] creamos tanta información como se creó desde los albores de la civilización hasta el año 2003, aproximadamente cinco exabytes de datos". Haciéndose eco de esta asombroso crecimiento, IBM afirma que cada día generamos 2,5 trillones de bytes de datos "[…] tanto que el 90 por ciento de los datos que actualmente existen en el mundo han sido creados en los últimos dos años"[142]. Una evidencia adicional de este fenómeno se refleja en las estadísticas recogidas en el Informe de IDC-EMC que señala que el universo digital aumenta su tamaño en más de dos veces cada dos años y alcanzará los 40 000 exabytes

142 http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

(40 billones de gigabytes) en 2020[143]. La revista The Economist recoge en su informe panorámico de 2012 (2012 Outlook) que los datos digitales a nivel mundial crecieron de 130 exabytes en 2005 a 1 227 exabytes en 2010 y predice que se alcanzarán los 7 910 exabytes en 2015[144]. La preocupación sobre esos inmensos volúmenes de datos se ha agudizado por la aparición del *Big Data* en el ecosistema digital.

En este apartado se analizan los marcos jurídico, político y reglamentario de la libertad en Internet y del *Big Data*.

Definición

Antes analizar los aspectos jurídicos y reglamentarios relacionados con la libertad en Internet, deben tenerse en cuenta las diversas definiciones de este término que han sido propuestas por especialistas y juristas.

Definir la libertad en Internet es un asunto de gran calado y controvertido; no existe acuerdo sobre una definición universal. El Presidente Obama dijo en una ocasión: "Internet ha desencadenado la innovación, ha habilitado el crecimiento y ha inspirado la libertad de una forma más rápida y amplia que cualquier otro avance tecnológico en la historia de la humanidad. Su independencia es su poder. Internet ofrece un sistema de comunicación libre de la intervención de los gobiernos de una forma sin igual."[145] Añadió específicamente: "La libertad en Internet es inconsistente con la regulación de la neutralidad de la red y supone una libertad sin igual con respecto a la intervención del gobierno."

Derek Bambuer, profesor de derecho de la Universidad de Arizona ha dicho: "Posiblemente, la libertad en Internet es, en última instancia, un término que debería abandonarse por ser demasiado general para ser útil. En su lugar, los países, las culturas y los usuarios deberían abordar los complejos equilibrios de la comunicación en Internet."[146]

---

143 http://www.baselinemag.com/analytics-big-data/slideshows/surprising-statistics-about-big-data.html última actualización 4 de agosto de 2014

144 "Welcome to the yotta world', The Outlook for 2012, Economist, diciembre de 2011; http://www.economist.com/node/21537922

145 http://freestatefoundation.blogspot.in/2012/08/the-true-meaning-of-internet-freedom.html

146 Bambauer, D., The Enigma of Internet Freedom, eJournal USA, Vol.15, No.6, 2010, pp. 4-6., véase también http://www.wseas.us/e-library/conferences/2013/Dubrovnik/ECC/ECC-38.pdf, última actualización 8 de agosto de 2014.

La publicación "*Media Marxist outfit Free Press*" define la libertad en Internet en su página web de la forma siguiente: "Libertad en Internet significa que los proveedores de servicios de Internet (ISP) no puedan discriminar entre distintos tipos de contenidos y aplicaciones en línea"[147]. Dictionary.com define la neutralidad de la red como el principio en virtud del cual los protocolos de Internet básicos no deben ser discriminatorios, en particular, considera que los proveedores de contenidos deben recibir todos el mismo tratamiento de los operadores de Internet.

Libertad en Internet significa espectro abierto

Si bien los radiodifusores y las empresas de telefonía móvil disponen de licencias otorgadas por los gobiernos para ciertos segmentos del espectro radioeléctrico, otras partes del espectro están abiertas, es decir, cualquier empresa puede desarrollar productos, como un teléfono sin cordón para el hogar, auriculares Bluetooth, dispositivos para la vigilancia de los niños o para el control a distancia, que utilicen dicho espacio abierto sin necesidad de una licencia del gobierno[148].

La libertad en Internet trae consigo no sólo la libertad de acceso a dicho medio, sino también la libertad de expresarse individualmente. Aún más importante, significa la libertad para hacer más fácil la vida de las personas gracias al gran número de facilidades que ofrece Internet.

Características más destacadas

Algunos estudiosos han llegado a la conclusión de que la libertad en Internet abarca una amplia gama de libertades fundamentales, como la libertad de palabra, el derecho a la privacidad, la libertad de innovar y de ser recompensado y reconocido, así como la libertad de la arquitectura de Internet en su conjunto[149].

---

147 http://pjmedia.com/tatler/2013/01/22/the-lefts-warped-definition-of-internet-freedom-and-an-open-internet/

148 http://pjmedia.com/tatler/2013/01/22/the-lefts-warped-definition-of-internet-freedom-and-an-open-internet/

149 Neelie Kroes, *Internet Freedom,* http://europa.eu/rapid/press-release_SPEECH-12-326_en.pdf, última actualización el 8 de agosto de 2014.

Marcos políticos y reglamentarios existentes

Pese al desarrollo de Internet como un medio global sin fronteras, sigue siendo un hecho que el mundo en su conjunto aún no ha dedicado recursos al desarrollo de normas internacionalmente aceptadas aplicables al ciberespacio. En consecuencia, cuando se habla de marcos jurídico, político y reglamentario es importante recordar que no existen tratados internacionales sobre la libertad en Internet. No obstante, se han logrado avances en esta dirección.

Tal como se señala en este Informe, el Convenio sobre la Ciberdelincuencia de 2001 del Consejo de Europa es un ejemplo relevante a este respecto. Las características más destacadas de dicho Convenio son las siguientes:

- Es el primer tratado internacional cuyo objetivo es abordar el ciberdelito mediante la armonización de las legislaciones nacionales pertinentes, proporcionar definiciones comunes para ciertos delitos mediante la mejora de las técnicas de investigación y aumentar la cooperación "en la mayor medida posible" entre las naciones para luchar contra este fenómeno[150].
- Exige la criminalización de actividades como el pirateo y los delitos de pornografía infantil y la ampliación de la responsabilidad penal por violaciones de la propiedad intelectual.
- Proporciona un política común sobre el delito destinada a proteger la sociedad contra el ciberdelito mediante la aprobación de una legislación adecuada y el impulso a la cooperación internacional[151].

La Declaración sobre la Libertad de Comunicación en Internet aprobada por el Consejo de Europa en 2003 es otro ejemplo notable de los esfuerzos en esta materia. Las características esenciales de dicha Declaración son las siguientes:

- establece la necesidad de equilibrar la libertad de expresión e información con otros derechos e intereses legítimos, de conformidad con el Artículo 10 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales
- expresa su preocupación por los intentos de limitar el acceso público a la comunicación en Internet por motivos políticos u otros motivos contrarios a principios democráticos;

---

150 http://en.wikipedia.org/wiki/Convention_on_Cybercrime, última actualización 8 de agosto de 2014.

151 http://epic.org/privacy/intl/ccc.html

- afirma que el control previo de las comunicaciones en Internet, con independencia de las fronteras, debe seguir siendo una excepción;
- considera necesario eliminar obstáculos al acceso individual a Internet, y complementar las medidas ya emprendidas para establecer puntos de acceso públicos;
- expresa su convicción de que la libertad de prestar servicios a través de Internet contribuirá a garantizar el derecho de los usuarios a un acceso plural a contenidos de una variedad de fuentes nacionales y extranjeras;
- subraya que la libertad de comunicación en Internet no debe ir en detrimento de la dignidad humana, los derechos humanos y las libertades fundamentales de los demás, especialmente de los menores de edad;
- acoge con satisfacción los esfuerzos de los proveedores de servicio de cooperar con las fuerzas del orden contra los contenidos ilícitos en Internet.

CMSI

La Cumbre Mundial sobre la Sociedad de la Información hizo las siguientes propuestas a la Alianza Mundial para la Medición de las TIC para el Desarrollo con el objetivo de:

- Que continúe, amplíe y profundice en su labor sobre la medición de la sociedad de la información, incluyendo la participación de las oficinas nacionales de estadística en las etapas más tempranas posibles de la elaboración de datos estadísticos.
- Que continúe elevando la sensibilización y la creación de capacidad, prestando especial atención a países de bajos ingresos.
- Que considere nuevas fuentes de datos y metodologías.
- Que establezca un Grupo de Expertos sobre las metas de la CMSI.

Hubo un gran consenso en que el proceso de la CMSI y la supervisión de la sociedad de la información deben continuar después de 2015 y, al mismo tiempo, continuar profundizando sobre la naturaleza de dicha supervisión. La cooperación internacional y la coordinación nacional deben continuar y construir sus trabajos en base al modelo de múltiples partes interesadas.[152]

---

152 *Documento de conclusiones del Evento de Alto Nivel CMSI+10. Vía del Foro*, http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/OutcomeDocument2014.pdf (última actualización 6 de noviembre de 2014).

La Declaración de Libertad en Internet constituye una defensa vibrante de las libertades en línea[153]. En su preámbulo declara que una Internet libre y abierta puede lograr un mundo mejor[154]. Persigue además que millones de usuarios de Internet firmen la Declaración[155]. La Declaración apoya la aplicación de cinco principios básicos de la política de Internet:

- Eliminación de la censura en Internet.
- Acceso universal a redes rápidas y asequibles.
- Libertad de conexión, comunicación, creación e innovación en Internet.
- Protección de las nuevas tecnologías y de los innovadores frente al abuso de los usuarios.
- Derechos a la privacidad y a la capacidad de los usuarios de Internet de proteger su privacidad mediante una revelación controlada de información sobre los mismos.[156]

Carencias del Marco

No obstante, lo que claramente falta es un régimen internacional sobre la libertad en Internet que sea aceptado por todas las partes interesadas. Además, el fenómeno de la libertad en Internet plantea diversas cuestiones jurídicas, políticas y reglamentarias, algunas de las cuales se analizan a continuación.

Hoy en día, en muchas jurisdicciones de todo el mundo existen derechos fundamentales/legislaciones nacionales que garantizan la libertad de palabra y de expresión. Estos mismos derechos también se han interpretado o aplicado a la libertad de palabra y de expresión en Internet. Sin embargo, las revelaciones de Snowden han puesto de manifiesto la existencia de intrusiones no autorizadas en la libertad de palabra y de expresión en Internet. Sin saberlo los usuarios, sus comunicaciones de audio, vídeo, imágenes o texto son vigiladas por varias fuentes. En efecto, Internet y sus instalaciones y plataformas se están convirtiendo en vectores que permiten una

---

153 http://en.wikipedia.org/wiki/Declaration_of_Internet_Freedom, última actualización 8 de agosto de 2014.

154 http://www.internetdeclaration.org/ última actualización 4 de agosto de 2014.

155 Declaración de la libertad en Internet, http://www.savetheinternet.com/internet-declaration

156 http://en.wikipedia.org/wiki/Declaration_of_Internet_Freedom, última actualización 8 de agosto de 2014.

sociedad basada en la vigilancia. Por tanto, es claro que existen dos tipos de personas en el mundo: las que saben y las que no saben que están siendo o han sido vigiladas.

El aumento de la vigilancia y la supervisión en línea se está convirtiendo en la norma, y tiene un impacto directo sobre la libertad de palabra y de expresión en Internet. En resumen, si bien Internet no es exactamente el "salvaje oeste", existen pruebas que ponen en evidencia que la libertad de palabra en el ciberespacio no es una libertad absoluta.

Las normas de comportamiento civilizado también se aplican al ciberespacio. Esto significa que la legislación nacional debe prohibir cualquier contenido en Internet destinado a causar molestias, animadversión, odio, enemistad, o que en ese sentido se dirija específicamente a una persona o grupo de personas.

Sin embargo, la cobertura de anonimato que ofrece Internet puede inclinar a algunos usuarios malintencionados o abusivos a la autocomplacencia de decir y hacer lo que deseen con inmunidad.

No obstante, en este contexto y en diversos regímenes de todo el mundo, se está creando jurisprudencia en virtud de la cual los tribunales empiezan a están tomando decisiones para desvelar el anonimato al ordenar a proveedores de servicios que comuniquen la verdadera identidad de las personas que están detrás de actividades ilegales. Sin embargo, como ya se ha dicho, sigue siendo un hecho que no existe una norma internacional que defina lo que constituye la libertad de palabra y de expresión en Internet.

La Declaración Universal de los Derechos Humanos de 1948 proporciona ciertos principios básicos que pueden interpretarse plenamente compatibles con el concepto de libertad en Internet.

Nuevos retos

Las redes sociales permiten que se celebren nuevos tipos de debates en línea en los que las personas manifiestan sus opiniones y formas de pensar. Sin embargo, las leyes y legislaciones de todo el mundo no han evolucionado lo suficientemente rápido como para hacer frente a los nuevos desafíos inherentes a las redes sociales.

Los teléfonos inteligentes y otros dispositivos de comunicación han impulsado la aparición de la web móvil. La combinación de teléfonos móviles e Internet permite manifestaciones hasta ahora desconocidas de libertad de palabra en línea. El problema surge cuando diferentes países tienen diferentes formas de tratar contenidos inadecuados en línea y el ámbito de la libertad de palabra en línea difiere entre jurisdicciones. A pesar de estas diferencias, hay un acuerdo universal en un área,

a saber, la necesidad de fortalecer la protección de la infancia en línea y perseguir los contenidos en línea de carácter abusivo y discriminatorio dirigidos a la explotación de la infancia por quienes tienen intereses creados en este asunto.

Otro asunto analizado anteriormente en este documento se refiere a la capacidad de comunicación libre y anónima en Internet. Como ya se ha dicho, algunas personas creen que el anonimato de Internet les permite decir lo que quieran en línea, sin preocuparse de su potenciales efectos sobre otras personas.[157]. A menudo, la víctima de una presunta difamación en línea presenta una demanda contra un acusado "Juan García" (nombre ficticio utilizado cuando no se conoce al autor).

Diferentes países tienen leyes diferentes contra la difamación que hacen referencia a diversos tipos de discursos o contenidos difamatorios. Estas leyes también son aplicables en el ciberespacio. En este sentido, la nueva jurisprudencia que se está generando es cada vez más clara en el sentido de que nadie tiene derecho a difamar a otra persona o a tratar de dañar la reputación de los demás.

En relación con este asunto, las disposiciones de las leyes nacionales varían de un país a otro. Algunos países sólo restringen el acceso a Internet cuando consideran que está justificado para proteger los valores morales, los derechos personales respaldados jurídicamente, la defensa nacional o la seguridad del Estado. Otros han reconocido formalmente que el derecho a la libertad de expresión se extiende al ciberespacio, o están considerando dar ese paso.

Actualmente vivimos una época de transición en la historia de la humanidad en la que la libertad en Internet está amenazada no sólo por órganos del Estado, sino también por agentes privados que realmente son los que gestionan y controlan los datos en Internet.

---

157 Eric Sinrod, *"Freedom of anonymous online speech has potential limits"* http://www.lexology.com/library/detail.aspx?g=7a8eb382-b007-49c6-8ca1-4a9197062d9d, última actualización 8 de agosto de 2014.

Otros desafíos que afectan a la libertad en Internet

La jurisdicción aplicable en Internet es un tema importante que se complica por el hecho de que la libertad de expresión de una persona en Internet puede restringirse dentro de los límites territoriales de un país, mientras que la persona pueda estar físicamente en la jurisdicción de otro país. Además, el hecho de que todos seamos sistemáticamente objetivo de ciberdelincuentes también puede contribuir a no poder disfrutar de las libertades en Internet. Por tanto, la ciberdelincuencia se ha convertido en un importante asunto de carácter jurídico, político y reglamentario que potencialmente puede afectar a la libertad en Internet de usuarios de todo el mundo.

Otra de las cuestiones que afectan la libertad en Internet se refiere a la ciberseguridad. Una persona sólo puede disfrutar de su libertad jurídica en Internet si ésta es segura, está protegida y es confiable. Sin embargo, las violaciones de la ciberseguridad han traído de nuevo al primer plano los distintos desafíos a que se enfrenta la protección y preservación de los recursos e infraestructuras electrónicas.

Dada la importancia global y las vulnerabilidades del medio cibernético, las libertades en Internet tendrán que ser contempladas en su conjunto desde una perspectiva diferente. El recrudecimiento de los ciberataques a sistemas y redes de computadoras de varios países, obliga a equilibrar la libertad en Internet con la necesidad de proteger y preservar la ciberseguridad.

Aún no hay unanimidad a nivel mundial sobre cómo hacer frente a la responsabilidad de los intermediarios. Algunos países como los Estados Unidos de América tienden a no atribuir tal responsabilidad a los proveedores de servicios. Otros obligan en ocasiones a los intermediarios a ejercer una debida diligencia cuando desean eludir la responsabilidad derivada de la posible responsabilidad por datos en línea de terceros, al tiempo que les liberan de obligaciones respecto a ciertas disposiciones básicas del régimen jurídico nacional.

La aparición de 'redes oscuras' es otro reto formidable para la libertad en Internet. Los ciberdelincuentes no dudan en acceder a estos dominios para llevar a cabo sus planes y actividades maliciosas dirigidas a perjudicar las libertades de las personas en Internet.

Otro desafío importante a la confianza en el uso del ciberespacio y las libertades en Internet es el creciente fenómeno de la ciberguerra, que actualmente es un secreto a voces. La aparición del ciberterrorismo afecta en la práctica al disfrute de las libertades en Internet.

Claramente, existe la necesidad de un entendimiento y unos principios comunes a nivel internacional sobre la libertad en Internet. Se han realizado grandes esfuerzos en relación con importantes cuestiones jurídicas y políticas antes mencionadas que afectan a la libertad en Internet. En este contexto, organizaciones como la Federación Mundial de Científicos y la Unión Internacional de Telecomunicaciones pueden seguir desempeñando un importante papel para contribuir a un consenso en continua evolución sobre este asunto.

Big Data

En la coyuntura actual, el impacto del *Big Data* sobre la libertad en Internet no debe ser ignorado ya que, en última instancia, la libertad debe contemplarse en el contexto de datos e información electrónica. Hoy en día, Internet es una red de redes gigantesca, un enorme dragón de datos con memoria infinita. Por tanto, debe considerarse que la libertad en Internet en todas sus formas tiene una conexión, asociación y relación directa con el *Big Data*.

El *Big Data* es la gran realidad de nuestro tiempo. Con tantos datos generados por diferentes sistemas y redes informáticas, es natural que las empresas deseen realizar la analítica de los datos. Diferentes grupos de interés definen el *Big Data* de distinta manera y es, sin duda, un asunto muy importante desde las perspectivas jurídica, política y reglamentaria.

Definición de *Big Data*

La **Wikipedia** define el *Big Data* de la siguiente manera: "[...] un término de amplio alcance para cualquier conjunto de datos tan grandes y complejos que resulta difícil procesarlos mediante herramientas de gestión de datos normalmente disponibles o aplicaciones de procesamiento de datos tradicionales. Por lo general, el *Big Data* incluye conjuntos de datos de un tamaño que supera la capacidad de las herramientas de software de uso común para poder ser recopilados, conservados, administrados y procesados en un plazo de tiempo admisible".[158] El **Diccionario Oxford** define el *Big Data* como conjuntos de datos demasiado grandes y complejos para ser manipulados o consultados con métodos o herramientas de uso común[159]. El **informe de la Casa Blanca sobre el *Big Data*** publicado el 1 de mayo de 2014 se hace eco de la definición ampliamente aceptada de que *Big Data* "[...] es tan grande en volumen,

158 http://en.wikipedia.org/wiki/Big_data

159 http://www.oxforddictionaries.com/definition/english/big-data

diverso en variedad y con una evolución a tal velocidad que los métodos de captura de datos de uso común resultan insuficientes".[160] La **Tech America Foundation** afirma que "el *Big Data* es un término que describe grandes volúmenes de datos de alta velocidad, complejos y variables que requieren técnicas y tecnologías avanzadas para la recopilación, almacenamiento, distribución, gestión y análisis de la información."[161]

Las características del *Big Data* incluyen:

- Debe ser elástico por naturaleza[162].
- Muchos sistemas de *Big Data* acumulan datos no revisados, por lo que siempre existen datos atípicos con valores extremos, lo que genera "puntos calientes" en el sistema.
- El *Big Data* puede dotarse rápidamente de los ciclos de computación [capacidad] necesarios gracias a la "infraestructura como servicio" (IaaS) basada en la nube[163].
- En este contexto, es muy importante la cantidad de datos generados. Es el volumen de datos lo que determina su valor y potencial, y si puede o no considerarse realmente *Big Data*.
- Variedad hace referencia a la complejidad de gestionar múltiples tipos de datos, incluyendo datos estructurados, semiestructurados y no estructurados.
- Velocidad se refiere a la velocidad a la que se crean, procesan y analizan los datos, un factor que continúa acelerándose. La característica de creación de datos en tiempo real y la necesidad de incorporar flujos de datos (*streaming*) en los procesos de negocio y en la toma de decisiones contribuyen a aumentar la velocidad.
- Incertidumbre de los datos: la veracidad se refiere al nivel de fiabilidad asociada a ciertos tipos de datos[164].

---

160 http://www.lexology.com/library/detail.aspx?g=e7161021-7570-476c-bf8a-b4637d10a355

161 TechAmerica Foundation, Demystifying Big Data: A Practical Guide to Transforming the Business of Government 2012, https://www-304.ibm.com/industries/publicsector/fileserve?contentid=239170, última actualización 4 de agosto de 2014.

162 http://hadoopblog.blogspot.in/2012/02/salient-features-for-bigdata-benchmark.html

163 http://www.dummies.com/how-to/content/characteristics-of-big-data-analysis.html

Existen numerosas preocupaciones de naturaleza jurídica, política y reglamentaria en relación con el *Big Data*. En primer lugar, y más importante, cabe señalar que no existe un marco internacional, ni tratados internacionales, que aborden el *Big Data*. El *Big Data* sigue estando regulado por legislaciones nacionales. La mayoría de los países no cuentan con legislaciones o disposiciones jurídicas específicas al respecto. No obstante, en relación con los marcos políticos y reglamentarios es imprescindible tener en cuenta una serie de parámetros importantes que se mencionan a continuación.

La protección de datos es uno de los mayores desafíos del *Big Data*. Las distintas jurisdicciones nacionales tienen diferentes requisitos reglamentarios para la protección de los datos. La Unión Europea ha desarrollado directivas para la protección de datos y países de otras regiones han incorporado en sus respectivas legislaciones nacionales diversas disposiciones de protección de datos. Los métodos de recopilación, protección y conservación de datos son aspectos importantes. La protección del *Big Data* requiere una revisión específica de la legislación de protección de datos ya que ésta se ha enmarcado hasta la fecha en el contexto de las cantidades de datos relativamente pequeñas generadas por individuos, minúsculas en comparación con los volúmenes del *Big Data*.

La protección del *Big Data* se enfrenta a enormes desafíos, tanto para quienes los procesan como para los reguladores. El volumen masivo y la arquitectura de referencia, así como la diversidad de orígenes de los datos, exige un marco legal seguro y protegido específico en defensa de usuarios y proveedores de datos.

La minimización de datos también plantea problemas de privacidad y de protección de datos. Es de especial relevancia la necesidad de desarrollar prácticas internacionales idóneas para la recopilación, retención y destrucción de los datos, incluidos datos personales que residen en un forma tal que permite la identificación de las personas.

Las legislaciones nacionales difieren en relación con los requisitos del consentimiento para la recopilación, uso o revelación de datos y el control individual de los mismos. Como ya se ha señalado, no existen disposiciones jurídicas internacionales sobre el *Big Data* en relación con este y otros asuntos relacionados con el ciberespacio.

---

164 IBM, Analytics: The real-world use of Big Data – How innovative enterprises extract value from uncertain data, http://www.ibm.com/smarterplanet/global/files/se__sv_se__intelligence__Analytics_-_The_real-world_use_of_big_data.pdf última actualización 8 de agosto de 2014.

Otra cuestión jurídica es la relacionada con el anonimato de los datos y el enmascaramiento de los datos personales de quienes que ponen información en Internet. Una cuestión importante que no ha sido adecuadamente abordada se refiere a los principios básicos que deben aplicarse a la recopilación, procesamiento, conservación y divulgación del *Big Data*. Dado que actualmente el *Big Data* reside en la nube, su protección y preservación presentan desafíos adicionales desde los puntos de vista jurídico, político y regulatorio.

La privacidad de los datos es un importante aspecto del *Big Data* debido a los grandes volúmenes de datos que se consumen, y por el hecho de que cada proveedor de datos tiene un derecho intrínseco a la protección y preservación de sus datos. Por tanto, la responsabilidad de garantizar una adecuada protección de los datos recae directamente en el servicio de red.

La jurisdicción sobre el *Big Data* es también un asunto importante desde los puntos de vista jurídico, político y regulatorio ya que los datos se alojan sistemáticamente en la nube y en servidores ubicados en diferentes partes del mundo. Cuando se viola la privacidad del *Big Data*, la persona afectada debe emprender acciones legales contra los correspondientes proveedores de servicio. El primer gran reto es identificar la ubicación física de dichos datos, ya que la ubicación del servidor en el que se produjo la infracción afecta a las leyes locales aplicables a la violación de la privacidad.

La ciberdelincuencia relacionada con el *Big Data* constituye asimismo un desafío jurídico significativo ya que el conjunto de la economía de Internet se basa en los datos, y la violación de la privacidad en el *Big Data* es un arma muy importantes para los ciberdelincuentes, por lo que probablemente el *Big Data* sea cada vez más uno de sus principales objetivos.

En octubre de 2013, Adobe informó de un acceso ilegal de ciberdelincuentes a su red, de donde robaron más de 2,9 millones de nombres de usuarios, números cifrados de tarjetas de crédito y de débito, fechas de caducidad de las tarjetas, identificaciones de acceso y contraseñas. También accedieron al código fuente de Adobe para varios productos, incluido Acrobat y ColdFusion[165].

---

165 http://blogs.mcafee.com/consumer/consumer-threat-notices/malicious-acrobatics-adobe-the-latest-target-in-string-of-cyber-attacks

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA), órgano consultivo de la Unión Europea, declaró en enero de 2013 que "La explotación del *Big Data* afectará a la privacidad de los datos. Al mismo tiempo, la explotación del *Big Data* por parte de adversarios podría abrir las puertas a un nuevo tipo de vectores de ataque".[166] ENISA añadió que el *Big Data* es la agregación de información generada "[...] como consecuencia de la proliferación de tecnologías de redes sociales, computación en la red, computación móvil y por el uso de Internet en general", y que se ha convertido en un nuevo asunto en la esfera de la seguridad.

Privacidad

La analítica del *Big Data* podría tener un efecto directo en la violación de la privacidad personal. En mayo de 2014, la Casa Blanca publicó su esperado Informe sobre el *Big Data*: "*Big Data: Seizing Opportunities, Preserving Values*". El Informe había sido solicitado por el presidente Barack Obama y aborda las diversas formas en que los rápidos avances tecnológicos permiten a gobiernos y al sector privado recopilar, almacenar, analizar y utilizar grandes cantidades de datos (*Big Data*). El Informe destaca las potenciales amenazas a la privacidad individual y a la igualdad que podrían derivarse del *Big Data* ahora y en el futuro, y aboga por iniciativas jurídicas, políticas y reglamentarias para la protección de los ciudadanos de los Estados Unidos de América y de todo el mundo frente a posibles abusos.[167]

El *Big Data* y la privacidad de los datos están adquiriendo una importancia cada vez mayor en la esfera jurídica. A menudo existen discrepancias sobre quién es el propietario del *Big Data*, particularmente cuando en el desarrollo de los sistemas en que se basa el *Big Data* han participado terceros. Otra preocupación importante es la protección de los datos, incluida la información personal sensible, mediante técnicas criptográficas y un control granular del acceso.

---

166 http://www.out-law.com/en/articles/2013/january/cloud-mobile-social-and-big-data-technology-innovations-increasing-threat-of-cyber-attacks-says-eu-body/

167 Kenneth R. Florin , Ieuan Jolly et. al "White House "Big Data" report highlights benefits and potential for abuses from Big Data" http://www.lexology.com/library/detail.aspx?g=a036aed0-cffb-4ae1-a518-44b92201effb, última actualización 4 de agosto de 2014.

La recuperación [de datos] y el acceso al *Big Data* también tienen una relación intrínseca con la privacidad, y son cuestiones jurídicas básicas para preservar los datos sujetos a procesos de minería de datos y la analítica de los mismos. El mantenimiento de la autenticidad, la integridad y la veracidad del *Big Data* accedido y recuperado es de interés primordial.

Además, la seguridad centrada en los datos y criptográficamente reforzada plantea cuestiones jurídicas específicas. Un control de acceso granular conlleva otros complejos aspectos de carácter jurídico y político relacionados con la privacidad. Finalmente, también es necesario salvaguardar la privacidad durante la difusión de la información.

Otra preocupación relacionada con el *Big Data* es que una vez recopilados los datos, puede ser muy difícil preservar el anonimato. Si bien están en marcha proyectos de investigación prometedores cuyo objetivo es ocultar información de identificación personal en grandes conjuntos de datos, actualmente se están realizando otros estudios mucho más avanzados para volver a identificar datos aparentemente "anónimos". La inversión total en capacidad para unificar o fusionar datos es muchas veces mayor que la dedicada a tecnologías para mejorar la privacidad.[168]. Una de las principales preocupaciones existentes es garantizar la autenticidad, integridad y veracidad del *Big Data* accedido y recuperado.

Otras cuestiones jurídicas están relacionadas con la seguridad de la infraestructura del *Big Data* de forma que se disponga de un marco jurídico adecuado para proteger los tratamientos de datos realizados en estructuras de programación distribuida. En este sentido, deben definirse prácticas idóneas para cumplir y mantener la seguridad de los repositorios de datos no relacionales. Otro aspecto jurídico importante se refiere a la gestión de los datos. En este sentido, se necesitan marcos jurídicos adecuados para la seguridad del almacenamiento de los datos y de los registros de transacciones, así como auditorías granulares.

---

168 Oficina Ejecutiva del Presidente, *Big Data: Seizing Opportunities, Preserving Values,* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf, última actualización 4 de agosto de 2014.

Los derechos de propiedad intelectual relacionados con el *Big Data* constituyen una cuestión jurídica adicional importante. ¿Quién tiene los derechos de propiedad intelectual del *Big Data*? ¿Cuáles son los derechos de propiedad intelectual relacionados con la recopilación, almacenamiento, procesamiento o uso compartido del *Big Data*? A menudo preocupa que las nuevas herramientas de búsqueda y análisis del *Big Data* puedan violar los derechos de autor de los datos. Otras preocupaciones son la determinación de la responsabilidad de las partes contratantes por una información inexacta o incompleta o el incumplimiento de acuerdos contractuales.

También es posible que la tecnología permita el acceso no autorizado a información sobre empresas competidoras, lo que genera cuestiones en el ámbito del derecho de la competencia. El hecho de que la rentabilidad del *Big Data* dependa de secretos comerciales y de datos personales sensibles afecta a la privacidad y la seguridad, y erosiona la confianza en el uso de ciberplataformas y tecnologías.

Se ha argumentado que la recopilación y procesamiento del *Big Data* influye en las identidades individuales y colectivas de los pueblos, lo que tiene un riesgo de erosión de la calidad de la democracia.

Una preocupación adicional está relacionada con el hecho de que muchos de los censores del *Big Data* son en su mayoría intermediarios poderosos, lo que aumenta el riesgo de que éstos actúen de manera indebida y abusiva para violar derechos y libertades individuales.

En resumen, es necesario disponer de un marco jurídico habilitador que asegure que el *Big Data* no perjudica en absoluto al ejercicio de los derechos de los ciudadanos ni al cumplimiento de sus obligaciones y deberes cívicos.

Papel de la Federación Mundial de Científicos y de la UIT

Dada la ausencia de parámetros internacionales relativos a marcos jurídicos y políticos para el *Big Data*, es imperativo que organizaciones como la Federación Mundial de Científicos y la Unión Internacional de Telecomunicaciones persistan en sus esfuerzos para su desarrollo.

Conclusión

En conclusión, puede afirmarse que tanto las libertades en Internet como el *Big Data* son conceptos fascinantes y en continua evolución que desempeñan un papel cada vez más importante en nuestra vida cotidiana. Por tanto, es de capital importancia desarrollar y poner en práctica marcos jurídicos, políticos y reglamentarios internacionales para preservar las libertades en Internet. Está en juego el futuro de las

estructuras de la era digital que tanto nos sirven y que condicionan nuestro crecimiento de formas muy diversas.

Existe una importante tarea pendiente de formulación y puesta en práctica de marcos políticos y reglamentarios internacionales basados en principios universalmente aceptados.

Estos marcos necesariamente evolucionarán con el tiempo. Se está generando una amplia jurisprudencia sobre las libertades en Internet y el *Big Data*. Sin embargo, es imperativo realizar los esfuerzos necesarios para asegurar que se elaboren marcos políticos y reglamentarios eficaces a nivel internacional. ¡

El Panel Permanente de Supervisión sobre la Seguridad de la Información de la Federación Mundial de Científicos puede jugar un papel extraordinariamente importante a este respecto, no sólo en lo que a capacidad de supervisión se refiere, sino también por su contribución al desarrollo de dichos marcos internacionales. Se espera que la Federación Mundial y otros organismos pertinentes realicen, junto con la Unión Internacional de Telecomunicaciones, contribuciones significativas a ese objetivo acordes con su experiencia y conocimientos de esta materia. La ayuda de estas organizaciones para el desarrollo de principios que conformen un común denominador universalmente aceptado y que garanticen un entorno adecuado en el ciberespacio, tendría un gran valor para todas las partes interesadas.

Tal como se ha mencionado, está en juego la capacidad de que todos los usuarios sigan disfrutando de los beneficios de las libertades en Internet mediante la superación de los desafíos a la ciberseguridad y otros aspectos que puedan erosionar la confianza en este universo en expansión y cada vez más esencial.

Debemos confiar en que se generará la jurisprudencia pertinente conforme aumente el número de usuarios de Internet y se acelere el avance de la cibertecnología. Sólo mediante un seguimiento constante del desarrollo de la jurisprudencia y contribuyendo al progreso en este campo, será posible para el mundo en sentido amplio, y específicamente para los actores clave, definir el camino a seguir.

El proceso de desarrollo de marcos jurídicos, políticos y reglamentarios para el *Big Data* y la libertad en Internet evolucionará con el tiempo. Un prerrequisito importante para el éxito será la extensión del respeto a los derechos fundamentales a todo el ámbito del ciberespacio.

3.3 Una perspectiva global de la vigilancia del Estado en el ciberespacio

por Howard Schmidt

Introducción

A fin de entender cabalmente y ofrecer una opinión fundada sobre la vigilancia en el ciberespacio, es importante, en primer lugar, entender que el marco de referencia está en gran medida basado en un entorno cuyas reglas de participación (escritas o no) han evolucionado con el tiempo, particularmente durante el periodo que precede a la aparición del ciberespacio.

Por cada opinión personal que considera que la vigilancia está justificada, siempre es posible encontrar una opinión en sentido contrario, así como un gran número de partes interesadas que en relación a este asunto se sitúan en una zona gris. Sólo mediante el análisis empírico de la información y una perspectiva global será posible definir un conjunto equilibrado de directrices que puedan ser aceptadas por todas las partes interesadas a la hora de determinar si la vigilancia por parte del Estado es apropiada y está justificada.

Recopilación de datos

El desarrollo tecnológico ha creado un entorno en el que grandes cantidades de datos se crean, transmiten y recopilan para diversos fines. Todo lo producido en el ciberespacio se basa en datos cuya captura es esencial, como también lo es su adecuada recopilación. Las transacciones financieras son ejemplos de datos esenciales que deben ser capturados y recopilados. Considérese, por ejemplo, los actuales pagos mediante cheques. Muchos de nosotros recibimos nuestro salario en forma de transferencia electrónica de fondos que se depositan en nuestras cuentas, y también muchos de nosotros recopilamos y archivamos estos datos electrónicos en una cuenta de ahorro. Los datos archivados pueden moverse a otro punto de recopilación en forma de transacción (por ejemplo, a una tienda de comestibles), donde se intercambian bienes por datos que representan un instrumento financiero.

Otro ejemplo de datos recopilados de forma similar son las llamadas móviles, en las que la empresa de telefonía móvil conoce a quien se hizo la llamada, dónde se hizo y su duración. Todo ello con fines de facturación, tal como la compañía telefónica explica a los consumidores. Los sitios web recopilan datos de los usuarios y de los servicios utilizados por éstos para diversos fines, algunos de los cuales incluyen el

establecimiento y mantenimiento de las preferencias del usuario y el archivo de información creada por el propio usuario (por ejemplo, el sitio web de una red social).

Como ciudadanos en el ciberespacio, todos entendemos y aceptamos que existen circunstancias en las que la recopilación de datos no sólo es razonable y aceptable, sino también en muchos casos deseable. Lo que determina que las partes interesadas admitan la recopilación de datos es su entendimiento claro de qué datos se recopilan y con qué propósito. En tales casos, el usuario o bien acepta los términos que acompañan a la recopilación de datos antes de participar en ella, o decide no hacerlo si considera que las políticas de recopilación y uso de los datos le son excesivamente onerosas.

Básicamente, como parte interesada el ciudadano acepta un contrato con quienes tienen acceso a sus datos, contrato que articula cómo pueden recopilarse y utilizarse los datos, quién tiene la custodia de los mismos (por ejemplo, la empresa de telefonía móvil), y en qué medida este último puede transferir la custodia, y a quién. Los custodios de datos tienen un enorme poder con respecto a los mismos, pero este poder no les permite hacer lo que deseen con ellos. En última instancia, si un custodio desea utilizar los datos al margen del acuerdo con la persona u organización a la que están ligados, debe alcanzar un nuevo acuerdo que permita ese uso ampliado. No hacerlo puede interpretarse razonablemente como un abuso de autoridad o una violación de la confianza.

Proceso judicial frente a recopilación de información de inteligencia

Por las razones mencionadas, actualmente existen procedimientos que permiten el uso ampliado de los datos más allá de las expectativas iniciales de las partes interesadas. Si hay una sospecha razonable de que alguien está involucrado en una actividad delictiva, los procedimientos jurídicos y judiciales permiten supervisar y acceder a los datos recopilados, que pueden utilizarse como prueba del delito. Las normas y procedimientos asociados a este tipo de vigilancia varían entre países, aunque la población suele tener por lo general acceso a las normas que rigen el proceso.

La cuestión se torna un tanto difusa cuando son las agencias de inteligencia del gobierno quienes realizan la vigilancia. A nivel global, las agencias de inteligencia supervisan y recopilan datos de forma encubierta, y utilizan la información para diversos fines. La mayoría de las agencias afirman que la información de inteligencia se recopila por razones de seguridad nacional (por ejemplo, el caso de las recientes revelaciones de la NSA), o por un bien mayor. Otras simplemente afirman que su autoridad soberana les permite hacerlo y que no tienen que explicar por qué recopilan información de inteligencia. La cuestión deviene especialmente compleja en una

economía global en la que dos o más naciones tienen posiciones distintas sobre dichas actividades de recopilación de datos. En tales casos, aunque los ciberciudadanos pueden creer que gozan de un nivel de confidencialidad según las normas de su gobierno, los datos pueden cruzar fronteras nacionales en su transmisión por el ciberespacio desde el origen hasta el destino. Una vez que los datos llegan a un lugar donde las reglas son otras, quedan sujetos a las mismas. Dado que la recopilación de información de inteligencia es un proceso inaccesible que normalmente no está sujeto a la transparencia que exige el cumplimiento de la ley y los procedimientos judiciales, es muy difícil determinar cuándo se ha cruzado una línea.

Métodos y normas para la recopilación de información de inteligencia

Cuando se permite la recopilación de información de inteligencia al margen de un procedimiento jurídico o judicial (y en muchos casos así ocurre), es importante tener en cuenta la utilización de programas maliciosos y de aplicaciones instaladas de forma oculta por comunidades que recopilan información de inteligencia. En muchos Estados soberanos, la creación de software malicioso y de aplicaciones destinadas a infiltrarse en los sistemas informáticos a través de diversos métodos de propagación es, en sí misma, una actividad ilegal grave. Cualquier actividad en la que participe el software malicioso una vez que se ha propagado, se considera un delito del creador del software, como también lo comete un usuario u organización que propague a sabiendas software malicioso. Existen procesos jurídicos y judiciales establecidos en todo el mundo que rigen en estos supuestos de violación de la ley, con castigos que pueden llegar a ser muy graves.

Una vez más, al considerar cómo operan las organizaciones patrocinadas por el Estado que recopilan información de inteligencia, las normas relacionadas con la participación en la creación y propagación de software malicioso, de aplicaciones encubiertas y de recopilación de datos mediante este tipo de "herramientas", son muy difusas. En función del Estado soberano de que se trate, existen razones muy diversas que pueden justificar que una organización de inteligencia del gobierno participe en dichas actividades, siendo quizás el motivo más frecuente la seguridad nacional. Sin embargo, es importante señalar que una vez instalado el software malicioso éste puede (y a menudo ocurre) propagarse más allá de los límites previstos, y afectar negativamente a sistemas que a todos los efectos se consideran fuera de los límites de actuación de la agencia de recopilación de información de inteligencia. Un ejemplo de ello serían los sistemas críticos, como las redes de hospitales, las redes de energía, y los sistemas de seguridad que controlan procesos peligrosos (como la producción de sustancias químicas). Además, los sistemas financieros, los sistemas de producción de alimentos y los sistemas de fabricación en general pueden sufrir efectos negativos que creen malestar social y pánico a gran escala.

Nivelación del escenario de utilización de ciberarmas

El uso del software malicioso, como aquí se describe, puede considerarse equivalente al lanzamiento de un arma cibernética, en el entendido que el arma puede tener un efecto muy superior al objetivo previsto. Además, la capacidad de crear y desplegar ciberarmas no está condicionada por limitaciones de los recursos económicos y naturales típicos de los conflictos físicos tradicionales. La disponibilidad de metales, instalaciones químicas o herramientas de alta tecnología, tiene un efecto muy escaso sobre la capacidad de los creadores de software malicioso. Un ordenador y una conexión de red, o un medio de almacenamiento externo y transportable (por ejemplo, un lápiz de memoria USB), es más que suficiente, junto con el conocimiento de cómo crear el software malicioso.

Una vez que el software malicioso se ha creado y propagado, puede convertirse en un arma y ser utilizado por cualquier persona u organización que lo identifique y aísle. Una consecuencia de ello es que la ciberarma puede volverse en contra de la organización que ha iniciado su propagación, por ejemplo, en forma de una versión mutada con funcionalidades más poderosas que las del software malicioso original. En tales casos, la organización que introdujo el software malicioso actúa como proveedor global de la ciberarma. Esto significa efectivamente que, más allá de la ventaja de ser el primero en golpear, la situación de las partes se nivela no mucho después de la puesta en marcha inicial, algo que puede desembocar en un entorno altamente destructivo, donde ninguna persona u organización puede estar segura. Por otra parte, una vez que se despliegan las ciberarmas, éstas existen para siempre y no hay existencias que eliminar.

El camino a seguir

Es lógico pensar que con independencia de las intenciones de quienes llevan a cabo la vigilancia subrepticia patrocinada por el Estado, se generan situaciones que pueden tener repercusiones negativas incontrolables e imprevisibles. Esto puede tener un efecto dominó que desestabilice las relaciones globales y el entorno económico. Si bien Internet puede permitir realizar una vigilancia efectiva que algunos pueden considerar realizada con buenas intenciones, es importante entender que Internet se ha convertido en parte integral y necesaria de la economía mundial, que permite a individuos, organizaciones y naciones de todos los tamaños participar como iguales. También permite el libre intercambio de ideas de forma instantánea, y la colaboración a todos los niveles de la cadena de valor.

Por tanto, es importante que la comunidad empresarial presione a escala mundial y desde todos los niveles a los gobiernos de todo el mundo para que aprueben las leyes pertinentes. Esas leyes deben servir para evitar efectos disruptivos en los beneficios económicos y sociales obtenidos gracias a Internet. También deben permitir un aumento continuo del número de individuos, organizaciones y naciones que puedan participar en una economía colaborativa alimentada por una Internet estable, donde todo el mundo siga confiando en que los intereses de los gobiernos no se anteponen a los de las personas a las que sirven.

3.4 Alcance de la vigilancia del Estado en el ciberespacio: perspectiva de la Unión Europea

por Henning Wegener

La inherente y creciente tensión entre la libertad y la integridad de Internet (y de la comunicación digital en general) y, por otro lado, los requisitos cada vez más urgentes derivados de la preocupación por el orden público y la seguridad colectiva, se reflejan extensamente en varios apartados de esta publicación, particularmente en el ensayo de Prof. Al Achkar sobre las libertades en Internet y las libertades civiles en la red.

La evidencia de que actualmente se producen intrusiones masivas en dispositivos y redes digitales y la preocupación entorno al *Big Data*, hacen que esta tensión esté más que nunca en primer plano de una sensación popular y generalizada de ansiedad en Europa. El extraordinario crecimiento de las posibilidades técnicas de recopilación y gestión de datos, que arrastran a la humanidad a una era de pérdida de privacidad, ha acrecentado el temor de que los principios del derecho nacional e internacional y los valores individuales y colectivos estén en grave peligro. Las cada vez más numerosas violaciones de los derechos humanos básicos se ha convertido en un asunto global y existe el clamor por una actuación a nivel mundial para que se definan normas y se pongan límites a esta ola aparentemente imparable.

Un primer paso importante en el establecimiento de las políticas necesarias ha sido la Resolución A/RES/68/167 de la Asamblea General de las Naciones Unidas, adoptada sin votación el 18 de diciembre de 2013, "El derecho a la privacidad en la era digital", que expresa la voluntad de la comunidad internacional de tomar las medidas necesarias contra la vigilancia, interceptación y recopilación a gran escala de datos personales. Para el cumplimiento operativo del párrafo 5 de esa Resolución, la Alta Comisionada de las Naciones Unidas para los Derechos Humanos remitió en junio de 2014 un Informe (A/HRC/27/37) que ha sido objeto de un debate de expertos en el 27º Periodo de Sesiones del Consejo de Derechos Humanos y que está previsto que se

traslade al 69º Periodo de Sesiones de la Asamblea General de las Naciones Unidas para que las "opiniones y recomendaciones" del mismo sean tenidas en cuenta por los Estados Miembros. El Informe establece inequívocamente los requisitos relacionados con los derechos humanos que deben cumplir las medidas de vigilancia de los Estados: deben ser necesarias y proporcionadas, transparentes y respetuosas con el derecho a la privacidad de las personas en el extranjero. El Relator del Informe deja ver claramente que no considera que estos requisitos se cumplan actualmente.

A la espera de resultados concretos de estos procesos globales, y a pesar de las necesidades y enfoques de ámbito mundial, existen diferencias regionales sobre la forma en que naciones y comunidades reaccionan a las revelaciones y realidades de injerencias en la privacidad digital, la soberanía nacional y los dominios de información protegida (en un amplio debate público provocado por el caso Snowden).

En algunas partes del mundo, hay más resignación que revolución, e incluso indiferencia; en muchos de los países más grandes, los sistemas políticos imperantes silencian las voces públicas de rechazo; en los Estados Unidos de América hay una comprensión notablemente mayor de las necesidades de seguridad pública, supuestas o reales, y se cuenta con el apoyo de un sistema legal más indulgente. Por el contrario, en Europa, y sobre todo en la Unión Europea, las revelaciones y la gran dimensión de los robos de datos han causado una tormenta de consternación y rechazo. Se ha generado un movimiento político de fondo que sería irresponsable subestimar, menos aún en sus dimensiones trasatlánticas, de pérdida de confianza o por decirlo así, de ciberconfianza. Sin duda, la perenne relación entre las democracias europeas y los Estados Unidos de América, en la que subyace una fuerte componente emocional, ha quedado afectada.

Este sentimiento colectivo en Europa refleja su ferviente deseo de libertad y privacidad, algo muy amplificado por su historia reciente marcada por dictaduras y su negación de la privacidad personal (algo que sigue muy vivo en la memoria), sino también por su estado altamente desarrollado de protección de datos y de libertades civiles, y por la naturaleza misma de la Unión Europea como entidad jurídica. El temor a un todopoderoso Gran Hermano, un Leviatán inasequible a ninguna ley, está mucho más presente en Europa que en otras partes, aunque sería un error subestimar la consternación colectiva de los estadounidenses como consecuencia de la vigilancia masiva de su gobierno. Es probable que esta controversia desempeñe un papel central en las próximas elecciones presidenciales.

Sin embargo, si se desean definir criterios globales para mantener la ciberconfianza en una época en la que es posible disponer de medios técnicos ilimitados para la intrusión, resulta recomendable echar una mirada a la situación en la Unión Europea y a su entorno jurídico, ya que puede ayudar a establecer un importante pilar para un marco reglamentario universal.

Una razón de ello es que la Unión Europea constituye una comunidad de derecho compuesta por 28 naciones altamente industrializadas que desempeñan un papel relevante en la economía digital mundial, y donde las tecnologías digitales son, mucho más que en ningún otro lugar, el paradigma de la economía y la sociedad; actualmente la Unión Europea es el mayor bloque económico del mundo. Esto hace que los países miembros estén proporcionalmente más amenazados por ciberataques que muchos otros; por ejemplo, según un estudio de la empresa McAfee, Alemania tiene una tasa de daños producidos por ciberataques del 1,65 por ciento de su producto interior bruto, un récord entre los países industrializados En un momento en que las bandas de ciberdelincuentes son la principal causa de daños a economías muy dependientes de la red, economías abiertas, y donde los servicios de espionaje extranjeros campan a sus anchas, la ciberdelincuencia se ha convertido en una triste realidad en Europa. Por este motivo, la Unión Europea ha desarrollado un sistema de ciberseguridad colectiva y uniforme muy avanzado.

La Unión Europea no sólo es la unión de 28 Estados soberanos sino que, además, es una organización con instituciones comunes y capacidad normativa. La mayoría de los actos legislativos son el resultado de la acción conjunta del Consejo Europeo (a propuesta de la Comisión Europea) y del Parlamento Europeo. De conformidad con las Directivas sobre la aplicación de los objetivos acordados, las Resoluciones y las Decisiones son vinculantes en todas sus partes y de forma inmediata para todos los Estados Miembros. Dichas Resoluciones y Decisiones deben ser traspuestas a la legislación nacional de los Estados Miembros, una característica singular en el sistema internacional. La base institucional común de la legislación europea no sólo tiene efectos jurídicos inmediatos en los Estados Miembros, sino que ejerce una notable influencia fuera del territorio europeo. Por tanto, la Unión Europea puede ser un ejemplo a emular por otros, a modo de laboratorio institucional donde un grupo numeroso de naciones ponen a prueba lo que también puede implementarse en el conjunto de la comunidad de naciones. La legislación de la Unión Europea es un instrumento poderoso de coordinación y armonización interna y marca el camino hacia la reglamentación internacional.

Tanto la ciberseguridad como las políticas destinadas a garantizar la protección de datos personales son competencia de los órganos europeos. La Comisión Europea ha estado trabajando durante más de una década en un marco regulatorio relativo a la ciberseguridad para todos sus Estados Miembros. Un conjunto de importantes documentos, en parte de carácter analítico y en parte prescriptivos, componen un amplio cuerpo legal de obligado cumplimiento para los Estados Miembros de la Unión Europea, que en su alcance y detalle no tiene igual en el mundo digital de las naciones, excepto en los Estados unidos de América. Además, en 2004 los 28 Estados Miembros crearon la Agencia Europea de Seguridad de Redes y de la Información (ENISA) a modo de comité asesor conjunto para coordinar importantes actividades colectivas de la Unión Europea y estimular la acción regulatoria. También cabe mencionar el Centro europeo de lucha contra la ciberdelincuencia, adscrito a EUROPOL, y un equipo de intervención en caso de emergencia informática (CERT) de alcance europeo como punto principal de contacto y actuación en caso de ciberataques. Sería excesivamente prolijo describir toda la gama de actividades sobre ciberseguridad de la Unión Europea, en sus dimensiones legal e institucional, no obstante puede obtenerse fácilmente una visión general consultando la página web de ENISA, y diversos análisis disponibles.[169]. La Unión Europea está firmemente comprometida con su Agenda Digital y la optimización de la ciberseguridad. Dos documentos recientes, muy completos y que incorporan normas anteriores que merecen estudio son la Estrategia de Ciberseguridad 2013 de la Unión Europea[170] y el proyecto de Directiva de Seguridad de las Redes y la Información (NIS)[171]. Ambos, pero específicamente la Directiva NIS, estipulan requisitos integrales, normas y obligaciones para el sector privado, los CERT, y los operadores de infraestructuras críticas, redes y sistemas de información.

El punto de interés en este contexto es que la Unión Europea constituye un territorio con leyes armonizadas en la esfera cibernética. De los 28 países, 23 han incorporado al derecho nacional el Convenio de Budapest sobre la Ciberdelincuencia (el resto, sin duda, lo hará en breve) y todos han incorporado la (similar) Directiva de 2002[172]. Por tanto, la ciberdelincuencia y cualquier intrusión en dispositivos y redes digitales son

---

169 www.enisa.europa.eu. Véase también Henning Wegener, *La ciberseguridad en la Unión Europea,* http://www.ieee.es/Galerias/fichero/docs_opinion/DIEEE077bis-2014_CiberseguridadProteccionInformación_H.Wegener.pdf. Hay una versión en alemán del documento en www.unibw.de/infosecur

170 JOIN (2013)1 final.

171 COM (2013)48 final.

172 COM (2002)173 final.

sancionados de igual manera en todos los países de la Unión Europea, y la aplicación de la ley pueden seguir su curso en cualquier lugar de la Unión.

Otro aspecto importante de la política digital de la Unión Europea es la protección de datos. La protección de información personal y de la esfera privada de los individuos ha pasado a ser relevante sólo con el desarrollo del almacenamiento de datos digitales. Las leyes vigentes en la Unión Europea son de gran calado. La base jurídica actual sigue siendo la Directiva de la UE 95/46 CE, que detalla las normas mínimas de protección que todos los miembros de la Unión Europea han incorporado en sus respectivas legislaciones nacionales. La Directiva se aplica a los datos personales de los individuos. El uso de los datos es legítimo si el interesado ha expresado su consentimiento, o si están presentes otras circunstancias estrictamente definidas. Las restricciones también se aplican en cierta medida a usuarios de datos externos a la Unión [173].

En 2010, la Comisión de la Unión Europea puso en marcha un proyecto legislativo más ambicioso para adaptar la protección de datos existente a las nuevas circunstancias.[174] El proyecto de Reglamento (Reglamento Europeo de Protección de Datos) pretende responder a las necesidades de una sociedad de la información avanzada caracterizada por un enorme aumento de los flujos de datos, el almacenamiento en la nube, las nuevas redes sociales y un aumento exponencial de la conectividad. Una vez aprobado el Reglamento, el nuevo texto será inmediatamente obligatorio en todos los Estados Miembros y creará un cuerpo legal uniforme de la Unión Europea, con un único conjunto detallado de reglas para los 28 Estados Miembros. El Reglamento es más estricto y detallado que la Directiva de 1995 y prevé fuertes multas en caso de incumplimiento. El proyecto de texto pasó el trámite del Parlamento Europeo en marzo de 2014 y actualmente está siendo discutido por los gobiernos con miras a una decisión en el Consejo Europeo. Es previsible que se disponga de una versión final en los próximos meses y que entre en vigor en 2016. Sin embargo, ya ha tenido efectos anticipados al mostrar que la Unión Europea camina hacia un régimen de datos muy estricto.

---

173 Para la mayoría de los Estados de la Unión Europea, también son pertinentes otros dos instrumentos internacionales, las Directrices de la OCDE sobre Protección de la privacidad y flujos transfronterizos de datos personales, y el Convenio Europeo de Protección de datos del Consejo de Europa, que obliga a los 46 Estados firmantes.

174 COM(2012)11 final.

Después de esta breve panorámica de la legislación europea actual e inminente como esquema jurídico coherente, volvamos al problema de la vigilancia en el ciberespacio. Cualquier intrusión en portadores de datos digitales (computadoras, teléfonos, redes, otros dispositivos digitales) así como la copia, el robo, el intercambio o la transferencia de datos almacenados constituye un ciberdelito si no existe una justificación concreta. La intrusión en dispositivos y redes digitales que afecte a datos personales también supone una violación de las leyes de protección de datos. Por tanto, la ciberdelincuencia y la manipulación de datos personales están estrechamente ligadas y es necesario invocar ambos cuerpos de prescripciones jurídicas. La libertad en Internet está en juego en ambas categorías de ciberdelitos.

El espionaje industrial o político en Internet (o de la nube o de otros sistemas de almacenamiento), es decir, el robo o manipulación de información sobre acontecimientos políticos o datos comerciales que no incluyan datos personales, no está sujeto a sanción por el derecho internacional. Sin embargo, sí es objeto de sanción en países con cobertura jurídica del derecho penal y el derecho civil normales, con independencia de que el autor del delito sea persona, empresa, institución o gobierno extranjero. En los países de la Unión Europea el Convenio de Budapest y/o la legislación interna proporcionan las herramientas necesarias. En el campo del derecho penal es aplicable aunque el ataque proceda de otros países siempre que el delito haya tenido efectos o causado daños en el interior del país. Conforme a la Convención, un Estado miembro está obligado a castigar los ciberdelitos cometidos en su territorio, aunque el autor no resida en el mismo.[175] La ubicuidad de los efectos de los ciberdelitos acerca el régimen jurídico de la ciberdelincuencia al derecho penal internacional, aunque aún no sea universalmente adoptado o aplicado, especialmente si el Estado de origen no coopera o es el perpetrador. Si la vigilancia y captura de datos incluye datos personales, también son de aplicación las prohibiciones y sanciones de las leyes de protección de datos.

Por tanto, lo cierto es que la actual situación de intrusión masiva en el ciberespacio por parte de gobiernos, nacionales o extranjeros y entes privados, constituye al amparo del derecho de la Unión Europea y allá donde existe de una legislación similar, una violación grave de la ley salvo que la intrusión esté justificada por motivos de seguridad pública y orden público y esté autorizada de conformidad con la legislación nacional y los correspondientes procedimientos jurídicos, lo que la convierten en una actividad legal. Para ser precisos, a pesar de las prácticas extendidas de los gobiernos, los ciberataques sobre objetivos en países extranjeros no se justifican en modo alguno

175 Véase el párrafo 233 del Informe Explicativo del Convenio de Budapest sobre el ciberdelito.

por convicciones nacionales, por necesidades percibidas de seguridad o por procedimientos legales de un gobierno extranjero, hasta que se disponga del consentimiento expreso del gobierno del país donde se produce la intrusión o donde se perciben sus efectos. En la Unión Europea, con frecuencia se realizan actuaciones conjuntas de gobiernos de Estados Miembros que, por tanto, se consideran legales. Se incluye la vigilancia a gran escala de las conexiones internacionales de Internet, los nodos de la red, las conexiones inalámbricas, etc. Ello hace aún más lamentable las noticias sobre el alcance ilimitado de la recopilación de datos (una auténtica inmoderación recopiladora) por parte de servicios de seguridad extranjeros. Dicha recopilación de datos aprovecha capacidades y medios disponibles como nunca lo han estado, que de forma patente exceden lo que sería una evaluación pragmática de riesgos y una lógica de seguridad aceptable, a menudo sin preocupación alguna por los gobiernos amigos, la protección de datos, los derechos humanos y los daños causados[176].

Es necesario hacer varias advertencias en relación con esta descripción de la situación jurídica, advertencias cuya aplicación va más allá de los límites de la Unión Europea. En primer lugar, el anonimato que brinda la red dificulta la detección de los ciberataques. La falta de imputabilidad y de seguimiento y rastreo hace que, en muchos casos, la aplicación de la ley sea inviable o al menos compleja. Si un ataque a datos se inicia desde el extranjero, existe la dificultad añadida de que el Estado de origen pueda no cooperar para detener al perpetrador. Eso, por supuesto, no es óbice para actuar con todas las armas jurídicas posibles. En segundo lugar, los gobiernos extranjeros operan en su mayoría bajo el manto de la soberanía y la inmunidad diplomática individual de los autores; no obstante, muchas actividades de vigilancia son realizadas por contratistas privados a los que no se les aplica esta lógica. Sin embargo, la incapacidad de procesar a los autores (en principio sólo puede recurrirse a procedimientos diplomáticos) no modifica la situación jurídica subyacente. En países donde en caso de sospecha de delito penal el fiscal tiene que actuar de oficio, como ocurre en la mayoría de los países de la Unión Europea, existe la obligación de iniciar un procedimiento penal aunque el acusado invoque la inviolabilidad de la soberanía. Actualmente hay en curso en Alemania procedimientos penales en contra de "desconocido" para el procesamiento por escuchas ilegales del teléfono móvil de la jefa de gobierno. Por higiene legal sería deseable que dichos procedimientos se llevaran a cabo con más frecuencia, o incluso que fueran la regla.

---

176 El informe del Comisionado de las Naciones Unidas para los Derechos Humanos antes citado incide enérgicamente en este punto.

En tercer lugar, probablemente sea muy adecuado formular, preferentemente en un contexto de aplicación internacional, una doctrina sobre la vigilancia digital de los servicios de seguridad del Estado, nacionales o extranjeros, cuando no exista autorización previa en caso de "peligro manifiesto e inmediato" por amenaza terrorista importante e inminente, cuando los criminales son sorprendidos en flagrante delito, o en caso de ataque o delito grave inminente contra infraestructuras críticas, y similares. Siempre es posible una autorización a posteriori de los hechos.

El actual sentimiento de rebelión que existe en la mayoría de países europeos contra la intrusión masiva y las actividades de espionaje de las agencias de los Estados Unidos de América, pero también de otros países, parece un tanto exagerada y alimentada artificialmente; antes de tratar de buscar criterios razonables para separar lo necesario de lo estrictamente inaceptable, sería útil inyectar al debate una dosis de realismo y desdramatizar la situación[177].

En primer lugar, es inevitable tener presente que se ha producido un progreso técnico sin precedentes que permite la injerencia masiva en dispositivos digitales, la recopilación de datos a gran escala y el procesamiento con potentes herramientas de búsqueda. Como cuestión de principio no puede condenarse el uso de estas tecnologías para fortalecer la política de seguridad nacional. Las tecnologías no pueden ignorarse, están aquí para quedarse. Las nuevas tecnologías se utilizan una vez que están disponibles y no es posible la marcha atrás.

En segundo lugar, los servicios de inteligencia de los países de la Unión Europea han utilizado igualmente estas técnicas, a menudo en un marco de una estrecha cooperación conspirativa con sus homólogos estadounidenses. Todos, o la mayoría de ellos, emplean estas tecnologías en sus operaciones exteriores, e incluso a nivel doméstico. Ese es particularmente el caso del Reino Unido, donde se utilizan datos y prácticas del programa PRISM de los Estados Unidos sin las garantías o controles judiciales requeridos. Incluso se utilizan en ausencia de sospecha de delito concreto, así como para recabar enormes cantidades de datos aleatorios a través del espionaje de las redes sociales y del acceso a todos los cables de fibra que circulan a través del territorio del Reino Unido ("Programa TEMPORA"). La gran indignación de muchos sectores europeos sobre las prácticas de los Estados Unidos tiene, por tanto, cierta dosis de hipocresía.

---

177 Nigel Inkster ha realizado intentos similares, *The Snowden Revelations: Myths and Misapprehensions,* SURVIVAL, febrero-marzo de 2014, p. 51; Joachim Krause, *Diskutieren statt moralisieren,* Internationale Politik, enero-febrero de 2014, p. 108.

En tercer lugar, los avances en materia de seguridad de los Estados Unidos de América en su lucha contra el terrorismo, el crimen organizado, el lavado de capitales, etc. son indiscutibles y, dada la superioridad tecnológica de los servicios de Estados Unidos, abundan ejemplos que muestran que los aliados europeos han estado entre sus principales beneficiarios.

En este sentido, puede debatirse de forma legítima el alcance de las medidas de vigilancia, pero en mucha menor medida una justificación básica de las mismas. En cuanto al alcance, sólo una fracción de los datos obtenidos o accesibles por los servicios de Estados Unidos se utiliza realmente. De acuerdo con las cifras de la NSA para 2013, la cantidad de datos que circulan por Internet a diario en Internet asciende a 1 828 petabytes. La NSA puede capturar solamente el 1,2 por ciento de ellos y examinar sólo una pequeña fracción de los mismos. Ello es equivalente al 0,0004 por ciento del tráfico de datos en la red, de forma que mediante los filtros utilizados sólo podría analizarse esa fracción de los datos.[178] Es importante tener en mente el orden de magnitud.

Finalmente, tal como ya se ha indicado, actualmente se está produciendo un saludable debate en los Estados Unidos. El país nunca ha sido un bloque monolítico de opinión, sino más bien es una democracia vibrante con una gran capacidad de aprendizaje. Es muy probable que el actual proceso desarrollado en los Estados Unidos para modificar las políticas y prácticas de vigilancia y protección de datos, de lugar finalmente a una contexto transatlántico más amigable. Ya en enero de 2014, el presidente Obama anunció medidas de limitación de daños.[179]. Ello supone, entre otras cosas, un control administrativo más estricto de las operaciones de inteligencia que en ocasiones gozan de gran autonomía; que la recopilación de datos sea estrictamente para fines de seguridad pública; que sea la industria quien almacene los datos relativos a las telecomunicaciones y que sólo sean accedidos por los servicios de inteligencia con autorización judicial.

Los argumentos anteriores, destinados a moderar el debate, no pretenden en absoluto trivializar una práctica actual de recopilación de datos que resulta imprudente y excesiva en cantidad. No hay duda de que las posiciones transatlánticas

---

178 Datos de Joachim Krause, ibid p. 114. Considerando la fuente, la NSA, algunos dudan de la veracidad de las cifras, pero aunque solo sean indicativas, muestran que la Agencia no es capaz de vigilar más de una fracción del tráfico en Internet, con datos parciales pertinentes a los efectos de seguridad, muy lejos de la recopilación total de los datos.

179 "Presidential Policy Directive" PPD 28, www.whitehouse.gov

en materia de vigilancia y protección de datos y sobre las necesarias limitaciones jurídicas, están aún distantes, en buena medida por razones históricas, por la tradición jurídica y por la traumática experiencia terrorista de 2001. Simplemente no se entiende de la misma forma el equilibrio entre seguridad y libertad. Es probable que esa diferencia no desaparezca a corto plazo. A pesar de la dudosa legalidad y el agravio que suponen el espionaje y la intrusión ilegal, no es probable que estas prácticas desaparezcan, aunque es importante expresar con claridad sus connotaciones delictivas y la responsabilidades penales. "Espiar a aliados" es un tema especialmente sensible, que afecta a la camaradería, a los objetivos comunes e incluso a lazos de amistad personales, pero es una actividad con una larga tradición, incluso en el contexto transatlántico. Pero al margen de tratarse de una violación de la etiqueta en la red (confianza), es poco probable que los aliados se apresuren a celebrar acuerdos formales de "no-espionaje"[180]. Un entendimiento informal sobre esta materia sería sin duda recibido con beneplácito.

Se han vertido ríos de tinta para ofrecer soluciones al dilema de la vigilancia, especialmente en lo relativo a la relación entre la Unión Europea y los Estados Unidos de América. El debate público y las discusiones a nivel de gobiernos siguen estando activas, y sería pretencioso ofrecer recomendaciones firmes y completas a las partes. En su lugar, esta contribución finaliza aportando consejos muy modestos.

En cuanto a la Unión Europea, es importante ultimar cuanto antes los documentos jurídicos previstos para completar los componentes de ciberseguridad de la Agenda Digital de la Unión Europea, a saber, la Directiva de Seguridad de las Redes y la Información (NIS) y el Reglamento General sobre la Protección de Datos (GRDP), bases comunes para los futuros acuerdos con los Estados Unidos y el resto del mundo.

Los Estados Miembros de la Unión Europea también deben asegurarse de que sus propios servicios de inteligencia cumplan estrictamente la legislación europea y nacional. No tendría ningún sentido pedir a los Estados Unidos más de lo que la propia Unión Europea hace. Los países de Unión Europea también deben llegar a un acuerdo mutuo de no espionaje en el ámbito de toda la Unión Europea y considerar el establecimiento gradual de un servicio de inteligencia de la Unión Europea que comparta toda la información entre los miembros de la Unión. Mientras tanto, debería haber una mejor coordinación entre los respectivos servicios de seguridad.

---

180 Véase Leif-Eric Easley, *Spying on Allies.* SURVIVAL, agosto-septiembre de 2014, p. 141, Rodri Jeffreys Jones, *Eine Frage der Etikette,* Internationale Politik, septiembre-octubre de 2014, p. 74.

En los países de la Unión Europea deben activarse efectivamente las leyes nacionales sobre el ciberespacio y la protección de datos a fin de demostrar que la ley puede hacer frente a las sospechosas operaciones de inteligencia y espionaje.

Tal como se demuestra en un capítulo anterior, la mejor ciberdefensa es la que se apoya en una resiliencia fortalecida y en prevenir la recopilación ilegal de datos y ataques a la información. Existe mucho margen para el fortalecimiento de la resiliencia técnica de sistemas y redes, lo que aumenta la auto-protección de los usuarios (mejor conciencia de la seguridad, mayor economía en la información y prácticas de respaldo, encriptación, etc.). En otras palabras, antes de lamentarse hay que hacer los deberes.

Recuperar la ciberconfianza en el contexto transatlántico es una tarea difícil que sólo rendirá resultados con el tiempo. Pero ha llegado el momento de trabajar en un entendimiento conjunto y transparente sobre cómo encontrar un equilibrio sólido entre los requisitos de libertad y seguridad, y sobre cómo el trabajo de inteligencia y vigilancia de gobiernos extranjeros puede hacerse compatible con las disposiciones legislativas internas de la Unión Europea. Es impensable que los agentes extranjeros se ciñan a las normas del país en el que operan. A este respecto, es posible que la brecha trasatlántica no se cierre pronto, pero debería reducirse. Claramente, la Unión Europea no puede apartarse de sus exigentes normas de protección de datos. Deben iniciarse los trabajos para un "acuerdo de puerto seguro" revisado que regule los prerrequisitos de las transferencias de datos transfronterizos y la aplicación rigurosa y sin demora del mismo.

Después de la actual avalancha de casos de intrusión en el mundo de los datos (cuyos excesos son ampliamente reconocidos) debe imponerse un nuevo espíritu de proporcionalidad y medida en virtud del cual el inmenso potencial técnico de captura de datos se utilice con moderación, teniendo en cuenta los intereses afectados, incluidos los derechos humanos, y el respeto a los principios jurídicos de los países donde se realizan las búsquedas de datos. Es necesaria una cultura que favorezca una evaluación más moderada de las necesidades de seguridad y una mayor limitación de las mismas.

A medio plazo, debe prevalecer la perspectiva global. La Unión Europea debe contribuir a identificar un marco reglamentario de alcance internacional, en total sintonía con la Resolución A/RES/68/167 de la Asamblea General de las Naciones Unidas, y contribuir así a un equilibrio razonable entre intereses comunes en materia de seguridad y la libertad en Internet.

3.5 Límites de la ciberlibertad: búsqueda de criterios

por William A. Barletta

La tecnología de las telecomunicaciones digitales, como ejemplifica de manera especial Internet, ha tenido efectos sociales disruptivos de una magnitud sólo comparable a la electrificación de ciudades y pueblos hace más de un siglo. Al igual que la electrificación, las telecomunicaciones digitales dependen de que exista un gran número de redes interconectadas. Pero a diferencia de las redes eléctricas (*grids*) cuyo alcance es regional, Internet está en todo el mundo, cruza fronteras nacionales y diferencias culturales. Al igual que en el ámbito de la electrificación, a la que no tienen acceso aproximadamente dos mil millones de personas que sufren "pobreza energética", en el contexto de Internet existe una cantidad comparable de personas que sufren "pobreza de información". Al igual que las redes eléctricas modernas que permiten a los consumidores transmitir y recibir energía, los usuarios de Internet transmiten y reciben información de forma rutinaria, a menudo en la misma medida.

Por tanto, tal como ocurre en el análisis jurídico y político de las redes de energía, el análisis de utilidad de la sociedad de la información ha generado sus propios términos de justicia distributiva e imperativo moral. Libertad[181] es un término que induce a muchos a pensar en la libertad en Internet como un derecho humano fundamental tal como éste se define en la Declaración Universal de los Derechos Humanos[182] (DUDH). En particular, el artículo 19 de la DUDH garantiza el derecho a la libertad de expresión:

"Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."

---

181 La libertad en Internet se ha denominado un término "plástico" (algo sin un sentido auténtico) que es utilizado por los Estados Unidos y sus aliados europeos en su lucha por la futura gobernanza de Internet. Véase "World War 3.0," Vanity Fair, mayo de 2012.

182 Asamblea General de las Naciones Unidas, Resolución 217A (III), 10 de diciembre de 1948, http://www.un.org/en/documents/udhr/

Wetsby apunta lo siguiente[183]: "Aunque la Declaración Universal de los Derechos Humanos no es directamente vinculante para los Estados Miembros de las Naciones Unidas, algunas partes de la Declaración, incluido el Artículo 19, han adquirido fuerza jurídica de derecho internacional consuetudinario. La redacción del Artículo 19, "[…] no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras" se adapta perfectamente a la taxonomía usual de la libertad en Internet, que incluye la libertad de acceso. Algunos consideran que la frase "no ser molestado" implica el derecho a la privacidad, al anonimato, a la seguridad de los datos e incluso a suprimir contenidos en la red."

En virtud del Artículo 19, el *acceso* a Internet puede considerarse una factor representativo para juzgar la libertad en Internet. El Artículo 19 implica además que los límites a los contenidos (o a su uso) y el grado de injerencia (privacidad e integridad de los contenidos) son también factores representativos de la evaluación de la libertad en Internet. La organización de vigilancia internacional, Freedom House, evalúa anualmente[184] la situación de la libertad en Internet. Su Informe de 2013[185] concluye que desde mediados de 2012, de los sesenta países evaluados, treinta y cuatro han "[...] experimentado una evolución negativa", mientras que dieciséis experimentaron una "evolución positiva".

---

183 J.R. Westby, The Role of Science and Technology as Empowerment of Person and State, Proceedings of 44th Session, International Seminars on Planetary Emergencies, 19-24 de agosto de 2011, Erice, Sicily.

184 Freedom House aplica un enfoque basado en tres pilares para valorar la libertad en Internet y en el mundo de las TIC:

- Obstáculos al acceso, incluidas barreras económicas y a las infraestructuras de acceso, de naturaleza jurídica y de control de la propiedad de los proveedores de acceso a Internet (ISP), así como la independencia de los órganos reguladores;
- Limites a los contenidos, incluida la regulación jurídica de contenidos, el filtrado y bloqueo técnico de sitios web, la autocensura, la vibrante y diversa variedad de medios de comunicación en línea y la utilización de las TIC para la movilización cívica;
- Violaciones de los derechos de los usuarios, incluida la vigilancia, la privacidad y las repercusiones por la actividad en línea, como la reclusión, el acoso extralegal o los ciberataques.

Sus informes están disponibles en http://www.freedomhouse.org/report-types/freedom-net#.VBB2dUhA140

185 Freedom on the Net 2013, A Summary of Findings, p. 2. Disponible en http://www.freedomhouse.org/report/freedom-net/freedom-net-2013#.VBB6CUhA140

Estas medidas podrían calificarse como formas de liberación de la represión, particularmente cuando Internet se utiliza para dar a conocer agravios sociales, organizar fuerzas políticas de la oposición, o simplemente difundir información que puede ser embarazosa para quienes detentan el poder. Los miembros de este grupo han escrito mucho sobre el asunto del empoderamiento de los ciudadanos a través de Internet y de su ciberrepresión.[186]. Westby ha declarado sin tapujos: "*Hay un choque entre los intereses del Estado nacional y los derechos de las personas, y las TIC son la herramienta que ambas partes han elegido para reafirmar su poder*."[187]

Lo que en las sociedades "libres" se reduce a un problema de equilibrio político permanente (cuya dificultad se reconoce) entre libertad e intervención del Estado en un marco de criterios jurídicos claros, en muchos otros Estados se convierte en un problema de derechos humanos y de la calidad del orden global de la información. La censura en Internet por parte de gobiernos mediante tecnologías de filtrado, sin restricciones jurídicas y con graves y profundas consecuencias para el individuo que desea buscar y compartir información, constituye una violación de los derechos humanos de dimensión muy relevante[188].

Si bien esta tensión se aprecia más fácilmente en relación con la conducta de los Estados, la ausencia de gobierno central en Internet, junto con su estructura distribuida, permite que organizaciones no gubernamentales y empresas limiten significativamente la libertad en Internet de poblaciones objetivo. Internet ha fortalecido el poder de los actores no estatales hasta tal punto que a los gobiernos les resulta atractivo coaccionar a empresas [189] para que realicen funciones de censura, de seguimiento de utilización, etc.

---

186 H. Wegener, "*Cyber Repression*: *Going Worse. What can be done*?" Actas del Seminario Internacional sobre Emergencias Planetarias, Erice, (2011), "Las consecuencias de un censura exhaustiva (ciberrepresión) son graves y no pueden subestimarse. Los ciudadanos se ven privados de importantes beneficios de la era de la información y reciben una visión sesgada de la realidad del mundo, quedando condenados a la inmadurez política. La ciberrepresión masiva puede modificar el pensamiento colectivo de una nación. La gravedad de la supresión masiva de información es equivalente a otras variantes del ciberdelito y de los ciberconflictos …".

187 Westby, op.cit.

188 Wegener, UIT 2011, p. 46.

189 "El gobierno de los Estados Unidos amenazó a Yahoo con una multa de 250 000 $ diarios si no acataba una amplia petición de datos de usuarios que la compañía consideraba inconstitucional, de conformidad con documentos judiciales descatalogados el pasado jueves." *U.S. threatened massive fine to force Yahoo to release data*, Washington Post, 11 de septiembre de 2014.

En países con industrias que producen la tecnología de Internet podría considerarse un posible enfoque para el equilibrio de la libertad de acceso a escala global. Los gobiernos de esos países podrían prohibir o, al menos requerir informes sobre la exportación de "[...] bienes y tecnologías que puedan ayudar a un gobierno extranjero a adquirir la capacidad de censurar, vigilar o realizar cualquier otra actividad conexa a través de las telecomunicaciones, incluida Internet".[190] Si bien la eficacia de tales medidas es discutible, ponen de relieve la complementariedad de las acciones de los Estados y de la industria en el establecimiento de los límites de la libertad en Internet.

Como la mayoría de indicadores de seguimiento del comportamiento, estas medidas negativas sólo son una parte del problema. Tan reveladores resultan, aunque más difíciles de cuantificar, los comportamientos que fomentan el bienestar social y económico de una sociedad. Una gobernanza estricta con el objetivo de asegurar la estabilidad, seguridad y resiliencia de la red puede anular la inventiva, los nuevos paradigmas de la red y la apertura tecnológica.

No puede sorprender que los legítimos intereses (colectivos) de los Estados puedan colisionar con los intereses de las personas en el ciberespacio. Estos intereses incluyen, pero no se limitan a, la protección de los ciudadanos de daños reconocidos como la preservación de las normas sociales (culturales), la prevención de crímenes atroces[191] y del terrorismo, la prevención de la interrupción de infraestructuras sociales críticas (incluyendo Internet y otras infraestructuras de las tecnologías de la información), la protección de secretos de Estado legítimos, la promoción de la política exterior del Estado, y la promoción de bienestar económico nacional, especialmente a través de externalidades. Aunque las normas de conducta para promover los intereses del Estado en competencia están bien desarrolladas fuera del ámbito del ciberespacio, en éste surgen dificultades por la confusión debida a 1) la ausencia de marcos jurídicos armonizados para regir el comportamiento en el ciberespacio y 2) las importantes diferencias culturales de origen histórico que abundan en una red mundial que cruza las fronteras nacionales.

---

190 Cámara de Representantes de los Estados Unidos, H.R.3605 - Global Online Freedom Act of 2011.

191 International police cooperation to root out child pornography is a universally agreed upon example.

Un ejemplo puede resultar ilustrativo. Los países de la Unión Europea tienen en general prohibiciones muy claras con respecto a contenidos que definen como "discurso del odio" o equivalente.[192]. Estas prohibiciones tienen sus raíces en la muerte de millones de personas durante la Segunda Guerra Mundial. Algunos Estados musulmanes tienen prohibiciones igualmente severas con respecto a la difusión de otras creencias[193] o la difusión de representaciones blasfemas de la palabra o la imagen del profeta Mahoma. En ambos casos, las prohibiciones reflejan valores culturales muy asentados, cuya violación puede llevar a la discordia social e incluso a la violencia. Cuando los gobiernos bloquean dichos sitios, ¿están cometiendo violaciones represivas de los derechos humanos?.

Por el contrario, Estados Unidos de América tiene una visión amplia de lo que constituye un discurso permisible, algo consagrado en su Constitución. El conocido jurista americano Lawrence Tribe (junto a otros colegas) ha escrito[194]:

> "La palabra es poderosa. Es el alma de la democracia, una condición previa para el descubrimiento de la verdad y vital para nuestro desarrollo personal. Pero la palabra también es peligrosa. Puede corromper la democracia, permitir o incitar a la delincuencia, alentar a los enemigos y entorpecer al gobierno. Puede esgrimirse como un arma y desplegarse contra objetivos indeseados."

Sin embargo, incluso en Estados Unidos las limitaciones al derecho de expresión con el objetico de frenar el "discurso del odio" y el "ciberacoso" son cada vez más comunes. En una sociedad como la estadounidense, con elevado índice de litigios, las limitaciones no constituyen restricciones de antemano a la capacidad de expresión, pero sí pueden justificar demandas por agravio o incluso sanciones penales.

---

192 Por ejemplo, un tribunal francés ordenó a Yahoo! Retirar símbolos nazis de su sitio de subastas. ¿Es eso más grave que la actitud de China forzando a Yahoo! a un "compromiso voluntario" para evitar la "producción, publicación o difusión de información perniciosa que pueda poner en peligro la seguridad del Estado y alterar la estabilidad social? Christopher Bodeen, "Web Portals Sign China Content Pact," Associated Press, 15 de Julio de 2002.

193 Hillary Clinton, "Internet Freedom". http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom.

194 Lawrence Tribe and Joshua Matz, Uncertain Justice, (New York, 2014) p.123.

Más allá del bloqueo físico del acceso a sitios web, los gobiernos pueden hacer que el acceso sea inaceptablemente costoso con la intención efectiva de limitar severamente el acceso en base a consideraciones políticas. Por ejemplo, la vigilancia de los sitios con contenido "peligroso" y/o provocativo o ilegal a fin de rastrear y restringir el acceso de quienes visitan estos sitios, puede ser seguido de la aplicación de procedimientos secretos que afecten a las libertades de las personas que los visitan. Muchas personas se han visto incluidas en listas de prohibición de viajar por vía aérea debido a una vigilancia defectuosa de sitios considerados "terroristas". Aunque es fácil admitir que dichos programas de vigilancia están respaldados por razones de interés de Estado, es preocupante la falta de procedimientos judiciales abiertos para equilibrar dicha situación con los intereses individuales afectados.

Existen desacuerdos significativos entre los países en relación con las políticas en materia de anonimato y privacidad. Muchos perciben el anonimato de las comunicaciones en Internet como un derecho. Dado que el anonimato puede proteger del acoso o la represalia a quien se expresa, se percibe como una libertad de expresión esencial. De hecho, Estados Unidos reconoce[195] el derecho a hacer campaña política en el anonimato; asimismo, se ha confirmado el derecho a interacciones anónimas entre personas "siempre y cuando esos actos no constituyan una violación de la ley".[196] Sin embargo, Estados Unidos no ha promulgado políticas generales relativas al anonimato y la privacidad en la web, prefiriendo regular industrias específicas. La Unión Europea ha sido más agresiva y ha optado por regular directamente los derechos de privacidad y al anonimato de las personas.

En contraste con lo anterior, el anonimato puede ser un escudo que proteja comportamientos disruptivos y criminales. Entre otras restricciones impuestas para reforzar los controles sobre el uso de Internet, Rusia ha prohibido recientemente el acceso anónimo a redes Wi-Fi en lugares públicos[197] donde la dirección IP no puede vincularse inequívocamente a individuos concretos. Por otra parte, tal como muestran las revelaciones de Snowden, el gobierno estadounidense sigue aplicando una prerrogativa muy amplia (y tal vez ilimitada) de rastrear las comunicaciones por Internet. No son sólo los gobiernos quienes rastrean en Internet, actores corporativos

---

195 Tribunal Supremo de los Estados Unidos de América, McIntyre v. Ohio Elections Commission (93-986), 514 U.S. 334 (1995).

196 "Decision *Columbia Insurance Company v. Seescandy.com, et al.* of the U.S. District Court in the Northern District of California".

197 "Medvedev signs order banning anonymous Wi-Fi," http://en.itar-tass.com/russia/744055, 8 de agosto de 2014.

muy importantes como Google también rastrean de manera generalizada la utilización de sus servicios. No es sorprendente que los usuarios tengan ahora, lo quieran o no, una experiencia de uso de Internet personalizada (u orientada).

El uso generalizado por parte de los Estados Unidos de América de redadas de vigilancia y el seguimiento de las comunicaciones de jefes de gobierno amigos, según las revelaciones de Snowden, sugiere que pocas comunicaciones, o acaso ninguna, son realmente privadas. Lamentablemente, se evita tener un debate público completo sobre el las motivaciones y autoría de tales actividades del Estado, incluso por parte del poder judicial, con el argumento del privilegio de los secretos de Estado.[198] La defensa que hace el gobierno de Estados Unidos de que "todo el mundo lo hace" no es tranquilizadora. De hecho, con el enorme aumento de la capacidad por unidad monetaria de las computadoras y del almacenamiento de datos, prácticamente cualquier Estado industrializado puede supervisar todo el tráfico de Internet que entra o sale del país. En el caso de los países con el nivel económico más elevado, es posible una vigilancia masiva de todo el tráfico con la complicidad (forzosa o voluntaria) de los proveedores de servicios de telecomunicaciones.

La respuesta de la opinión pública, tanto en los Estados Unidos de América como en Europa, tras la revelación de la vigilancia casi universal realizada sobre el tráfico de telefonía móvil, ha hecho que Apple dote a su sistema operativo móvil más reciente (iOS 8) de una potente capacidad de encriptación y que no tenga puerta trasera. Así, ni siquiera Apple puede descifrar un teléfono sobre el que pese un mandato judicial.[199] Si bien los críticos de Apple insisten en que el sistema operativo iOS 8 "sólo detiene

---

198 "El privilegio de secreto de Estado es una regla probatoria existente en los Estados Unidos de América y basada en precedentes jurídicos. La aplicación del privilegio conlleva la exclusión de una prueba […] exclusivamente en base a una declaración jurada remitida por el Gobierno que informa de que los procesos judiciales pueden desvelar información sensible que puede poner en peligro la seguridad nacional. El primer caso en el que se reconoció formalmente el privilegio fue en *Estados Unidos contra Reynolds*, en el que se vieron involucrados secretos militares." http://en.wikipedia.org/wiki/State_secrets_privilege

199 Código privado de Apple: "Nuestro compromiso con la privacidad de nuestros clientes no termina porque exista un petición de información del gobierno." https://www.apple.com/privacy/government-information-requests/ Véase también Matthew Green, "Is Apple picking a fight with the US government," Slate, 23 de septiembre de 2014. Disponible en http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html

investigaciones legales que gozan de garantías legales"[200], sus defensores argumentan que Apple "construye sistemas que impiden el acceso al teléfono de un usuario a quienes desean obtener los datos del mismo, incluidos piratas informáticos, personal interno malicioso e incluso gobiernos extranjeros hostiles. Ello sirve absolutamente al interés público. Además, al hacerlo Apple sienta el precedente de que sean los usuarios y no las empresas, quienes controlen las claves de acceso a sus propios dispositivos."[201] Aún no se conoce la respuesta oficial del gobierno de los Estados Unidos, sin embargo, varios funcionarios públicos ha denunciado[202] el enfoque de Apple. No sería sorprendente que hubiera una respuesta oficial de carácter más coercitivo que de persuasión moral.

Estados Unidos ha tratado con anterioridad de imponer requisitos a los fabricantes de hardware que permitan el seguimiento, revelar identidades y desencriptar el tráfico de Internet. Al describir cómo trabaja el Departamento de Estado de los Estados Unidos de América para "proteger y defender una Internet libre y abierta " como elemento de su política[203], la Secretaria Clinton ha explicado:[204]

> "Todas las sociedades reconocen que la libertad de expresión tiene sus límites. No toleramos a aquellos que incitan a otros a la violencia, como los miembros de Al Qaeda que utilizan Internet para promover el asesinato en masa de personas inocentes. El discurso del odio dirigido a las personas en razón de su origen étnico, género u orientación sexual es condenable. Es lamentable que estos asuntos sean retos crecientes de la comunidad internacional, que debe combatirlos unida. También es necesario hacer

---

200 Oren Kerr, "Apple's dangerous game," http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/Kerr ha cambiado en cierta forma su opinión, y reconoce que un sistema con una puerta trasera para la encriptación está sujeto al pirateo por cualquiera y, por tanto, compromete la seguridad del sistema en su conjunto.

201 Matthew Green, Ibid.

202 En una entrevista en el programa de noticias de la CBS "60 minutes" del 12 de octubre de 2014, el Director del FBI James Carney dijo que la nuevas características de privacidad de Apple protegen a secuestradores, pedófilos y terroristas. Véase http://money.cnn.com/2014/10/13/technology/security/fbi-apple/index.html?hpt=hp_t2

203 Departamento de Estado de los EE.UU., "International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World," http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

204 Clinton, op. cit.

> frente al discurso anónimo. Aquellos que usan Internet para reclutar terroristas o para distribuir propiedad intelectual robada no pueden pretender separar sus acciones en línea de sus identidades en el mundo real".

No obstante, de forma simultánea el FBI ha advertido a los propietarios de cibercafés en los Estados Unidos "[...] que la utilización de determinadas medidas básicas de ciberseguridad podría considerarse motivo suficiente para sospechar de una posible actividad terrorista".[205]

En el mundo en desarrollo existen tensiones similares entre los intereses individuales y del Estado, mientras que en el mundo industrializado se considera que la criptografía es un arma que pueden utilizar tanto ciudadanos respetuosos de la ley como delincuentes y terroristas.

En África, las leyes específicas sobre encriptación parecen circunscribirse a países del Norte del continente, a saber, Argelia, Egipto, Marruecos y Túnez, junto con Nigeria y Sudáfrica. En el continente, Sudáfrica está a la vanguardia en materia de leyes sobre criptografía, aunque los aspectos éticos de la ley [sudafricana] de divulgación de claves es cuestionada por algunos defensores a ultranza de los derechos humanos. Para algunos, la criptografía parece ser la única solución ante las amenazas a la privacidad conforme la sociedad humana se adapta a la digitalización de las redes mundiales.[206]

Los sistemas de criptografía de clave simétrica, como Open PGP que está considerada una tecnología potente, están a disposición de cualquier persona que no resida en un Estado que apoye al terrorismo, según la clasificación del Departamento de Estado de Estados Unidos. Es difícil pensar que esta restricción disuada a las células terroristas. Asimismo, también resulta difícil imaginar que quienes proponen una encriptación de nivel militar consideren realistas propuestas de "depósito voluntario de claves" bajo la custodia del poder judicial de su propio gobierno[207].

---

205 Vanity Fair, op. cit.

206 Cory Farmer y Judson L. Jeffries, "Telecommunications Surveillance and Cryptography Regulatory Policy in Africa," African Policy Journal, mayo de 2013, disponible en http://apj.fas.harvard.edu/category/articles/

207 "En este escenario se mantendrían ocultas tras capas de seguridad copias de claves secretas en un estado durmiente y a las que sólo se tendría acceso si se aseguraran las garantías y esquemas de desencriptación adecuados", Cory y Farmer, Ibid, p.3.

Es evidente que pueden existir conflictos entre gobiernos por la protección de lo que consideran intereses legítimos de sus respectivos ciudadanos. Sin embargo, precisamente cuando los delitos percibidos atraviesan las fronteras nacionales se reducen notablemente las posibilidades de aplicar medias de resarcimiento por el Estado agraviado, salvo el bloqueo de la dirección IP del delincuente. La falta de marcos jurídicos armonizados que rijan el comportamiento en el ciberespacio es un obstáculo muy importante. Incluso si la actuación en el ciberespacio se considera un delito grave en el Estado de la supuesta víctima, el presunto delincuente puede estar fuera del alcance de la ley[208].

Cuando los intereses de los ciudadanos se enmarcan en el lenguaje de los derechos humanos más que en el equilibrio de intereses legítimos, crece la importancia de lo que individuos y empresas consideran que está en juego. El ingeniero y pionero de Internet, Vint Cerf[209] ha señalado lo siguiente:

> "[...] La tecnología es un facilitador de los derechos, no un derecho en sí mismo. El listón debe ponerse muy alto para considerar que algo es un derecho humano. Dicho de forma sencilla, debe ser algo que los seres humanos necesitemos para llevar una vida digna y con sentido, como la libertad contra la tortura y la libertad de conciencia. Es un error incluir una tecnología en particular en esta elevada categoría, pues con el tiempo acabaríamos valorando las cosas equivocadas".[210]

---

208 Para que un país realice una labor de investigación y acusación, sus agentes del orden deben poder recopilar información y pruebas en otros países. El obstáculo fundamental a las investigaciones en las que las pruebas y las sospechas están distribuidas en varios países es la necesidad de que los funcionarios respeten la soberanía de dichos países. Normalmente, los agentes del orden de un país no pueden entrar en otro país a investigar pistas, recoger pruebas y detener a sospechosos. En consecuencia, las investigaciones internacionales requieren la cooperación y ayuda de las autoridades de los países donde se encuentran las víctimas, las pruebas y los sospechosos. Incluso si se ha identificado a los sospechosos, los países no suelen permitir la extradición de sus propios ciudadanos, señalando que lo que procede es una acusación en ese país, en base a que la extradición es inconsistente con su marco jurisdiccional, que violaría las protecciones individuales de sus ciudadanos y que ello conduciría a obstaculizar la validez de las pruebas en el juicio. Sin embargo, las fiscalías han detectado que algunos países que no permiten la extradición de sus ciudadanos no llevan a cabo consistentemente una acusación fiscal a nivel nacional. G.A. Barletta, comunicación privada, 201.

209 Reconocido como uno de los "padres de Internet".

210 V. Cerf, "Internet Access is Not a Human Right", New York Times, 4 de enero de 2012.

Desafortunadamente, considerar la libertad en Internet (acceso) como un derecho humano brinda la ocasión de que, en el debate político, la ideología se imponga al sentido común. Ya sea en forma de "neutralidad de la red" o de "acceso abierto" a publicaciones, tanto la anchura de banda como la gestión de contenidos tienen un coste económico. Con demasiada frecuencia, los ideólogos han tratado de garantizar la "neutralidad" y el "acceso" como un mandato sin respaldo económico en la hipótesis de que "alguien, por lo general el editor, pagará" con un argumento[211] frecuentemente asociado a garantizar la libertad en Internet. No obstante, un acceso generalizado y la minimización de las barreras a la infraestructura son metas deseables que pueden lograrse en el contexto de numerosos modelos de negocio posibles.

La industria ha jugado un papel fundamental en la creación y gobierno de la sociedad digital. La actual libertad de acción en Internet es, en gran medida, consecuencia de los conocimientos que acumula el sector privado en esta materia. Aunque los gobiernos presionan a las empresas para que participen en la aplicación de medidas represivas, la empresas han constituido alianzas de gran alcance con grupos de derechos humanos, académicos, inversores y organizaciones de la sociedad civil para resistirse a tales presiones. Un esfuerzo destacable en este sentido es la Iniciativa de Red Mundial (GNI, *global network initiative*)[212]. La GNI ha presentado su visión[213] sobre "la libertad de expresión y los factores de riesgo de la privacidad" en la cadena de valor de la industria de las TIC. En este sentido, la Iniciativa ha señalado que la industria desarrolla nuevas tecnologías (tanto hardware como software) y productos de seguridad a un ritmo acelerado, productos que suponen nuevos riesgos y oportunidades para la libertad en Internet. Aunque la industria tiene poco control directo sobre el uso de la tecnología por parte de los usuarios finales, sí puede brindar los consejos tecnológicos más adecuados a los proveedores de servicios de telecomunicaciones a fin de minimizar las amenazas incipientes a la libertad en Internet.

La industria de las TIC ha sido cada vez más proactiva en los últimos años en la definición de enfoques para proteger la libertad de expresión y la privacidad. Por ejemplo, la Iniciativa de Red Mundial proporciona a las empresas orientaciones y

---

211 Un ejemplo es el "op-doc" "A Threat to Internet Freedom," de B. Knappenburger, New York Times, 9 de julio de 2014.

212 https://globalnetworkinitiative.org/

213 D.A. Hope, "Protecting Human Rights in the Digital Age," febrero de 2011, http://www.globalnetworkinitiative.org/cms/uploads/1/BSR_ICT_Human_Rights_Report.pdf

directrices sobre la forma de responder a las demandas de los gobiernos para eliminar, filtrar o bloquear contenidos, y sobre cómo responder a las exigencias de las agencias de orden público para la revelación de información personal. Estos tipos de factores de riesgo serán relevantes para empresas que acumulan gran cantidad de información personal y/o que actúan como guardianes del acceso a contenidos, principalmente proveedores de servicios de telecomunicación y empresas de servicios de Internet.

Cabe esperar que a medida que el hardware evolucione con nuevos elementos de seguridad incorporados a nivel de circuito integrado, los gobiernos ejerzan una presión cada vez mayor sobre los fabricantes para permitir su acceso a puertas traseras (por parte de agencias del orden y de agencias de inteligencia) para la vigilancia, el seguimiento de individuos, el conocimiento de actuaciones en Internet y la obtención de pruebas para procesos judiciales. Aún más inquietante es que los productos podrían desarrollarse y configurarse para permitir la censura y las restricciones de contenidos a nivel de chip. Aunque las industrias están en el punto de mira de las presiones para restringir la libertad, también disponen de más conocimientos y están en una posición muy ventajosa para eludir dichas presiones.

La rápida respuesta de la industria a las múltiples amenazas a la seguridad de las TIC y a la información que generan, transmiten, reciben y almacenan, constituye una salvaguarda básica para la libertad de los individuos e instituciones en la utilización a voluntad de la información digital. Esta libertad implica la confianza del usuario final en la propiedad[214], los derechos de usuario[215], la credibilidad[216] y la privacidad de

---

214 Los [supuestos] propietarios de la información a menudo piden la protección de sus derechos frente a la difusión y utilización de la misma. El propietario puede fijar los criterios o incluso el control del acceso a la información. Esos criterios pueden incluir el derecho a una ulterior difusión por el usuario autorizado (u organización usuaria). Dicho control es la forma de llevar a la práctica la seguridad de la información del Estado, la información que tiene propietario y la información confidencial de carácter personal. Los ataques oblicuos o indirectos [y legalistas] sobre los derechos de propiedad pueden reducir la utilidad de la información hasta el punto de que deje de tener valor.

215 El propietario de la información puede fijar los criterios de uso o incluso controlar el acceso a la misma. Ese control es normal cuando se considera que la información es propiedad intelectual legalmente protegida.

216 El usuario de los datos debería (y puede ser requerido legalmente a ello) evaluar (y quizás documentar) su nivel de confianza en quien genera los datos, en la fuente (proveedor) y en las incertidumbres sobre el contenido de los datos (tales como mediciones, registros de transacciones, estadísticas, etc.). Los ataques a la credibilidad de la información persiguen reducir la utilidad de los datos y minar la confianza en la competencia de las partes (e instituciones) que utilizan los datos por parte de las partes interesadas.

los datos[217]. Algunos también incluyen en esa lista la capacidad de eliminar datos de Internet y las salvaguardas jurídicas frente a la coacción para revelar contraseñas de sitios personales, salvo que exista una orden judicial. Las amenazas a la libertad de uso provienen de una amplia variedad de actores, desde piratas informáticos que actúan en solitario hasta bandas criminales y grupos patrocinados por un Estado.

Garantizar la libertad personal en una infraestructura de Internet resiliente y segura no es algo que se logre sin esfuerzos. Deben adoptarse medidas reales que equilibren los intereses del Estado y los intereses individuales y del sector privado, al tiempo que se protege a los usuarios frente a agentes maliciosos. La naturaleza de las actuaciones del Estado pueden tomar diferentes formas en distintas sociedades.

En los países occidentales es previsible una dependencia básica respecto al control judicial, ya sea confidencial[218] o no, a fin de tener un dictamen de cada caso individual en lugar de autorizaciones en masa a los agentes del orden y a las agencias de inteligencia. La participación activa de la industria, tanto fabricantes de hardware como diseñadores de software, ofrecería mayores niveles de seguridad y privacidad a los usuarios. De manera concertada, los proveedores de servicios de Internet podrían gestionar confidencialmente la recopilación y almacenamiento de datos de usuarios para que los gobiernos puedan acceder a los mismos sólo bajo condiciones claras y transparentes. Debería aplicarse alguna regla de proporcionalidad, cesar la vehemencia sin límites de la intrusión y recopilación de datos de los gobiernos, desarrollar la cooperación intergubernamental para establecer condiciones relativas al espionaje a aliados y desarrollar acuerdos como el marco de puerto seguro[219] ("Safe Harbour Framework"). El marco jurídico finalmente aplicable debe ser el resultado de una legislación integral, un debate público abierto y la consulta a aliados y organismos internacionales.

---

217 Es de especial preocupación para las personas en caso de información de identificación personal concreta.

218 Como los tribunales de Vigilancia de Inteligencia Extranjera (FISA) de los EE.UU. Las simples comisiones administrativas son insuficientes.

219 https://safeharbor.export.gov/list.aspx

En contraste, China ha construido una Internet nacional diferente:

> "El régimen autoritario chino no sólo ha sobrevivido a Internet, sino que el Estado ha demostrado una gran habilidad para poner la tecnología al servicio de sus intereses, aplicar un mayor control a su propia sociedad y ser un ejemplo para otros regímenes represivos. El partido-Estado de China ha desplegado un ejército de ciberpolicías, ingenieros de hardware, desarrolladores de software, supervisores de la web y propagandistas en línea a sueldo para supervisar, filtrar, censurar y guiar a los usuarios de Internet en China. Se ha permitido el desarrollo y crecimiento de compañías chinas privadas de Internet, muchas de ellas clones de otras occidentales, siempre y cuando no se desvíen de la línea del partido […]
>
> La Internet china se parece a un recinto vallado con guardas paternalistas. Al igual que la Internet que se disfruta en el resto del mundo, es desordenada e indisciplinada, ofrece entretenimiento, juegos, compras y mucho más. Permitir el desarrollo exitoso de una Internet china diferenciada ha sido parte de un plan para construir una jaula mejor, pero permanentemente observada y manipulada"[220].

La venta de tecnología en Asia Central y el Sureste asiático, en el Este de Europa y en África, permite a China ganar aliados en su disputa con Estados Unidos y Europa sobre la gobernanza de Internet. Probablemente el resultado de esta disputa establecerá los límites de la libertad en Internet a escala mundial.

220 "China's Internet: A giant cage," The Economist, 6 de abril de 2013.

Abreviaturas

AFACT	Consejo de Asia-Pacífico para la Facilitación del Comercio y del Comercio Electrónico (*Asia Pacific Council for Trade Facilitation and Electronic Business*)
AGNU	Asamblea General de las Naciones Unidas
APS	Sociedad Americana de Física (*American Physical Society*)
ARPANET	*Advanced Research Projects Agency Network*
ASEAN	Asociación de Naciones del Sudeste Asiático (*Association of Southeast Asian Nations*)
CAPTEL	Centro sobre Legislación y Política Tecnológica de Asia-Pacífico (*Centre for Asia Pacific Technology Law and Policy*)
CBMs	Medidas de fomento de la confianza (*confidence-building measures*)
CCDCOE	Centro de Excelencia para la Ciberdefensa Cooperativa (*Cooperative Cyber Defence Centre of Excellence*)
CEI	Comisión Electrotécnica Internacional
CERN	Organización Europea de Investigación Nuclear (*Conseil Européen pour la Recherche Nucléaire*)
CERT	Equipo de intervención en caso de emergencia informática (*computer emergency readiness team*)
CESPAO	Comisión Económica y Social para Asia Occidental de las Naciones Unidas
CESPAP	Comisión Económica y Social para Asia y el Pacífico de las Naciones Unidas
CIA	Confidencialidad, integridad y disponibilidad (*confidentiality, integrity and availability*)
CIRT	Equipo encargado de los incidentes informáticos (*computer incident response team*)
CMSI	Cumbre Mundial de la Sociedad de la Información
CoE	Consejo de Europa (*Council of Europe*)

COP	Iniciativa de Protección de la Infancia en Línea de la UIT (*Child Online Protection Initiative*)
CSCE	Organización para la Seguridad y la Cooperación en Europa (*Commission on Security and Cooperation in Europe*)
DUDH	Declaración Universal de los Derechos Humanos
EAU	Emiratos Árabes Unidos
EC3	Centro Europeo de Ciberdelincuencia (*European Cybercrime Centre*) (Europol)
EEAS	Servicio Europeo de Acción Exterior (Unión Europea)
ENISA	Agencia Europea de Seguridad de las Redes y la Información (*European Network and Information Security Agency*)
EPFL	Escuela Politécnica Federal de Lausana (*Ecole Polytechnique Fédérale de Lausanne*)
EUROPOL	Oficina Europea de Policía (*European Police Office*)
FBI	Oficina Federal de Investigación (*Federal Bureau of Investigation*)
G8	Grupo de los Ocho (*Group of Eight*)
GCA	Agenda sobre Ciberseguridad Global (UIT) (*Global Cybersecurity Agenda*)
GDPR	Regulación general sobre la protección de datos (*General Data Protection Regulation*)
GGE	Grupo de expertos gubernamentales (*Group of Governmental Experts*)
GNI	Iniciativa de Red Mundial (*Global Network Initiative*)
GNUD	Grupo de las Naciones Unidas para el Desarrollo
GPS	Sistema mundial de determinación de posición (*Global Positioning System*)
HLCM	Comité de Alto Nivel sobre Gestión (*High-Level Committee on Management*)
HLCP	Comité de Alto Nivel sobre Programas (*High-Level Committee on Programmes*)

HLEG	Grupo de Expertos de Alto Nivel (*High-Level Experts Group*)
HRC	Comité de Derechos Humanos (*Human Rights Committee*)
ICANN	Corporación de Internet para la Asignación de Nombres y Números (*Internet Corporation for Assigned Names and Numbers*)
ICSC	Centro Internacional para la Cultura Científica (*International Centre for Scientific Culture*)
IGF	Foro para la Gobernanza de Internet (*Internet Governance Forum)*
IMPACT	Alianza Internacional Multilateral contra las Ciberamenazas (Malasia) (*International Multilateral Partnership Against Cyber Threats*)
INDECT	Sistema de información inteligente para la observación, búsqueda y detección con fines de seguridad de ciudadanos en entornos urbanos
IP	Protocolo de Internet (*Internet protocol*)
ISF	Foro sobre la Seguridad de la Información (*Information Security Forum*)
ISO	Organización Internacional de Normalización (*International Organization for Standardization*)
ISP	Proveedor de servicio de Internet (*Internet Service Provider*)
ITIS	Instituto de Sistemas Inteligentes (*Institute for Intelligent Systems*)
ITU HLEG	Grupo de Expertos de Alto Nivel de la UIT (*High-Level Experts Group*)
JJE	Junta de los Jefes Ejecutivos (*CEB – Chief Executives Board*)
LDC	Países menos desarrollados (*Least Developed Countries*)
LINC	Centro de Internet del Líbano (*Lebanese Internet Center*)
LITA	Asociación Libanesa de Tecnologías de la Información (*Lebanese Information Technologies Association*)
MAC	Control de acceso obligatorio (*mandatory access control*)
MIT	Instituto de Tecnología de Massachusetts
NIS	Seguridad de la red y de los sistemas de información (*network and information system security*)

NSA	Agencia de Seguridad Nacional (*National Security Agency*)
NU	Naciones Unidas
OIEA	Organismo Internacional de Energía Atómica
OMPI	Organización Mundial de la Propiedad Intelectual
OSCE	Organización para la Seguridad y la Cooperación en Europa (*Organization for Security and Cooperation in Europe*)
OTAN	Organización del Tratado del Atlántico Norte
PDA	Asistente digital personal (*Personal Digital assistant*)
PGP	Sistema de encriptación (*Pretty Good Privacy*)
PMP	Panel Permanente de Supervisión sobre la Seguridad de la Información (perteneciente al Foro Mundial de Científicos)
PNUD	Programa de las Naciones Unidas para el Desarrollo
RFID	Identificación por radiofrecuencia
SaaS	Software como servicio (*Software as a Service*)
SAFE Code	Foro de garantía del software para la excelencia de la codificación (*Software Assurance Forum for Excellence in Code*)
SCADA	Control de supervisión y adquisición de datos
SIL	Nivel de seguridad integrada (*Safety Integrated Level*)
SLA	Acuerdo de nivel de servicio (*Service Level Agreement*)
SMAC	Redes sociales, móvil, análisis de datos y nube (*Social, Mobile, Analytics and Cloud*)
SOA	Arquitectura orientada a servicios (*Service Oriented Architecture*)
SORM	Sistema para Actividades Operativas de Investigación (Rusia) (*System for Operative Investigative Activities*)
TCP	Protocolo de control de transmisión (*Transmission Control Protocol*)
TI	Tecnología de la Información

TIC	Tecnología de la Información y la Comunicación
UCLA	Universidad de California (Los Ángeles)
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones
UN CEFACT	Centro de las Naciones Unidas para la Facilitación del Comercio y del Comercio Electrónico (en el marco del UNECE)
UNCTAD	Conferencia de las Naciones Unidas sobre Comercio y Desarrollo
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
UNGGE	Grupo de las Naciones Unidas de Expertos Gubernamentales
UNIDIR	Instituto de las Naciones Unidas de Investigación para el Desarme
UNODC	Oficina de las Naciones Unidas contra la Droga y el Delito
US-CERT	Equipo de intervención en caso de emergencia informática de los Estados Unidos de América (*United States Computer Emergency Readiness Team*)
WFS	Federación Mundial de Científicos (*World Federation of Scientists*)
WMD	Armas de destrucción masiva (*Weapon of Mass Destruction*)

Contacto:
Unión Internacional de Telecomunicaciones
Place des Nations
CH-1211 Ginebra 20
Suiza
Correo electrónico: cybersecurity@itu.int
Sitio web: www.itu.int/cybersecurity

ISBN: 978-92-61-15303-8

Impreso en Suiza
Ginebra, 2014

11/2014