ppi 201502ZU4644
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN 1315-6268 / Depósito legal pp 199402ZU33

Frónesis

Revista de Filosofía Jurídica, Social y Política

Vol. 22, No. 2
Mayo - Agosto de 2015

Περὶ δὲ φρονήσεώς... λείπεται... αὐτὴν εἶναι ἕξιν ἀληθῆ μετὰ λόγου πρακτικὴν περὶ τὰ ἀνθρώπῳ ἀγαθὰ καὶ κακά.

Universidad del Zulia
Facultad de Ciencias Jurídicas y Políticas
Instituto de Filosofía del Derecho "Dr. José Manuel Delgado Ocando"

Scriptorium
La ciberseguridad: una asignatura pendiente en la sociedad de la información

Gladys Stella Rodríguez
Instituto de Filosofía del Derecho
Sección de informática jurídica y Derecho informático
Universidad del Zulia
Maracaibo - Venezuela
gr1970ve@yahoo.es

La Unión Internacional de Telecomunicaciones ha informado en mayo de 2015, que de las 940 millones de personas que habitan los países menos desarrollados, sólo 89 millones están conectadas. El organismo internacional ha señalado que más de 3 millardos de personas en el mundo usan actualmente Internet, sin embargo, otras 4 millardos que residen en los países más pobres del planeta siguen sin estar conectadas.

Estas 4 millardos de personas representan dos terceras partes de la población que reside en los países en desarrollo, y no tienen perspectivas a corto plazo para poder tener acceso a las nuevas tecnologías de la información (TIC en adelante).De hecho, de los 940 millones de personas que viven en los Países Menos Desarrollados sólo 89 millones usan Internet, lo que indica una penetración de tan solo 9,5%.

No obstante, la proporción de hogares que tienen acceso a Internet pasó de un 18% en 2005 a un 46% en 2015. (1)Actualmente hay más de 7 millardos de líneas de móvil en el mundo, cuando en el año 2000 eran solo 738 millones.

Bajo este contexto en los países se ha iniciado una serie de medidas, esto es legislaciones en materia de terrorismo, ciberdelincuencia, la creación de organismos de certificación electrónica y resguardo frente a posibles ataques cibernéticos bien hacia

sus ciudadanos o contra la misma soberanía de los Estados cuando se accede a los sistemas de información, redes o alas infraestructuras de comunicación en general.

Hoy más que nunca se está asistiendo a una concienciación creciente de la necesidad de controlar los riesgos informáticos operacionales debido a la utilización extensiva de las nuevas tecnologías, a la existencia de una infraestructura de información mundial y a la aparición de nuevos riesgos. Además, también es cierto que la transformación de las sociedades en sociedades de la información, gracias a la integración de nuevas tecnologías en todas sus actividades e infraestructuras, aumenta la dependencia de los individuos, de las organizaciones y de los Estados, de los sistemas de información y de las redes. Esto constituye un riesgo de primer orden que debe contemplarse inclusive como un riesgo de seguridad.

Sin embargo, los países en desarrollo se enfrentan a la necesidad de formar parte de la sociedad de la información asumiendo el riesgo de su dependencia de las tecnologías y de los proveedores de las mismas intentando que la brecha digital existente no dé lugar a una brecha de seguridad y menos aún a una dependencia más estrecha de entidades que controlen sus necesidades y los medios de seguridad de las tecnologías de la información (2).

En consecuencia, las infraestructuras de telecomunicaciones y los servicios y actividades que éstas permiten desarrollar y generar, deben plantearse, concebirse, instalarse y administrarse en términos de seguridad. La seguridad es la piedra angular de toda actividad y debe contemplarse como un servicio que permite crear otros y generar valor añadido (cibergobierno, cibersalud, ciberenseñanza, etc.) con independencia de las tecnologías (3). No obstante, hasta el momento, las herramientas básicas de comunicación disponibles no cuentan con los medios suficientes ni necesarios para establecer o garantizar un nivel mínimo de seguridad.

Los sistemas informáticos conectados en red son recursos accesibles a distancia y blancos potenciales de ataques informáticos. Esto incrementa los riesgos de intrusión en los sistemas y ofrece un terreno favorable para la realización y propagación de ataques y delitos. Los ataques pueden afectar a la capacidad de tratamiento, salvaguarda y comunicación del capital de información, de los valores y materiales y de los símbolos, y al proceso de producción o de decisión de los que los poseen. Así pues, las redes de telecomunicaciones y la apertura de los sistemas plantean problemas de seguridad informática, complejos y multiformes, que son relativamente difíciles de controlar y que pueden tener consecuencias y repercusiones críticas sobre el funcionamiento de las organizaciones y de los Estados. De la capacidad de controlar la seguridad de las informaciones, de los procesos, de los sistemas, y de las infraestructuras dependen los factores críticos de éxito de las economías.

La interconexión extensiva de sistemas, la interdependencia de las infraestructuras, el aumento de la dependencia de las tecnologías digitales, las amenazas y los riesgos, exigen dotar a los individuos, las organizaciones y los Estados de medidas, procedimientos y herramientas que permitan mejorar la gestión de los riesgos tecnológicos y de la información. Así surge la denominada ciberseguridad. Los retos del dominio de los riesgos tecnológicos son propios del siglo XXI y exigen un planteamiento global a nivel internacional y su integración en el proceso de la seguridad de los países en desarrollo.

No basta con establecer puntos de acceso a las redes de telecomunicación, es indispensable desplegar infraestructuras y servicios informáticos fiables, susceptibles de mantenimiento, robustos y seguros, para respetar los derechos fundamentales de las personas y de los Estados. La protección de los sistemas y de la información de valor debe complementarse y armonizarse con la protección de los individuos y de su intimidad digital (privacidad).

La entrada en la sociedad de la información sin un riesgo excesivo y aprovechando las experiencias obtenidas de los países en desarrollo, sin que la ciberseguridad se convierta en un factor adicional de exclusión, constituye un nuevos reto para los países en desarrollo.

Se ha afirmado que el tema de la ciberseguridad es fundamental para sustentar un modelo tecnológicamente coherente. Las perturbaciones del tendido eléctrico o los problemas causados a los sistemas financieros por injerencias en las redes de las TIC son muy concretos y constituyen amenazas para la seguridad nacional. Las personas malintencionadas en línea son numerosas, están bien organizadas y son muy diversas van desde organizaciones políticas, delincuentes, terroristas o *hacktivistas*. Recientemente (Navarro, 2015) (4), ha asegurado que Internet es "la gran arma" del terrorismo *yihadista*y abogó por la cooperación internacional en la lucha contra el terrorismo de inspiración *yihadista*. Agrega Navarro, 2015, "existen más de 30.000 páginas *yihadistas* que hoy circulan por la red, por lo que argumentó que los estados democráticos deben buscar una "respuesta congruente" con las nuevas amenazas. Éstos grupos mal intencionados disponen de herramientas cada vez más sofisticadas y complejas, y adquieren experiencia con el tiempo; el número creciente de plataformas conectadas no hace más que ofrecerles nuevos vectores de ataque. Es imposible volver a los tiempos primitivos, razón por la cual la ciberseguridad debe formar parte integrante e indivisible del progreso tecnológico.

Lamentablemente, afirman (ABI Research y la Unión Internacional de Telecomunicaciones, 2014), que la ciberseguridad todavía no se considera esencial en muchas estrategias tecnológicas nacionales e industriales. Los esfuerzos para aumentar

la ciberseguridad son numerosos pero eclécticos y dispersos. Las disparidades en la penetración de Internet, el desarrollo tecnológico, el dinamismo del sector privado o las estrategias públicas significan que la ciberseguridad evoluciona de lo particular a lo general, lo que es natural cuando existen esas disparidades entre Estados, sector público y privado e incluso sectores industriales. Ahora bien, una cultura mundial de la ciberseguridad tendría más éxito en esencia si evolucionara de lo general a lo particular. La divulgación de información y la cooperación son fundamentales para afrontar las amenazas internacionales

Y precisamente frente a ello, surge la solicitud hecha por el Secretario de la UNCTAD (5)para conocer las tendencias, los logros y obstáculos de la aplicación de los resultados de la Cumbre Mundial sobre Sociedad de la Información (CMSI en adelante), que necesariamente inciden sobre el tema de la ciberseguridad y, los cuales se describen a continuación:

a. Oportunidades en el ámbito digital y brecha digital

Si bien por una parte, la adopción y el uso de las TIC en los países desarrollados y en desarrollo no han dejado de ir en aumento. Según los datos ofrecido tanto por la UIT y los publicados por la Asociación para la Medición de las TIC para el Desarrollo en su "Examen Final de los Resultados de la CMSI" *Final WSIS Targets Review,* muestran que más del 90% de la población mundial tiene actualmente cobertura de redes de telefonía móvil. Según las estimaciones, casi el 50% de la población mundial tiene algún abono de telefonía, mientras que el 44% de los hogares tiene acceso a Internet y el 39% de la población utiliza Internet. Según la Asociación, el objetivo de la CMSI de que más de la mitad de los habitantes del planeta tenga acceso a las TIC y las utilice se logrará para fines de 2016 (6)

Sin embargo, los datos publicados tanto por la UIT como por la Asociación también muestran que siguen existiendo brechas digitales entre los países desarrollados y en desarrollo, entre los cuales se encuentra Venezuela y la Región de América Latina. Mientras que el 78% de los hogares de los países desarrollados tienen acceso a Internet, en los países menos adelantados solo el 5% lo tienen. Las conexiones de banda ancha fijas y móviles son mucho más accesibles, y más asequibles, en los países desarrollados que en los países en desarrollo. En las zonas rurales de muchos países todavía hay escaso acceso de banda ancha. En consecuencia, existe el riesgo de que aumenten las brechas digitales y de que los países en desarrollo, en particular los países menos adelantados, no puedan aprovechar plenamente los beneficios de la sociedad de la información (7)

b. Evolución de Internet

La tecnología, los servicios y la gobernanza de Internet siguen experimentando rápidos cambios. Las redes sociales y los servicios interactivos en la web han ampliado su implantación en la sociedad, de manera que los usuarios pueden publicar opiniones y acceder a más contenidos. En el tráfico de Internet predominan cada vez más los contenidos de vídeo y la transferencia de datos y aplicaciones de los equipos de los usuarios a la nube. Pero ello trae a debate lo referente a la privacidad y la vigilancia de los contenidos en línea, temas fundamentales de la ciberseguridad.

Se han celebrado debates sobre el futuro de la gobernanza de Internet en las Naciones Unidas y otros foros, como el Foro para la Gobernanza de Internet y la Conferencia de Plenipotenciarios de la UIT. La Asamblea General observó que Brasil había acogido NETmundial, la Reunión Global de Múltiples Partes Interesadas sobre el Futuro de la Gobernanza de Internet, en abril de 2014 (8).

La UNESCO puso en marcha un estudio exhaustivo sobre cuestiones relacionadas con Internet, cuyos resultados se darán a conocer en su Conferencia General en 2015 (9). El Banco Mundial está preparando su "Informe sobre el Desarrollo Mundial" de 2016 en torno al tema de Internet para el desarrollo (10).

c. Rápida evolución de la tecnología, los servicios y las aplicaciones

La rápida evolución de las TIC hace que surjan continuamente nuevos servicios y nuevas oportunidades de aplicaciones para el desarrollo. Se ha estimado que la capacidad de las redes y servicios de TIC es ahora 30 veces mayor que cuando se celebró la última CMSI, y que seguirá aumentando con la misma rapidez (11).

Cuatro acontecimientos en particular están influyendo de manera considerable en los gobiernos, las empresas y los consumidores. La aparición de los teléfonos inteligentes y las tabletas ha desplazado la computación individual y organizativa a dispositivos móviles más flexibles. Las personas, las empresas y los gobiernos están transfiriendo sus datos y aplicaciones a la nube y a servicios basados en la nube. La datificación de la actividad gubernamental y empresarial y los recursos de gestión de datos en nube permiten un uso más generalizado del análisis de macrodatos y de los datos abiertos. La aparición de la "Internet de las cosas", que conecta dispositivos y personas a Internet, aumentará considerablemente los datos disponibles para mejorar las oportunidades de desarrollo (12), pero también hace que los Estados y sus ciudadanos estén más expuestos a fraude, acceso indebido o sabotaje informático.

Estos acontecimientos también plantean importantes desafíos. El aumento del tráfico de datos ejerce presión sobre el espectro radioeléctrico y refuerza la necesidad de una transición hacia lo que la UIT llama nuevos paradigmas de la reglamentación, una "reglamentación de cuarta generación" que responda a la reciente evolución dinámica de las TIC y los mercados (13). Se requieren cambios en la legislación nacional y el comercio internacional para dar cabida a las transacciones electrónicas y prepararse para otras innovaciones, mientras que la datificación y la computación en nube suscitan preocupación en relación con la protección de los datos, la privacidad y la soberanía de los datos, tópicos que la ciberseguridad demanda.

d. La sociedad de la información y la agenda para el desarrollo después de 2015

Las TIC han llegado para quedarse y lo cierto es que la evolución de la sociedad de la información influirá cada vez más en el desarrollo social y económico durante la aplicación de la agenda para el desarrollo después de 2015. En los documentos finales del Evento de Alto Nivel CMSI+10 se destacó la importancia de aprovechar el valor potencial de las TIC para el desarrollo y de tener en cuenta el avance de la sociedad de la información incluyente en el contexto más amplio de la agenda para el desarrollo después de 2015. En su resolución 69/204, de 19 de diciembre de 2014, la Asamblea General destacó la necesidad de aprovechar el potencial de las TIC como vector clave del desarrollo sostenible y de tener en cuenta el desarrollo de la capacidad para su uso productivo al elaborar la agenda para el desarrollo después de 2015.

Por su parte la región latinoamericana no es ajena a este fenómeno tecnológico, en el Plan de Trabajo 2013-2015 para la implementación del plan de acción sobre la sociedad de la información y del conocimiento para América Latina y el Caribe (ELAC2015), se exponen un conjunto de temas considerados emergentes o que revisten importancia para el desarrollo digital de la región y, por lo tanto, deberían dar origen a iniciativas de cooperación regional en el marco del eLAC2015. Entre ellos está: Incentivar el uso de las nuevas tecnologías en ámbitos de seguridad pública y Promover la cooperación en materia de ciberseguridad y de protección en infraestructuras críticas con miras a lograr su sostenibilidad y proteger a los usuarios.

Como se aprecia la tecnología es vista como la última maravilla del mundo capaz de resolver todos los problemas, pero para los países latinoamericanos le es ajena, pues es el producto de los países altamente industrializados. Para que las TIC sean un autentica clave para el desarrollo, ha de incorporarse y adaptarse a las condiciones propias de estos países menos desarrollados, de lo contrario se quedaría en un mundo mágico e intangible (14)

Notas:

1. (Disponible en http://www.elnacional.com/tecnologia/millardos-personas-mundo-acceso-Internet_0_635336505.html Consultado 20-05-2015)
2. S. Ghernaouti-Hélie: «From digital divide to digital unsecurity: challenges to developp and deploy a unified e-security framework in a multidimensional context». International cooperation and theInformationSociety, Capítulo del Anuario Suizo de Política de Desarrollo. Iuéd publications.Ginebra, Noviembre de 2003.
3. A. Ntoko: «Mandate and activities in cybersecurity – ITU-D». Reunión temática de la CMSI sobre ciberseguridad. UIT − Ginebra, 28 de junio a 1 de julio de 2005
4. Presidente de la Audiencia Nacional española José Ramón Navarro Disponible en https://es- us.noticias.yahoo.com/magistrado-espa%C3%B1ol-alerta-internet-arma-yihadism 174600225.html. Consultado 20-05-2015
5. En el marco de la Asamblea General en su Septuagésimo período de sesiones, sobre Tema 17 de la lista preliminar* Las tecnologías de la información y las comunicaciones para el desarrollo, en cumplimiento de la resolución 2006/46 del Consejo Económico y Social. Período de sesiones de 2015 de fecha 21 de julio de 2014 a 22 de julio de 2015 Tema 18 b) del programa provisional** Cuestiones económicas y ambientales: Ciencia y tecnología para el desarrollo. Informe Progresos realizados en la aplicación y el seguimiento de los resultados de la Cumbre Mundial sobre la Sociedad de la Información a nivel regional e internacional.
6. Disponible en http://www.itu.int/en/ITU-D/Statistics/Documents/publications/wsisreview2014/WSIS2014_review.pdf. Consultado 22-02-2015
7. Disponible en http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf. Consultado 22-04-2015
8. A/RES/69/204 Disponible en http://netmundial.br/. Consultado 22-04-2015
9. Disponible en http://www.unesco.org/new/en/internetstudy. Consultada 23-05-2015
10. Disponible en http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTRESEARCH/EXTWDRS5~pagePK:8258258~piPK:8258412~theSitePK:8258025,00.html Consultado 23-05-2015
11. Disponible en http://unctad.org/meetings/en/SessionalDocuments/ecn162014d3_en.pdf. Consultado 23-05-2015

12. Disponible en http://unctad.org/meetings/en/SessionalDocuments/ecn162014d3_en.pdf. Consultado 23-05-2015

13. Disponible en http://www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.15-2014-PDF-S.pdf. Consultado 22-04-2015

14. Rodríguez, G y Bozo, A (1999) "Algunas reflexiones filosóficas sobre la tecnología moderna". En ***FRONESIS***, Vol. 6, No. 2 Agosto 1999. 39-57

UNIVERSIDAD
DEL ZULIA

Frónesis
Revista de Filosofía Jurídica, Social y Política.
Vol.22 Nº2 (2015) _____

Esta revista fue editada en formato digital y publicada en agosto de 2015, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
produccioncientifica.luz.edu.ve