Políticas de información: de lo instrumental a lo informacional

Egbert John Sánchez Vanderkast
COORDINADOR

Publicación conmemorativa del X Aniversario del Instituto de Investigaciones Bibliotecológicas y de la Información: "A 40 años de investigación en Bibliotecología e Información en la UNAM"

Diseño de portada: Mario Ocampo Chávez

Primera edición: octubre de 2023

Instituto de Investigaciones Bibliotecológicas y de la Información
Circuito Interior s/n, Torre II de Humanidades,
pisos 11, 12 y 13, Ciudad Universitaria, C. P. 04510,
Alcaldía Coyoacán, Ciudad de México

Impreso y hecho en México

Contenido

Políticas de información en ciberseguridad en México: atención y tratamiento a conductas disvalorativas en red

Rosa Amelia Domínguez Arteaga
El Colegio de Tamaulipas, México

Introducción

Las políticas de información (PI) son una guía que orienta a las estrategias relacionadas con el uso de la información en un determinado lugar y con lo que esto conlleva. Lo anterior implica que los sistemas o servicios en los cuales este recurso sea el eje central deben estar seguros y, con ello, dar certeza sobre el derecho a la información. Por lo tanto, es necesario que dichas garantías sean válidas para el ejercicio libre y pleno de tal jurisprudencia en el entorno digital, principalmente a los más vulnerables.

En el periodo de contingencia sanitaria provocada por la COVID-19, el uso de las Tecnologías de la Información y la Comunicación (TIC) se generalizó incluso para actividades esenciales. Este hecho puso en riesgo la integridad e incluso la vida de las personas, pues en los últimos años los ciberdelitos han aumentado en todo el mundo. Al respecto, el Banco Interamericano de Desarrollo refiere que este contexto ha mostrado las vulnerabilidades del ciberespacio de América Latina y el Caribe.[1]

1 Banco Interamericano de Desarrollo - Organización de los Estados Americanos (BID - OEA), *Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y El Caribe. Reporte Ciberseguridad*, 2020. file:///C:/Users/Usuario%20Final/Downloads/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Desde este enfoque, el cibercrimen provoca afectaciones económicas de hasta el 1% del Producto Interno Bruto (PIB) en algunas naciones.[2] Es preciso resaltar que el principal ciberdelito tiene que ver con la instalación indebida de *software* para infectar servidores web de información financiera (*formjacking*).[3] Por su parte, el estudio y análisis de los ciberdelitos no despierta mucho interés entre los investigadores, lo que provoca que el abordaje de este tipo de infracciones sea escaso como objeto de estudio.[4]

Una situación similar se ha venido presentando con la investigación sobre las PI,[5] incluyendo aquellas que contemplen la seguridad de la información. Y es que el tema de los ciberdelitos y sus consecuencias es registrado más por consultorías que por especialistas en la materia, lo cual repercute en las consideraciones que la ciencia podría aportar a la temática. Esto se hace todavía más visible a través de un análisis profundo de lo sucedido en ambientes de contingencia social, principalmente en un país como México, que posee altos niveles de ciberdelitos.

Por lo tanto, debido a la expansión del cibercrimen, esta investigación busca exponer la importancia de las PI en ciberseguridad. El estudio describe la situación en México de los llamados *ciberdelitos* en el transcurso de la pandemia y, además, se detallan los mecanismos existentes para la atención de este problema. En la indagación, se realizó un análisis sistemático de datos ofrecidos por las dependencias encargadas de la atención de los ciberdelitos que sirvan de base para el rediseño de PI en ciberseguridad en el territorio.

En un primer momento, se caracteriza lo sucedido en México respecto a los ciberdelitos en el contexto de la pandemia, así como las políticas para la atención de estas faltas. Después, se establece el desarrollo de las PI en ciberseguridad y su lugar en los estudios de dicho campo. Se termina con una reflexión acerca de la relevancia de incorporar estas iniciativas en la agenda política, de cara al aumento del cibercrimen en el mundo.

2 *Idem*.

3 Symantec, Internet Security Threat Report, 24, February 2019. http://latixns.mx/wp-content/uploads/2019/03/ Internet-Security-Threat-Report-20190314.pdf

4 Martín Pecoy, "Delito en el comercio electrónico". *Prisma Jurídico*, 10, núm. 1 (2011), 209-224.

5 Egbert John Sánchez Vanderkast, "Políticas de información: el amplio espectro de la investigación". *Investigación bibliotecológica: archivonomía, bibliotecología e información*, 9, núm. 38 (2005), 97-117.

Desarrollo

Los ciberdelitos en México durante la pandemia

Para Acosta *et al*., los ciberdelitos son "actos ilícitos cometidos mediante el uso inadecuado de la tecnología, atentando contra la privacidad de la información de terceras personas, dañando o extrayendo cualquier tipo de datos que se encuentren almacenados en servidores o gadgets."[6] Asimismo, para algunos autores, con este tipo de sucesos se atenta contra atribuciones y se restringen derechos y libertades fundamentales.[7] En este trabajo, los ciberdelitos son considerados conductas disvalorativas realizadas a través y con las TIC para perpetrar un daño, sea material o moral, a los usuarios de estas tecnologías.

A la fecha, se ha llegado a clasificar a la ciberdelincuencia como económica e intrusiva. Esta última atentaría contra la moral y la dignidad de las personas.[8] No obstante, el principal ciberdelito documentado en la actualidad es el fraude cometido en internet, el cual genera grandes pérdidas económicas. La carga onerosa derivada de éste y otros ataques cibernéticos podría superar el 1% del PIB en el mundo. Por su parte, en México, los ciberdelitos también generan grandes afectaciones económicas.[9] Se señala que el país se posiciona entre las naciones que registra más pérdidas provocadas por el cibercrimen, junto con Estados Unidos, Brasil y China.[10] Además, México fue uno de los cinco países

6 María Gabriela Acosta *et al*., "Delitos informáticos: impunidad organizacional y su complejidad en el mundo de los negocios". *Revista Venezolana de Gerencia*, 25, núm. 89 (2020), 18. www.redalyc.org/articulo.oa?id=29062641023

7 Hiram Piña, "Cibercriminalidad y ciberseguridad en México". *Ius Comitialis*, 2, núm. 4 (2019), 47-69. doi:10.36677/iuscomitialis. v2i4.13203.

8 Josefina Quevedo González, "Investigación y prueba del ciberdelito" [Tesis. Programa de Doctorado en Derecho y Ciencia Política]. (Barcelona: Universitat de Barcelona, 2017). https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1

9 Secretaría de Hacienda y Crédito Público - Consejo Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (SHCP - CONDUSEF), Portal de Fraudes Financieros en México, 2018. https://www.condusef.gob.mx/documentos/prensa/400983_PORTAL_DE_FRAUDES_FINANCIEROS_vers7.pdf

10 María González, "La cibercriminalidad como instrumento para la expansión y empoderamiento del crimen organizado". *Análisis GESI (Grupo de Estudios sobre Seguridad Internacional*), núm. 46 (2017). https://www.seguridadinternacional.es/?q=es/content/la-cibercriminalidad-como-instrumento-para-la-expansi%C3%B3n-y-empoderamiento-del-crimen

de América Latina que, en 2018, recibió más ataques *ransomware* (infección de sistemas informáticos mediante virus que bloquean una computadora).[11]

Ahora bien, ¿qué pasó con los ciberdelitos durante la pandemia en México? ¿Con qué políticas de información sobre ciberseguridad cuenta el país para atacar la problemática, mayoritariamente en etapa de alarma mundial? Según lo investigado en este trabajo, los ataques cibernéticos durante el confinamiento fueron variados. Un primer ejemplo fue la estafa a familiares de pacientes de COVID-19 mediante la venta de oxígeno para atender la emergencia de salud en las familias afectadas.[12]

Se agrega a lo expuesto la suplantación de identidad, incluso en las campañas de vacunación contra el SARS-COV-2 dirigida a adultos mayores.[13] Para ello, los delincuentes utilizaron enlaces electrónicos falsos de instituciones de gobierno para cometer fraude. En este caso, la conducta disvalorativa se basó en el diseño de un sitio web para el registro de datos de personas de este grupo poblacional que requería intervención médica. De acuerdo con la dependencia federal encargada de atender estos asuntos, el *link* de dicho sitio circuló por redes sociales y aplicaciones de mensajería.[14]

A la par, de acuerdo con la Unidad de Inteligencia Financiera (UIF), se presentó la venta de pruebas falsas de COVID-19 y medicamentos apócrifos para este padecimiento.[15] Junto con esta dependencia, la Comisión Nacional Bancaria y de Valores (CNBV) y el Buró Federal de Investigaciones (FBI) ubicaron fraudes electrónicos, mediante la técnica del *pishing* (envío masivo de correos

11 Cámara Colombiana de Informática y Telecomunicaciones (CCIT), *Tendencias cibercrimen Colombia 2019–2020*, 2020. https://www.ccit.org.co/wp-content/uploads/ informe-tendencias-cibercrimen_compressed-3.pdf

12 Secretaría de Seguridad Ciudadana (SSC), "La SSC a través de la Policía Cibernética, alerta a la ciudadanía a verificar los sitios de compra y venta de tanques de oxígeno en línea", 01, enero, 2021. https://www.ssc.cdmx.gob. mx/comunicacion/nota/001-la-ssc-traves-de-la-policiacibernetica-alerta-la-ciudadania-verificar-los-sitios-decompra-y-venta-de-tanques-de-oxigeno-en-linea

13 Secretaría de Seguridad Ciudadana (SSC), "La Policía Cibernética de la SSC alerta a la ciudadanía sobre fake news relacionadas con las campañas de vacunación", 25, marzo, 2021. https://www.ssc.cdmx.gob.mx/comunicacion/nota/673-la-policia-cibernetica-de-la-ssc-alerta-la-ciudadania-sobre-fake-news-relacionadas-con-las-campanas-de-vacunacion

14 *Idem*.

15 Cámara de Diputados, "Comisión de Hacienda se reúne con Santiago Nieto, titular de la UIF". Reunión virtual de la Junta Directiva de la Comisión de Hacienda y Crédito Público con Santiago Nieto, titular de la Unidad de Inteligencia Financiera, 24, abril, 2020. https://youtu.be/Mw7iZJBLmAo

electrónicos mediante *spam*), provenientes de otros países.[16] Algunos de estos fraudes se perpetraron utilizando también algunas redes sociales, donde, en nombre de la Secretaría de Bienestar Social, se aseguraba la supuesta entrega de tarjetas alimentarias por COVID-19. Para adquirirlas, los ciberdelincuentes pedían dinero a las víctimas para su aparente activación.[17]

Ahora bien, para atender la problemática y como derivación de los estudios en derecho informático en el país, se reconocen avances en políticas de información para la ciberseguridad. Por un lado, México cuenta con la Policía Cibernética, adscrita a la Dirección General Científica de la Guardia Nacional. Esta última alberga además al Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), encargado de vigilar virtualmente la infraestructura tecnológica de la nación. Por otro lado, existen esfuerzos por conformar la Estrategia Nacional de Ciberseguridad.[18] Con ella se busca lograr un uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado mexicano. Cabe mencionar que el marco legal nacional ha sufrido varias modificaciones al respecto. Existen en las entidades del país varias hipótesis jurídicas que contemplan conductas criminales en el ecosistema digital y que han sido registradas en actualidad. Además, el Código Penal Federal, en su artículo 211, presenta diversas figuras normativas aplicables a los ciberdelitos y dignas de análisis.[19]

Sin embargo, esos trabajos carecen de fuerza ante los riesgos en internet pues, según el Banco interamericano de Desarrollo, actualmente, México y otros países de América Latina poseen una preparación insuficiente para enfrentar los ataques cibernéticos.[20] Además, en relación con las leyes, algunos analistas opinan que éstas contienen complejidades de tipo epistemológico, así como de hermenéutica interpretativa. El motivo sería un desconocimiento de referentes internacionales que orientan la atención de estos actos disvalorativos, lo cual provocaría una mala gestión en su tratamiento en el país, además de una falta de actualización en la materia.[21]

16 Unidad de Inteligencia Financiera (UIF), "UIF combate los fraudes electrónicos denominados 'BEC'", ´12, noviembre, 2020. https://www.gob.mx/uif/articulos/nota-informativa-uif-combate-los-fraudes-electronicos-denominados-bec

17 Secretaría de Bienestar, "Bienestar alerta por presunto fraude con entrega de tarjetas falsas", 29, abril, 2020. https://www.gob.mx/bienestar/prensa/bienestar-alerta-por-presunto-fraude-con-entrega-de-tarjetas-falsas?state=published

18 Estrategia Nacional de Ciberseguridad (ENCS), 2017. www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

19 Hiram Piña, *op. cit*.

20 Banco Interamericano de Desarrollo - Organización de los Estados Americanos (BID - OEA), *op. cit*., 10.

21 Hiram Piña, *op. cit*.

Políticas de información sobre ciberseguridad

Las PI tienen como propósito regular el camino de la información, desde su creación hasta su comunicación. Esto conlleva el proceso de crear y poseer información de diferente índole, en distintos ámbitos. Por otro lado, las PI fueron pensadas para normar la capacidad, pero también la libertad de obtener, poseer y guardar información, así como de usarla y transmitirla. En ello, queda entendido que, a través de las PI, se persigue el alcance de condiciones idóneas para una gestión eficaz de la información en todos sus formatos y entornos.

Hoy en día, con el advenimiento de la sociedad de la información, existe más que nunca una estrecha relación entre política e información; en especial, lo concerniente a la política digital. Es bien sabido que los niveles de penetración de las tecnologías digitales en el mundo se elevaron todavía más por el confinamiento sanitario a causa del SARS-COV-2. Según la Unión Internacional de Telecomunicaciones (UIT),[22] 4 900 millones de individuos poseían una conexión a internet hacia finales de 2021, lo que representa, aproximadamente, un 63% de la población mundial.

Estos esfuerzos son resultado de una serie de políticas públicas de información implementadas por los Estados a inicios del presente milenio, como el Libro Blanco y el Informe Bangemann para la Unión Europea; la Política de Información Federal para Estados Unidos, y el Plan de Acción sobre la Sociedad de la Información de América Latina y el Caribe (eLAC) para nuestra región. El objetivo de estas iniciativas ha estado encaminado a buscar la inclusión digital, con miras a alcanzar una sociedad de la información para todos; por ello, tales propuestas se han basado mayoritariamente en el acceso a las TIC y en poner en marcha las agendas digitales como potenciadoras de una sociedad de la información y del conocimiento (SIC) como una estrategia del progreso.

Como se observa, dichas acciones podrían calificarse como exitosas. Sin embargo, una alta penetración de TIC conlleva, a la vez, una serie de implicaciones negativas. Prueba de ello son la presencia de ciberdelitos en la actualidad y el aumento de las ciberagresiones señaladas líneas arriba. Pero entonces, ¿qué ha pasado con el tópico de la ciberseguridad en el proceso de la información y el desarrollo de políticas de información al respecto? ¿Qué se puede decir el día de hoy sobre las PI en ciberseguridad?

22 Unión Internacional de Telecomunicaciones (UIT), "Inclusión digital para todos", 2022. https://www.itu.int/es/mediacentre/backgrounders/Pages/digital-inclusion-of-all.aspx

Muchos han sido los estudios que abordan las PI. Por ejemplo, Sánchez Vanderkast y Gama[23] opinan que los abordajes de las PI pueden llevarse a cabo desde distintas ópticas, visiones, fases de instrumentación o impacto en la sociedad. Esto queda demostrado en algunas investigaciones; por ejemplo, en los trabajos realizados por Rowlands[24] y Bender.[25] Rowlands[26] dividió a las PI en cinco grandes grupos para un mejor análisis: mercado de la información; radiodifusión y telecomunicaciones; acceso a la información gubernamental; sociedad de la información e infraestructura, y protección de la información.

Por su parte, Bender[27] estableció una lista de asuntos apremiantes para el análisis de las PI: tecnologías de la información; fronteras de la información; protección de datos; derechos intelectuales; industria de la información, pública y privada; información científica y técnica; telecomunicaciones; estandarización del uso de la información, y educación y formación. A pesar de estas clasificaciones, se señala que entre los estudiosos de la información el análisis de las PI, al abarcar múltiples aristas, no ha despertado mucho interés,[28] lo cual se replica en las que incluyen la seguridad de la información.

Los tópicos incluidos en las PI son muy variados, y en ellos se puede identificar la relación seguridad-información con miras a la defensa de los derechos humanos.[29] Sin embargo, según Sánchez Vanderkast[30] —en referencia a los trabajos de Frohmann y Rosenberg realizados entre los años setenta y noventa—, desde sus inicios, el estudio de PI estuvo enfocado en la conservación y la diseminación de la información científica y técnica. Esas perspectivas tenían que ver mayormente con el resguardo de datos sensibles y en formatos físicos, como los depositados en centros de documentación y bibliotecas. Asimismo, los sectores de interés para el desarrollo de éstas fueron el gubernamental y el

23 Egbert John Sánchez Vanderkast y Miguel Gama, "Tópicos de políticas de información en el entorno científico y técnico: México 1989 -1994". *Ciência da Informação*, 35, núm 3 (2006), 76.

24 Ian Rowlands, "Understanding information policy: concepts, frameworks and research tools". *Journal of information Science*, 22, núm. 1 (1996), 13-25.

25 David R. Bender, "A strategy for international information policy". *LIBRI*, 43, núm. 3 (1993), 210-231.

26 Ian Rowlands, *op. cit*.

27 David R. Bender, *op. cit*.

28 Egbert John Sánchez Vanderkast, "Políticas de información: el amplio espectro de la investigación", *op. cit*.

29 Egbert John Sánchez Vanderkast y Miguel Gama, *op. cit*.

30 Egbert John Sánchez Vanderkast, "Políticas de información: temáticas emergentes y su repercusión en la bibliotecología y los estudios de la información". Miguel Ángel Rendón Rojas (coord.). *Hacia una escuela de pensamiento iberoamericana de la ciencia de la información documental* (Ciudad de México: UNAM, Instituto de Investigaciones Bibliotecológicas y de la Información, 2020), 99-130.

económico. Posteriormente, con la intención de incursionar en la SIC, el centro de atención fue el acceso a las TIC, principalmente en temas de inclusión digital.

Como consecuencia, el enfoque de las PI fue el desarrollo digital y las telecomunicaciones. Así, el estudio de la sociedad de la información se basó particularmente en el abordaje de la brecha digital con miras a aumentar la penetración de las TIC entre los pueblos. No obstante esta atención, para algunos autores, se ha desestimado la dimensión del uso y de la apropiación de las TIC, además de escenarios como el económico, el de habilidades digitales, el del capital cultural y el político, que se interrelacionan con dicho fenómeno.[31] Por lo tanto, se puede establecer que varios aspectos de las agendas digitales integrales han pasado a segundo plano, como los riesgos que dichas acciones conllevan.

Y es que los delitos presentes en internet dan cuenta de la violencia que se vive en el uso de la información dentro del ecosistema digital. Por ejemplo, la web 2.0 hace que agresiones electrónicas como el ciberacoso (principalmente del tipo sexual) sean más crueles; esto, por el hecho de que tales prácticas se realizan mediante el uso de aplicaciones como las redes sociales digitales, que permiten la rapidez e instantaneidad de los mensajes emitidos.[32] De tal manera, la coyuntura originada por el confinamiento motivó el interés de analizar y abordar la resignificación de los consumos culturales con miras a construir "sensibilidades políticas".[33]

Para atender las problemáticas derivadas del cibercrimen, se puede hablar de un avance en la materia. Por ejemplo, el Convenio de Budapest sobre ciberdelincuencia en la Unión Europea[34] tuvo como objetivo instituir una legislación penal común entre los Estados parte. Con ese mismo propósito, se creó la Agenda de Ciberseguridad Global de la UIT lanzada en 2007, de la cual se desprendieron la Alianza Internacional Multilateral contra el Ciberterrorismo (IMPACT) y la iniciativa Protección de los Niños en Línea (COP). El objetivo de dicha agenda fue mejorar la seguridad y la confianza en la sociedad de la

31 Delia Crovi, "Dimensión social del acceso, uso apropiación de las TIC". *Revista contratexto*, núm. 16 (2008), 65-79.

32 Valentín Martínez Otero, "Acoso y ciberacoso en una muestra de alumnos de educación secundaria". *Profesorado. Revista de Currículum y Formación de Profesorado*, 21, núm. 3 (2017), 277-298.

33 Bianca Racioppe y Lía Gómez, "Migrar lo digital: desafíos político-tecnológicos del arte en tiempos de pandemia". Lía Gómez (coord.). *Medios y escrituras críticas. Libro de cátedra de análisis y crítica de medios* (Buenos Aires: Universidad Nacional de la Plata, Editorial de la UNLP, 2022), 69.

34 Council of Europe, *Convention on Cybercrime. European Treaty Series - No. 185*, 23, núm. 11 (2001), 1-22. https://rm.coe.int/1680081561

información.[35] Igualmente, destaca la *Declaración de Doha* de 2015, donde se establece la necesidad de abordar "medidas concretas destinadas a crear un entorno cibernético seguro y resistente, prevenir y combatir las actividades delictivas realizadas por Internet".[36]

A pesar de lo expuesto, las políticas de información que atañen a la ciberseguridad son un tópico reciente, por lo cual éstas se ubican dentro de las temáticas emergentes de análisis. En ese sentido, para Sánchez Vanderkast[37] el avance de los estudios en PI se enfocó en los contextos históricos de las sociedades, pero sobreponiendo un examen a partir de los sujetos. De tal modo, en los últimos tiempos el abordaje de PI se ha basado en poner énfasis en las problemáticas y en la consonancia con los sujetos en momentos particulares. Así, los contextos ejercen una influencia sobre las temáticas de frontera de los estudios de políticas de información desde la perspectiva de la bibliotecología y los estudios de la información.

El autor remarca que "cada momento crea nuevas perspectivas sobre los estudios de políticas de información".[38] Al respecto, Caridad Sebastián *et al*. afirmaban que "las políticas de información suelen responder a estímulos concretos en un período de tiempo, y por consiguiente deben ser flexibles",[39] en respuesta a los avances tecnológicos que originaron el nacimiento de internet. Lo anterior concuerda con la perspectiva de Moore,[40] que afirmaba que, al implementarse una serie de políticas de información, se debe cubrir un número de áreas diferente, sujeto a los efectos del rápido cambio tecnológico.

---

35 Unión Internacional de Telecomunicaciones (UIT), "La Agenda sobre Ciberseguridad Global", 2022. https://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html#:~:text=La%20Agenda%20sobre%20Ciberseguridad%20Global%20(GCA)%20de%20la%20UIT%2C,la%20sociedad%20de%20la%20informaci%C3%B3n

36 Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), *Declaración de Doha sobre la integración de la prevención del delito y la justicia penal en el marco más amplio del programa de las Naciones Unidas para abordar los problemas sociales y económicos y promover el estado de derecho a nivel nacional e internacional y la participación pública. Informe del 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 12 a 19 de abril de 2015* (Doha: UNODC, 2015), 11. efaidnbmnnnibpcajpcglclefindmkaj/https://www.unodc.org/documents/congress/Declaration/V1504154_Spanish.pdf

37 Egbert John Sánchez Vanderkast, "Políticas de información: temáticas emergentes y su repercusión en la bibliotecología y los estudios de la información", *op. cit*.

38 *Ibidem*, 127.

39 Mercedes Caridad Sebastián *et al*., "La necesidad de políticas de información ante la nueva sociedad globalizada. El caso español". *Ciência da Informação*, 29, núm. 2 (2000), 23.

40 Nick Moore, "Information policy and strategic development: a framework for the analysis of policy objectives". *Aslib Proceedings*, 45, núm. 11/12 (1993), 281-285.

En el presente, los efectos de la alta penetración de las TIC son indudablemente los ciberdelitos registrados en internet, que se encuentran en expansión. De acuerdo con Bitdefender,[41] los ataques cibernéticos relacionados con el coronavirus se multiplicaron por cinco en el primer trimestre de la pandemia. Por lo tanto, existe una apremiante necesidad por desarrollar un marco de políticas que posibiliten un uso eficiente de la información como recurso nacional económico, social y político. En ese encuadre, y como afirmaba Moore,[42] será necesario tomar en cuenta, además de la expansión de las industrias de la información, el crecimiento del uso de la información como un recurso corporativo y como elemento de la ciudadanía.

Al respecto, hoy en día se afirma que las PI son útiles:

> […] para salvaguardar los derechos de los ciudadanos en el ámbito digital tales como la privacidad, la propiedad, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que estos puedan sentirse cómodos accediendo a dichas tecnologías.[43]

Sin embargo, se puede determinar que esto no ha sido posible en la actualidad debido al número denuncias por ciberdelitos atendidas últimamente en México y en países homólogos.

Conclusiones

Como resultado, se puede establecer que incluir la seguridad en el proceso de la información sigue siendo vigente, según se propuso en los primeros abordajes de las PI. Asimismo, en relación con el ciberespacio, estas políticas son una materia por incorporar en las agendas de gobierno. Sin embargo, otras temáticas han sido más relevantes para los Estados, en perjuicio de los ciudadanos digitales, principalmente en contextos convulsos como los actuales.

En la sociedad postpandémica, el usuario prosumidor no sólo accede a la red para divertirse, sino que se ha visto orillado a utilizarla para actividades vitales como resultado de la epidemia por COVID-19. Esto incluye acciones que involucran el área financiera y moral de las personas, con lo cual se propician

41 Bitdefender, *Evolution of coronavirus-Themed Malware. Europe weekly view*. March-April 2020. April 18. https://labs.bitdefender.com/wp-content/ uploads/2020/04/Weekly-Evolution-of-Coronavirusthemed-threats-in-Europe-during-March-and-April.gif

42 Nick Moore, *op. cit*.

43 Banco Interamericano de Desarrollo - Organización de los Estados Americanos (BID - OEA), *op. cit*., 10.

nuevas disposiciones prácticas y legales que afrontar. En el país se ha procurado atenderlas, pero no se han obtenido los resultados esperados.

En ese sentido, las políticas y estrategias de información en México deben alinearse a la realidad vivida. Si bien se pueden valorar los avances en la materia, conviene atender las debilidades en cuestión respecto al uso y apropiación de las TIC y los riegos que esto conlleva. Atender los ciberdelitos se convierte en un tema prioritario, además, para la agenda investigativa, donde la literatura al respecto todavía es escasa.

Así, se concluye que un redireccionamiento en el diseño y puesta en marcha de políticas de información es esencial para mantener la paz y la seguridad en red en el país. Esto, frente a la convergencia tecnológica presente y derivada de la expansión de la web 2.0, que ha transformado la comunicación y la organización de la vida de las personas.

Bibliografía

Acosta, María Gabriela; Benavides, Merck Milko; García, Nelson Patricio. "Delitos informáticos: impunidad organizacional y su complejidad en el mundo de los negocios". *Revista Venezolana de Gerencia*, 25, núm. 89 (2020), 18-22. www.redalyc.org/articulo.oa?id=29062641023

Banco Interamericano de Desarrollo - Organización de los Estados Americanos (BID - OEA). *Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y El Caribe. Reporte Ciberseguridad*, 2020. file:///C:/Users/Usuario%20Final/Downloads/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Bender, David. R. "A strategy for international information policy". *LIBRI*, 43, núm. 3 (1993), 210-231.

Bitdefender. *Evolution of coronavirus-Themed Malware. Europe weekly view*. March-April 2020. April 18. https://labs.bitdefender.com/wp-content/ uploads/2020/04/Weekly-Evolution-of-Coronavirusthemed-threats-in-Europe-during-March-and-April.gif

Cámara Colombiana de Informática y Telecomunicaciones (CCIT). *Tendencias cibercrimen Colombia 2019-2020*, 2020. https://www.ccit.org.co/wp-content/uploads/ informe-tendencias-cibercrimen_compressed-3.pdf

Cámara de Diputados. "Comisión de Hacienda se reúne con Santiago Nieto, titular de la UIF". Reunión virtual de la Junta Directiva de la Comisión de Hacienda y Crédito Público con Santiago Nieto, titular de la Unidad de Inteligencia Financiera, 24, abril, 2020. https://youtu.be/Mw7iZJBLmAo

Caridad Sebastián, Mercedes; Méndez Rodríguez, Eva; Rodríguez Mateos, David. "La necesidad de políticas de información ante la nueva sociedad globalizada. El caso español". *Ciência da Informação*, 29, núm. 2 (2000), 22-36.

Council of Europe. *Convention on Cybercrime. European Treaty Series - No. 185*, 23, núm. 11 (2001), 1-22. https://rm.coe.int/1680081561

Crovi, Delia. "Dimensión social del acceso, uso apropiación de las TIC". *Revista contratexto*, núm. 16 (2008), 65-79.

Estrategia Nacional de Ciberseguridad (ENCS). 2017. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

González, María. "La cibercriminalidad como instrumento para la expansión y empoderamiento del crimen organizado". *Análisis GESI (Grupo de Estudios sobre Seguridad Internacional*), núm. 46 (2017). https://www.seguridadinternacional.es/?q=es/content/la-cibercriminalidad-como-instrumento-para-la-expansi%C3%B3n-y-empoderamiento-del-crimen

Martínez Otero, Valentín. "Acoso y ciberacoso en una muestra de alumnos de educación secundaria". *Profesorado. Revista de Currículum y Formación de Profesorado*, 21, núm. 3 (2017), 277-298.

Moore, Nick. "Information policy and strategic development: a framework for the analysis of policy objectives". *Aslib Proceedings*, 45, núm. 11/12 (1993), 281-285.

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). *Declaración de Doha sobre la integración de la prevención del delito y la justicia penal en el marco más amplio del programa de las Naciones Unidas para abordar los problemas sociales y económicos y promover el estado de derecho a nivel nacional e internacional y la participación pública, 12 a 19 de abril de 2015.* Doha: UNODC, 2015. efaidnbmnnnibpcajpcglclefindmkaj/https://www.unodc.org/documents/congress/Declaration/V1504154_Spanish.pdf

Pecoy, Martín. "Delito en el comercio electrónico". *Prisma Jurídico*, 10, núm. 1 (2011) 209-224.

Piña, Hiram. "Cibercriminalidad y ciberseguridad en México". *Ius Comitialis*, 2, núm. 4 (2019), 47-69. doi:10.36677/iuscomitialis. v2i4.13203.

Quevedo González, Josefina. "Investigación y prueba del ciberdelito" [Tesis. Programa de Doctorado en Derecho y Ciencia Política] (Barcelona: Universitat de Barcelona, 2017). https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1

Racioppe, Bianca; Gómez, Lía. "Migrar lo digital: desafíos político-tecnológicos del arte en tiempos de pandemia". Lía Gómez (coord.) *Medios y escrituras críticas. Libro de cátedra de análisis y crítica de medios*. Buenos Aires: Universidad Nacional de la Plata, Editorial de la UNLP, 2022, 69-79. http://sedici.unlp.edu.ar/bitstream/handle/10915/134534/Documento_completo.pdf-PDFA.pdf?sequence=1&fbclid=IwAR2Dwa3NFH-xST6oRhuvCOrytc8gzNv8wx7CQbG28coQu0ijPM_LuDmeysg

Rowlands, Ian. "Understanding information policy: concepts, frameworks and research tools". *Journal of information Science*, 22, núm. 1 (1996), 13–25.

Sánchez Vanderkast, Egbert John. "Políticas de información: el amplio espectro de la investigación". *Investigación bibliotecológica: archivonomía, bibliotecología e información*, 9, núm. 38 (2005), 97-117.

Sánchez Vanderkast, Egbert John. "Políticas de información: temáticas emergentes y su repercusión en la bibliotecología y los estudios de la información". Miguel Ángel Rendón Rojas (coord.) *Hacia una escuela de pensamiento iberoamericana de la ciencia de la información documental*. Ciudad de México: UNAM, Instituto de Investigaciones Bibliotecológicas y de la Información, 2020, 99-130.

Sánchez Vanderkast, Egbert John; Gama, Miguel. "Tópicos de políticas de información en el entorno científico y técnico: México 1989 -1994". *Ciência da Informação*, 35, núm. 3 (2006), 75-88.

Secretaría de Bienestar. "Bienestar alerta por presunto fraude con entrega de tarjetas falsas", 29, abril, 2020. https://www.

gob.mx/bienestar/prensa/bienestar-alerta-por-presunto-fraude-con-entrega-de-tarjetas-falsas?state=published

Secretaría de Hacienda y Crédito Público - Consejo Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (SHCP - CONDUSEF). Portal de Fraudes Financieros en México, 2018. https://www.condusef.gob.mx/documentos/prensa/400983_PORTAL_DE_FRAUDES_FINANCIEROS_vers7.pdf

Secretaría de Seguridad Ciudadana (SSC). "La Policía Cibernética de la SSC alerta a la ciudadanía sobre fake news relacionadas con las campañas de vacunación", 25, marzo, 2021. https://www.ssc.cdmx.gob.mx/comunicacion/nota/673-la-policia-cibernetica-de-la-ssc-alerta-la-ciudadania-sobre-fake-news-relacionadas-con-las-campanas-de-vacunacion

Secretaría de Seguridad Ciudadana (SSC). "La SSC a través de la Policía Cibernética, alerta a la ciudadanía a verificar los sitios de compra y venta de tanques de oxígeno en línea", 01, enero, 2021. https://www.ssc.cdmx.gob. mx/comunicacion/nota/001-la-ssc-traves-de-la-policiacibernetica-alerta-la-ciudadania-verificar-los-sitios-decompra-y-venta-de-tanques-de-oxigeno-en-linea

Symantec, Internet Security Threat Report, 24, February 2019. http://latixns.mx/wp-content/uploads/2019/03/ Internet-Security-Threat-Report-20190314.pdf

Unidad de Inteligencia Financiera (UIF). "UIF combate los fraudes electrónicos denominados 'BEC'", ´12, noviembre, 2020. https://www.gob.mx/uif/articulos/nota-informativa-uif-combate-los-fraudes-electronicos-denominados-bec

Unión Internacional de Telecomunicaciones (UIT), "Inclusión digital para todos", 2022. https://www.itu.int/es/mediacentre/backgrounders/Pages/digital-inclusion-of-all.aspx

Unión Internacional de Telecomunicaciones (UIT), "La Agenda sobre Ciberseguridad Global", 2022. https://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html#:~:text=La%20Agenda%20sobre%20Ciberseguridad%20Global%20(GCA)%20de%20la%20UIT%2C,la%20sociedad%20de%20la%20informaci%C3%B3n

Políticas de información: de lo instrumental a lo informacional. Instituto de Investigaciones Bibliotecológicas y de la Información / UNAM. La edición consta de 50 ejemplares. Coordinación editorial: Anabel Olivares Chávez. Revisión especializada, corrección de pruebas y formación editorial: LOGIEM, ANÁLISIS Y SOLUCIONES S. DE R.L. DE C.V. Fue impreso en papel cultural de 90 g en en los talleres de MIGAL Impresiones Digitales S.A. de C.V., 3er Anillo de Circunvalación, No. 73, colonia Barrio Santa Bárbara, Alcaldía Iztapalapa, Ciudad de México, C.P. 09000. Se terminó de imprimir en octubre de 2023.