LA SEGURIDAD CIBERNÉTICA Y LOS DERECHOS HUMANOS

LOS LÍMITES DE LA RESTRICCIÓN DE DERECHOS HUMANOS PARA LA PROTECCIÓN DEL ESPACIO CIBERNÉTICO

A Nicu e Isa
mi Norte y mi Sur

ALEXANDRA CERASELA PANĂ

LA SEGURIDAD CIBERNÉTICA Y LOS DERECHOS HUMANOS

LOS LÍMITES DE LA RESTRICCIÓN DE DERECHOS HUMANOS PARA LA PROTECCIÓN DEL ESPACIO CIBERNÉTICO

EDITURA UNIVERSITARĂ
Bucureşti

Colecţia ŞTIINŢE JURIDICE ŞI ADMINISTRATIVE

Redactor: Gheorghe Iovan
Tehnoredactor: Ameluţa Vişan
Coperta: Monica Balaban

Editură recunoscută de Consiliul Naţional al Cercetării Ştiinţifice (C.N.C.S.) şi inclusă de Consiliul Naţional de Atestare a Titlurilor, Diplomelor şi Certificatelor Universitare (C.N.A.T.D.C.U.) în categoria editurilor de prestigiu recunoscut.

Descrierea CIP a Bibliotecii Naţionale a României
PANĂ, ALEXANDRA CERASELA
La seguridad cibernética y los derechos humanos : los límites de la restricción de derechos humanos para la protección del espacio cibernético / Alexandra Cerasela Pană. - Bucureşti : Editura Universitară, 2021
Conţine bibliografie
ISBN 978-606-28-1360-4

004
34

DOI: (Digital Object Identifier): 10.5682/ ISBN 9786062813604

Editura Universitară
Editor: Vasile Muscalu
B-dul. N. Bălcescu nr. 27-33, Sector 1, Bucureşti
Tel.: 021.315.32.47
www.editurauniversitara.ro
e-mail: redactia@editurauniversitara.ro

Distribuţie: tel.: 021.315.32.47 / 0745 200 718/ 0745 200 357
comenzi@editurauniversitara.ro
www.editurauniversitara.ro

AGRADECIMIENTOS

A mi estimado profesor José Manuel Rodríguez Uribes, por toda su transferencia de conocimiento y por su paciencia para orientarme y apoyarme en todo este largo y duro camino académico. Tengo suerte de haber conocido este gran hombre de cultura; a usted exteriorizo mi profundo agradecimiento. Ser su alumna ha sido un gran honor.

Al estimado profesor Carlos Lema Añón, director del programa de doctorado en Estudios Avanzados en Derechos Humanos, y a Dña. María Carmen Alcubilla Raboso, por brindarme siempre su tiempo, paciencia y quedar siempre pendiente a mis solicitudes e inquietudes.

A mi hermano Dorin y a su hermosa Janeth que me apoyaron en todos estos cinco años de estudio y esfuerzo, inspirándome en cada momento.

A mis padres y suegros, hermanos y cuñados, y a todos mis familiares que me aceptan tal como soy y me ayudan a seguir siempre adelante.

A mis primeros profesores españoles Luis Gutiérrez Sanjuán y Nicolas Rodríguez Castellano que me enseñaron la riqueza jurídica y cultural de España en mi experiencia Erasmus, un momento clave en mi camino académico.

A mis amigos españoles: Isabel, Juan, Seila, Mateo, José y Lisa por su amistad y apoyo en esta aventura académica.

A todos mis colaboradores y compañeros que han aportado buenas experiencias en mi vida, me han orientado en mis decisiones y me han ayudado a crecer profesionalmente.

A mi querido Nicu por caminar de mano más de 20 años, ayudándome a pasar todos los momentos difíciles de mi vida, por su paciencia y su amor infinito.

A mi hija Isa, por compartirme con esta tesis.

CONTENIDOS PUBLICADOS Y PRESENTADOS

- PANA, Alexandra Cerasela (2020). Aplicarea regulamentelor europene în domeniul securităţii cibernetice. Rolul Agenţiei Uniunii Europene pentru securitate cibernetică *(La aplicacion de los reglamentos europeos en el ambito de la seguridad cibernetila. El papel de la Agencia de Seguridad Cibernética de la Unión Europea*). Revista Pandectele Romane no. 3/2020, Editorial Wolters Kluwer România, pp. 71-88. Esta fuente está incluida en el capítulo III de esta tesis.
- PANA, Alexandra Cerasela (2019). Rolul factorului uman în asigurarea protecţiei datelor personale prelucrate în cadrul comunităţilor virtuale *(El papel del factor humano para garantizar la protección de los datos personales procesados dentro de las comunidades virtuales);* Revista Pandectele Române, nr. 6/2019, Wolters Kluwer România, pp. 79-91. Esta fuente está incluida en el capítulo II.

CONTENIDO

INTRODUCCIÓN

Actualmente, la sociedad cambia y se moviliza de la calle a las redes sociales y las plataformas. El mundo cambia y el mundo material se convierte cada vez más en mundo virtual. La sociedad moderna evoluciona, cambia, y se traslada a las redes sociales y plataformas virtuales, conllevando a que nuestros sentimientos se manifiesten en frases cortas y emoticones. La comunicación se comprime en palabras cortas o cortadas, las cartas se transforman en e-mails de máximo dos frases, y el tiempo ya no es suficiente para ninguno de nuestros planes.

En toda esta tormenta de transformaciones, ¿qué vamos a hacer con nuestras reglas de convivencia y con nuestro sistema legal?, todos los principios y las reglas de nuestra sociedad tienen que trasladarse en la nueva sociedad cibernética. Es el momento cuando el Derecho, como ciencia social, está enfrentando un gran desafío: el de adaptarse al espacio abierto creado en Internet o caer en desuso.

El www (World Wide Web) se está organizando y pasa desde el simple usuario a las comunidades virtuales, lo que implica la importación de las reglas sociales en el mundo virtual. Siendo también, el momento idóneo para reformar y mejorar los sistemas sociales y jurídicos.

En la sociedad clásica estamos acostumbrados a ser protegidos por varias autoridades que vigilan que nuestros derechos fundamentales estén garantizados: la libertad, la integridad física, la propiedad, la seguridad etc. ¿Pero en la sociedad virtual, quien vigila nuestros derechos y garantiza su respeto ante cualquier violación?

Al mismo tiempo, es importante conocer el coste de la protección del ser humano en el espacio cibernético. La presente tesis trata de identificar los derechos fundamentales más vulnerables en el nuevo entorno online y a las autoridades responsables para protegerlos.

Al mismo tiempo, se analizará el precio justo de la seguridad cibernética, de una forma analógica con la seguridad individual que gozamos todos los días en nuestras sociedades clásicas[1]. Como ya sabemos, a veces el precio de la seguridad es la limitación de otros derechos fundamentales del ser humano, como el derecho a la vida privada

[1] Hurtaud, S. (2014) *Cyber security. Time for a new paradigm*. Information & Technology Risk. Editorial Deloitte, pp. 90-95

(vigilancia, intervención de conversaciones privadas, etc.), el derecho de la libertad (detención de posibles de infractores), el derecho a la libre expresión (censura de los materiales o medios con contenidos ilícitos o inmorales), el derecho a la libertad de movimiento o a moverse libremente (prohibición de inmigración ilegal) y otros derechos de la persona que interfieren con las reglas sociales cuando se ejercen más allá de los límites establecidos.

Al principio las redes de Internet nacieron libres, como un espacio donde el internauta puede manifestarse de cualquier manera según sus propios límites. Una situación similar al jardín de Edén. Pero, con el tiempo, la cantidad de usuarios virtuales ha aumentado y el entorno digital se transformó en un laberinto y en una verdadera Torre Babel, donde cada usuario habla su idioma y expresa variedad de pensamientos, según sus intereses. Es el crecimiento de internet, su uso masivo y la aparición de cada vez más conflictos cuando hizo pensar que era necesario regularlo[2]. Se pensó en la necesidad de crear reglamentos y organismos de control para su uso correcto.

Después de la aparición de los organismos de reglamentación y vigilancia en Internet, todos los problemas relacionados con la intervención de tales organismos en la vida privada de la ciudadanía aparecieron. Había que fijar un marco legal claro que estableciera la frontera clara entre la necesidad de controlar el espaciador virtual de internet y la protección de los derechos y las libertades de los internautas. Para las organizaciones de Derechos Humanos hay un peligro de restricción de derechos humanos en las redes digitales. Los activistas de los derechos humanos han trasladado su lucha en el entorno digital: "mantener el Internet libre y abierto" es el eslogan de todas sus manifestaciones virtuales. Pero ninguno de estos activistas propone las soluciones para la seguridad cibernética del ser humano (el usuario virtual) que también es uno de nuestros derechos fundamentales muy relacionado con el derecho a la vida. El derecho a la seguridad garantiza el pleno cumplimiento de los demás derechos fundamentales del ser humano y el libre ejercicio de estos derechos en los límites establecidos por los derechos de los demás.

Pues el derecho a la seguridad cibernética del usuario permite que este individuo se manifieste libre y protegido en el entorno online, sin tener miedo de que sus datos personales puedan ser robados, que sus derechos de propiedad intelectual no van a ser vulnerados, que su intimidad no será violada por otros usuarios, que sus conversaciones no serán publicadas sin

[2] Kurbalija, J y Gelbstein, E. (2005) *Gobernanza de Internet: Asuntos, Actores y Brechas*, Editorial DiploFoundation y la Sociedad para el Conocimiento Mundial, p. 82,

su consentimiento. Para garantizar su derecho a la seguridad cibernética algunos organismos tienen que "vigilar" el entorno virtual.

Igual que en la sociedad clásica, a veces, los estados y las autoridades responsables para "vigilar" el respecto de las normas sociales y la seguridad del individuo pasan un poco más de los límites e intervienen en la vida privada de las personas "un poco más de lo que se debe". Por estas razones la sociedad internacional estableció reglas y límites de la intervención de las autoridades en la vida de los protegidos. Al mismo tiempo, organizaciones y organismos internacionales y estatales están analizando y sacando a la luz los casos de abuso por parte de los estados o las autoridades.

El mundo virtual abrió oportunidades tanto para las personas como para Estados y organismo privados. El ciber espionaje internacional, patrocinado por los Estados, ha dado luz a nuevas nociones como *"guerra cibernética"* y a una nueva industria de armas cibernéticas[3]. Las nuevas historias están siendo utilizadas en algunas partes del mundo para animar a los ciudadanos a renunciar a las libertades civiles para una mayor sensación de seguridad[4]. En los EE. UU., por ejemplo, el espionaje cibernético practicado por los hackers chinos es un argumento clave que se utiliza para apoyar la controvertida ley "*Cyber Intelligence Sharing and Protection Act"* (CISPA) que permitiría a las autoridades acceder a grandes cantidades de datos de usuarios sin una orden judicial.

En otros lugares, las amenazas internas a la seguridad nacional que plantea el uso de las nuevas tecnologías han sido utilizadas para justificar extensas medidas de vigilancia[5]. Por ejemplo, en India, no es posible acceder a los teléfonos móviles o a conexiones de Internet, incluso en los cibercafés, sin identificación oficial, y se requiere a los proveedores de Internet y los cibercafés que mantengan registros detallados de la historia de la navegación de los usuarios.

Las narrativas de la fatalidad que invariablemente acompañan a dichas medidas se basan aún más en la fuerza del crecimiento real de la delincuencia cibernética - que ahora se dice que hay más de 150.000 virus y

---

[3] Gómez, A. (2012) *El ciberespacio como escenario de conflicto. Identificación de las amenazas*, en El ciberespacio. Nuevo escenario de confrontación, Madrid, Ed. Ministerio de Defensa, pp. 167-204

[4] Pepitone, J. (2013) *Cybersecurity lobbying doubled in 2012*. CNN Money (New York). The Cybercrime Economy, Recuperado de: https://money.cnn.com/2013/04/08/technology/security/cybersecurity-lobbying/index.html#_blank.

[5] Glenny, M. (2011) *DarkMarket: Cyberthieves, Cybercops and You*. Editorial Knopf; Canadian First edition, p. 217.

otros tipos de código malicioso en circulación, con un millón de personas que se convierten en víctimas de delitos cibernéticos cada día[6].

De esta manera el tema de la seguridad cibernética y la protección de los derechos de la ciudadanía en las redes preocupa cada vez y es un tema controversial. Sobre este problema se pronuncian cada vez más los Estados y los agentes políticos y sociales, también del ámbito internacional.

En realidad, existen amenazas reales y van en aumento. El acceso ilegal a los datos y a las computadoras, así como la interferencia de datos, se han convertido en problemas más comunes y complejos que afectan a un gran número de personas. Temas como: el fraude está adoptando nuevas formas en Internet, y a medida que más de nuestra infraestructura crítica se vuelve dependiente de Internet, las infracciones de seguridad pueden tener repercusiones significativas, incluyendo afectación de los derechos humanos cuando, por ejemplo, un ataque impide que las personas accedan a los servicios públicos o al ejercicio de su derecho a la expresión.

La obligación de los Estados es garantizar los derechos y libertades dentro de su territorio y cambien en este tema, no tan nuevo ya, del uso masivo de las redes y la criminalidad que le acompaña[7].

Sin embargo, las estrategias de seguridad cibernética deben ser diseñadas e implementadas de una manera que es convergente con el derecho internacional de los derechos humanos - con demasiada frecuencia esto no es el caso, como se ve en los regímenes de vigilancia descritos anteriormente. La aplicación de las normas de protección de derechos humanos a las políticas de Seguridad Cibernética se basará, en primer lugar, en la familiarización de todos los actores implicados con las normas de derechos humanos y la promoción de manera coherente[8].

En otros casos, se encontró incluso, Estados que están detrás de las amenazas como los ataques cibernéticos dirigidos hacia los defensores de los derechos humanos o la oposición política. Por tanto, es importante que la comunidad de derechos humanos empiece a comprometerse con estos discursos más de cerca, para anular las amenazas contra los mismos. Además, deben ofrecer propuestas de solución para que no se repitan y

---

[6] Deibert R. (2012) *The Growing Dark Side of Cyberspace (. . . and What To Do About It)*, Penn State Journal of Law & International Affairs, vol. I, Issue 2, p. 260.
Recuperado de: https://elibrary.law.psu.edu/jlia/vol1/iss2/3.

[7] Torrecuadrada, S. (2013) *Internet y el uso de la fuerza*, en Ciberseguridad global. Oportunidades y
compromisos en el uso del ciberespacio, Granada, Ed. Universidad de Granada, pp. 91-118.

[8] Shackelford, S. J. (2009) *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. Berkley Journal of International Law, Vol. 25, No. 3/2009, recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1396375

garanticen las reglas y normas de derechos humanos también en las redes digitales, garantizando la seguridad cibernética a la vez.

La investigación realizada en la presente tesis busca identificar y analizar los puntos neurálgicos en el conjunto de los derechos fundamentales que se activan con la interacción del ser humano y el mundo virtual. El principal objetivo de esta tesis es de establecer los límites de las intrusiones legales sobre los derechos individuales por parte de las autoridades, usando las nuevas tecnologías y el Internet. Para encontrar respuestas a las preguntas que se formularán más adelante, se utilizó diversas fuentes de información como: los textos de los tratados internacionales y convenios regionales sobre los derechos humanos, los textos constitucionales de diferentes países, pero con acento especial sobre el marco jurídico de España y Rumania, la doctrina constitucional emanada de los órganos jurisdiccionales, y los pronunciamientos doctrinales.

Entre los métodos de investigación empleados para llegar a las conclusiones perseguidas mencionamos el método comparativo (se han comparado las normas que regulan los derechos fundamentales en distintos sistemas de derecho), el método histórico (presentando la evolución de los derechos en los últimos años), el método correlacional y el método deductivo para proponer soluciones adaptadas a los nuevos desafíos.

La tesis se desarrollará en ocho capítulos que tratan sobre los problemas y desafíos jurídicos mencionados en los párrafos anteriores. En líneas generales, la investigación se centra en buscar respuestas a tres grandes preguntas sobre el contenido de la noción de *seguridad cibernética*, la existencia de un estado de derecho en el entorno digital y la posibilidad de regular la conducta del usuario en el espacio virtual en armonía con los intereses de seguridad colectiva y el respeto de los derechos humanos.

¿Qué es la seguridad cibernética?

En la actualidad, el término *seguridad cibernética* goza de varias definiciones, ya que se utiliza para cubrir una amplia gama de preocupaciones: en diferentes contextos y por diferentes actores, el término se utiliza para referirse a la seguridad de la infraestructura nacional; la seguridad de la infraestructura de Internet; la seguridad de las aplicaciones y servicios; la seguridad de los usuarios (que van desde las empresas a los usuarios individuales); a la estabilidad del Estado y de las estructuras políticas[9].

[9] Robinson, N. (2014): *EU cyber-defence: a work in progress*. EU Institute for Security Studies, vol.10, pp 1-10, recuperado de: http://www.iss.europa.eu/uploads/media/Brief_10_Cyber_defence.pdf.

De acuerdo con la Comisión Europea, la ciberseguridad representa "*todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciber amenazas*"[10].

Citando a Kaspersky, una de las más importantes compañías internacionales dedicadas a la seguridad informática, con presencia en aproximadamente 195 países del mundo (su sede central en Rusia, mientras que el holding está registrado en Reino Unido):

> *"La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes"*[11].

Esta terminología apunta a una de las principales preocupaciones acerca de este discurso en crecimiento: la terminología cubre una agenda que es inexacta, que mezcla preocupaciones legítimas e ilegítimas y fusiona diferentes tipos y niveles de riesgo. Esto evita que el escrutinio verdadero, objetiva e inevitablemente, conduzca a respuestas que son de amplio alcance y pueden ser fácilmente usadas de manera indebida o abusiva.

El uso de un lenguaje cargado y ambiguo puede determinar, de hecho, consecuencias de gran alcance, ya que muchos gobiernos están utilizando vagas amenazas internas y externas como argumentos para justificar cada vez mayores inversiones en armas cibernéticas y sistemas de vigilancia masiva y cada vez mayor control gubernamental sobre el Internet y sobre sus ciudadanos[12].

La sensación de alarma o peligro inminente, incorporada en las narrativas de seguridad cibernética, representa una forma de manipulación de la mente humana para aceptar la limitación de sus derechos en nombre de la seguridad. No obstante, en 2020 el peligro de contaminación con el coronavirus COVID 19 ha determinado una histeria

---

[10] Artículo 2 (1) del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) no 526/2013 (en adelante Reglamento sobre la Ciberseguridad)

[11] Eugene Kaspersky – cofundador y Director General de Kaspersky, el proveedor privado de soluciones de ciberseguridad y protección de endpoints más grande del mundo. Mas información en: https://latam.kaspersky.com/about/team.

[12] Farwell, J.P. y Rohozinski, R. (2011) *Stuxnet and the Future of Cyber War*, Revista Survival, Global Politics and Strategy , vol. 53, issue 1, pp. 23-40.

global, aunque los datos sobre el virus, la manera de transmisión y sus efectos son controversiales. Los estados y los individuos se han alarmado de una manera tan fuerte que los derechos fundamentales pasaron a segundo plano, siendo limitados, restringidos con el acepto general de las mases. Aunque todavía estamos viviendo este experimento, nuestros derechos están siendo limitados, con la justificación de preservar otro derecho fundamental que es el derecho a la salud y a la seguridad. La amenaza de un peligro inminente, invisible, no detectable parece ser motivo suficiente para que la ciudadanía renuncie a derechos fundamentales.

La histeria social originada por la idea de un ataque inminente físico, cibernético, médico, puede crear la opinión de que todas las respuestas son válidas y legítimas, de manera acrítica. Por ejemplo, como se manifestó anteriormente, en muchos países, tanto democráticos y no democráticos, las amenazas a la seguridad nacional han sido utilizadas para justificar los mecanismos de vigilancia amplios, con más y más datos de los ciudadanos recogidos y de fácil acceso por las autoridades estatales.

Otras medidas nefastas de "seguridad" incluyen el desarrollo de los llamados "interruptores de Internet" (la noción de cierre de Internet con el fin de protegerlo), que restringe el uso de la encriptación, la implementación de mecanismos de filtrado y bloqueo y la introducción de políticas de nombres reales[13]. Estas medidas que representan una amenaza para las libertades civiles, sin embargo, tienden a carecer de supervisión judicial.

¿Cómo se protegen los derechos humanos en el entorno online y cuáles son las perspectivas sobre el futuro democrático del Internet?

"*Los mismos derechos que tienen las personas fuera de la línea también deben ser protegidos en línea*"[14] - esta simple declaración, aprobada por una resolución del Consejo de Derechos Humanos de la ONU el 2 de junio de 2012, confirma lo que parecía evidente para los activistas de derechos humanos desde hace muchos años. Aunque otros derechos humanos (como el derecho de reunión y asociación pacíficas, el derecho a un recurso efectivo y la presunción de inocencia) también son pertinentes, dos derechos humanos en particular formarán los elementos básicos de los enfoques de la seguridad cibernética que respetan los derechos. Uno de estos es el derecho a la vida privada, o el derecho de mantener los datos y la comunicación fuera de los ojos del gobierno, las empresas u otros

[13] Perlroth, N. (2013) *Researchers Find 25 Countries Using Surveillance Software*, The New York Time Journal. Recuperado de: https://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/.

[14] Consejo de Derechos Humanos (2012) *Promoción, protección y disfrute de los derechos humanos en Internet* (A/HRC/20/L.13), New York, United Nations General Assembly, 29 June 2012.

ciudadanos. El derecho a la vida privada es un componente necesario en el desarrollo de una política de seguridad centrada en el ciudadano. Sin embargo, no es suficiente, ya que no cumple todos los requisitos para estar uno seguro en línea de la manera que hemos definido anteriormente. Por ejemplo, el derecho a la vida privada no ofrece salvaguardias suficientes contra los controles de contenido instituidos por los gobiernos en el nombre de las políticas de seguridad en los puntos donde los cables de Internet entran en un país.

En la evaluación de las políticas de seguridad cibernética se debe otorgar la misma importancia al disfrute sustantivo por parte de todos los ciudadanos del derecho a la libertad de expresión. La libertad de expresión se ve interferida cuando una acción impide que alguien busque, reciba o imparte otra expresión que no sea la legítimamente limitada, y acciones que desalienta o inhibe esa expresión.

Ambos derechos pueden ser restringidos bajo ciertas circunstancias y solo si tal restricción está prevista por la ley. Sin embargo, las interferencias con la libertad de expresión solo serán legítimas si siguen la prueba acumulativa tripartita que está prevista por la ley, es decir legalidad, proporcionalidad y necesidad.

Asimismo, las interferencias con el derecho a la vida privada requieren que "*debe existir una ley que defina claramente las condiciones por las cuales el derecho de los individuos a la privacidad puede ser restringido en circunstancias excepcionales y las medidas que invaden este derecho deben tomarse sobre la base de una decisión específica por una autoridad estatal expresamente facultada por la ley para hacerlo, generalmente el poder judicial, con el fin de proteger los derechos de los demás, por ejemplo para obtener pruebas que impidan la comisión de un delito y deben respetar el principio de proporcionalidad*"[15].

Según el Relator Especial existen algunas situaciones cuando es posible y recomendable restringir el derecho a la libre expresión:

> *"En este sentido, entre los tipos legítimos de información que pueden restringirse cabe mencionar la pornografía infantil (para proteger los derechos del niño), la incitación verbal al odio (para proteger los derechos de las comunidades afectadas), la difamación (para proteger los derechos y la reputación de los demás contra ataques injustificados), la incitación directa y pública a cometer actos de genocidio (para proteger los derechos*

[15] Frank La Rue (2011) *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, New York, Asamblea General de las naciones Unidas, 16 de Mayo 2011. Recuperado de: https://www.acnur.org/fileadmin/Documentos/BDL/2015/10048.pdf.

de los demás) y el fomento del odio nacional, racial o religioso que constituya incitación a la discriminación, hostilidad o violencia (para proteger los derechos de los demás, como el derecho a la vida)"[16].

Estos términos y pruebas han sido desarrollados y elaborados a través de la jurisprudencia y normas de derecho indicativo[17] *"soft law"*. Cualquier medida de seguridad que no se adhiera a estos criterios estrictos, aunque posiblemente incremente la seguridad de la red afecta la seguridad sustantiva del pueblo. Es muy importante que existan claros límites legales internacionales sobre las acciones que pueden tomar legalmente en el dominio cibernético. Leyes y prácticas que interfieren con los derechos humanos en línea sólo son legítimas en la medida en la que caen dentro de los estrechos límites permitidos por la ley internacional de derechos humanos. Por tanto, es necesario volver a examinar la agenda de seguridad cibernética a la luz de las normas y valores de los derechos humanos.

Sin embargo, la vigilancia tiene que ser necesaria y proporcionada a la amenaza[18]. Con frecuencia, estas condiciones quedan sin cumplirse. En lugar de apoyarse unos a otros, la seguridad informática y la vigilancia están en frecuente desacuerdo. Si a desarrollar políticas de seguridad informática que apoyan fundamentalmente los derechos humanos, es esencial que esto se reconozca y se contabilice el estado de derecho que existe en el mundo físico, offline, debe trasladarse con todos sus elementos y principios al entorno online.

Las políticas de seguridad informática no deberían limitarse a desempeñar un papel defensivo, sino un papel facilitador, poniendo efectivamente la autonomía y el bienestar de las personas en su centro. Con la finalidad de evaluar la eficacia de una medida de seguridad cibernética, es esencial tener en cuenta no sólo el impacto potencial de las diversas amenazas a la seguridad cibernética, sino también las soluciones propuestas. Si una medida, aplicada para proteger a las personas, afecta ella misma los derechos humanos, de tal manera y en tal medida que incluso limita la capacidad de las personas para acceder y utilizar el Internet, no puede ser considerada como una medida de seguridad razonable.

---

[16] Ibidem.

[17] El derecho indicativo (soft law) representa "un conjunto de instrumentos jurídicos de carácter no vinculante que, sin embargo, aspiran a influir en la legislación vinculante indicando un camino al que se aspira llegar. Es el antónimo de derecho imperativo" (hard law) – **RAE: Diccionario panhispánico del español jurídico.**

[18] Deibert, R. (2012) idem.

¿Es posible una Carta Cibernética de Derechos Humanos?

En los últimos años se ha producido una serie de intentos por definir exactamente cómo se aplican las normas internacionales de derechos humanos en el entorno online. Los "*Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones"*[19] es una propuesta de reglamentación elaborada por unos ONG para demonstrar que las normas y estándares internacionales de derechos humanos son aplicables en los casos de la vigilancia de las comunicaciones en el entorno electrónico.

El texto[20] reafirma el carácter fundamental del derecho a la intimidad y subraya la conexión esencial con la dignidad humana, demostrando que las actividades de vigilancia sobre las comunicaciones de las personas tanto en el entorno electrónico como también en el medio real constituye una injerencia con los derechos fundamentales. los principios declaran una vez más que solo la ley puede ser el único fundamento para la intervención de las autoridades en la vida privada de una persona. Para ser autorizada, toda restricción debe lograr un objetivo legítimo, ser idónea, necesaria y proporcional con la amenaza publica que se quiere neutralizar. Los fundamentos y las ideas de estos 13 principios se encuentran regulados en los instrumentos internacionales importantes de derechos humanos como la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, la Convención Americana sobre Derechos Humanos y Deberes del Hombre, la Declaración de los Derechos Humanos de ASEAN y la Carta Africana de Derechos Humanos y de los Pueblos.

Los activistas proponen la adopción de un convenio internacional cibernético dedicado a la protección de los derechos humanos, construido sobre una base de estos trece principios fundamentales, dedicados a garantizar una mayor transparencia y un control cívico. El principal objectivo de tal convenio seria la limitación de las injerencias en la vida

[19] Los principios, que son el fruto de un trabajo común de los representantes de la sociedad civil y expertos, fueron elaborados y publicados por las organizaciones Access, Artículo 19, Asociación Civil por la Igualdad y la Justicia, Asociación por los Derechos Civiles, Association for Progressive Communications, Bits of Freedom, Center for Internet & Society India, Comisión Colombiana de Juristas, Electronic Frontier Foundation, European Digital Rights, Fundación Karisma, Open Net Korea, Open Rights Group, Privacy International, y Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, entre otros..

[20] El texto integral de los principios es disponible en https://necessaryandproportionate. org/principles/.