IUS ET SCIENTIA
2022 • Vol. 8 • Nº 2• ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2022

El estado, el desarrollo tecnológico y algunos problemas éticos en internet

THE STATE, TECHNOLOGICAL DEVELOPMENT AND SOME ETHICAL PROBLEMS ON THE INTERNET

Francisco Javier Chan Chan*
Universidad Autónoma de Yucatán
chancheatman@hotmail.com 0000-0002-5733-9318

Recibido: 23 de junio de 2022 | Aceptado: 24 de noviembre de 2022

RESUMEN

El presente trabajo plantea dos cuestiones principales: la relación entre el Estado y el desarrollo tecnológico; y el estudio de cuatro problemas éticos en línea. Respecto de la primera, se pretender responder a la preguntar sobre la existencia de una relación entre el Estado y su desarrollo tecnológico y cómo éste influye específicamente en el caso de Internet. En relación a la segunda, exponemos cuatro problemas éticos en Internet: *deep web*, venta de órganos en línea, ciberguerra y pornografía infantil. Todo lo anterior se describe con el fin de dar un panorama general del desarrollo tecnológico estatal, los problemas éticos que pueden surgir y las conductas que los usuarios tienen en relación a estos últimos.

PALABRAS CLAVE

Internet
Ética
Estado
Desarrollo

ABSTRACT

The present article raises two main questions: the relationship between the State and technological development; and the study of four ethical problems online.
Regarding the first question, it is intended to answer the question about the existence of a relationship between the State and its technological development and how it specifically influences the Internet. Related to the second question, we expose four ethical problems on the Internet: deep web, online organ sales, cyberwar and child pornography. All the above is described in order to give an overview of the state technological development, the ethical problems that may arise and the behaviors that users have in relation to the ethical problems in particular.

KEYWORDS

Internet
Ethic
State
Development.

* Maestro en derecho por la UNAM, profesor de asignatura de la Facultad de Derecho de la UADY y estudiante del doctorado en derecho en el IIJ UNAM. Quiero agradecer las observaciones de Edith Cuautle para realizar el presente artículo.

I. Introducción

Internet es un espacio donde millones de personas se comunican, quienes pasan horas diariamente realizando actividades de diversa índole en una computadora o dispositivo. En este espacio digital podemos realizar numerosas actividades, desde consultar alguna referencia bibliográfica en alguna biblioteca virtual hasta revisar correos electrónicos o incluso entrar a bases de datos.

Estas acciones que las personas realizan en el quehacer cotidiano se llevan a cabo de manera totalmente diferente, es decir, depende de las costumbres o formas habituales en las cuales están acostumbradas a ello, pero además, involucran muchos aspectos como el contexto en el que se desenvuelven y el lugar en el que se encuentran.

Valores, principios y reglas regulan nuestro comportamiento, así como la forma en la que actuamos y nos relacionamos unos con otros. En relación a ello, si bien las acciones se diferencian en lo individual; también es verdad que se distinguen en lo colectivo, toda vez que las personas tienden a realizar conductas determinadas cuando se encuentran en conjunto.

Dicho lo anterior, nos hacemos las siguientes cuestiones: *a)* ¿Existe una relación entre el Estado y el desarrollo tecnológico?, es decir, tiene una injerencia directa el Estado en el desarrollo tecnológico para el mejor uso y aprovechamiento de Internet; y *b)* Dentro de la red, ¿qué problemas éticos pueden surgir derivados de los diferentes usuarios que conviven en línea?

En el presente trabajo se pretende explicar dos cuestiones: la primera, la problemática entre el Estado y el desarrollo tecnológico; y la segunda, algunos problemas éticos en Internet importantes y las diversas conductas de los usuarios en este espacio. Es importante destacar que, respecto a este último apartado, este estudio no es limitativo, sino por el contrario muestra un pequeño bosquejo de las problemáticas existentes actualmente en la red y cómo esta situación afecta a usuarios en todo el mundo.

II. El Estado y el desarrollo tecnológico

El Estado puede ser concebido de diferentes formas: como comunidad política desarrolladora, como estructura del poder político de una comunidad, o como un espacio geográfico donde se escenifican las aspiraciones nacionales (Tamayo y Salmorán, 2011, p. 215). Asimismo, es entendido como una institución que interviene en las actividades de los individuos que conviven en un territorio determinado, y facilita la comunicación y organización entre los mismos. En esta función de *coordinación* el Estado debe velar por la justicia y seguridad social de los ciudadanos, que es fundamental para el desarrollo de los mismos y el bienestar social. En relación con lo anterior, dos principios son los que enuncia Rawls para llegar a una justicia social: *a.* libertades básicas; y *b.* que de las desigualdades sociales y económicas se espere sean ventajosas y asequibles para todos (Rawls, 2011, pp. 68 y 69).

Dentro de este grupo de libertades básicas podemos considerar el derecho a la libertad de conciencia y el derecho a la información. Aquellos se relacionan entre sí, ya que

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

una libertad de pensamiento, nace a partir de un ciudadano que tiene conocimiento, que reflexiona y comprende el entorno que lo rodea. Sin embargo, la información no se limita únicamente a preparación o formación cultural y profesional, sino que involucra los medios para llegar a tales, y uno de éstos es la tecnología. En esta tesitura, esta última y la sociedad tienen una relación existente y el Estado juega un papel fundamental y decisivo en el proceso general de dirección e innovación tecnológica hacia la sociedad, en virtud que expresa y organiza las fuerzas culturales que dominan un espacio y tiempo determinado (Rawls, 2011).

Desde la Revolución Industrial hasta la tecnológica, el Estado ha sido parte toral en el proceso histórico mediante el cual tiene lugar el desarrollo de fuerzas productivas basadas en tecnología y relaciones sociales. Esta última revolución no es distinguida por el carácter central de conocimiento y la información, sino por la aplicación de tales aparatos de generación y procesamiento de datos.

Las nuevas tecnologías no son exclusivamente herramientas que se aplican, sino que son procesos que se van desarrollando, en los cuales tanto los usuarios como los creadores pueden jugar ambos roles. Esta circunstancia, crea una participación activa en la sociedad que tiene alcance a estas tecnologías y los involucra en procesos sociales de creación y capacidad de producir y distribuir bienes y servicios. De esta forma, para Manuel Castells, los ordenadores, los sistemas de comunicación y la decodificación y programación genética son todos amplificadores y prolongaciones de la mente humana.

La revolución tecnológica de la información no nace a partir de programadores, ni innovadores, ni mucho menos de especialistas en informática, sino del Estado mismo quien es el iniciador. Sin embargo, y en sentido contrario, aquel puede ser un limitador del desarrollo tecnológico, como un ancla, y dejando a la sociedad estancada en un retroceso contundente. De tal suerte que puede limitar los medios o las herramientas que sirven para la transmisión de información o comunicación, aislando a un país de la realidad; o por el contrario, el avance tecnológico puede ser tan elevado que los bienes y servicios tienen una innovación y mejoramiento beneficioso para la sociedad.

Castells determina lo anterior de la siguiente forma:

> El Estado puede ser, y lo ha sido en la historia, en China y otros lugares, una fuerza dirigente de innovación tecnológica; por otra, precisamente debido a ello, cuando cambia su interés por el desarrollo tecnológico, o se vuelve incapaz de llevarlo a cabo en condiciones nuevas, el modelo estatista de innovación conduce al estancamiento debido a la esterilización de la energía innovadora autónoma de la sociedad para crear y aplicar la tecnología (Castells, 2011, pp. 38 y 39).

Este desarrollo tecnológico es parte del modelo estatista de innovación, y el Estado se vuelve el motor de este. Con el fin de esclarecer lo anteriormente expuesto, señalaremos a dos países como ejemplo, y compararemos su desarrollo tecnológico. La República de Corea es un pequeño país ubicado en el extremo oriental de Asia que ha logrado un crecimiento económico impresionante en un periodo de tiempo muy corto. En la actualidad, es un país con un nivel de desarrollo tecnológico muy alto, fabricante de semiconductores, automóviles, construcción naval, acero y diversas industrias tecnológicas

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

de la información (Internet World Stats, Usage and Population Statistics, 2022) que son de las más avanzadas en los mercados mundiales. Por su parte, México es un país con un desarrollo tecnológico limitado, debido al escaso interés gubernamental observado en apoyo a la ciencia. En el año 2021 México tenía la posición 55 con relación al Índice Mundial de Innovación, a diferencia de Corea que ocupaba el puesto número 5 (OMPI, 2021). Esta diferencia en inversión se ve reflejada en la actualidad, en el nivel tecnológico y en la aplicación que tienen los ciudadanos de aquel.

A raíz del atraso científico que puede suscitarse en un Estado, se causa un distanciamiento entre los ciudadanos, así como entre los habitantes de unas u otras naciones. Esta situación marca una diferencia inevitable entre la forma en la cual se desenvuelve cada una de las personas y en los servicios que son ofrecidos por las diversas instituciones de cada entidad. Por ejemplo, las políticas públicas en las cuales ofrezca el Estado Internet gratuito en espacios públicos como parques y bibliotecas dependerán enteramente de la disposición que las personas tengan de un aparato, llámese computadora, tableta, celular, etcétera., para poder navegar en la red, por lo cual, si la ciudadanía no cuenta con tal dispositivo, le será imposible.

Este problema es repetido en otras circunstancias e instituciones públicas y privadas, en las cuales, la manera en que las actividades se llevan a cabo es dependientesde los equipos con que los usuarios cuentan (Lazcano Ponce, 2013). Si bien todos los estudiantes tienen el derecho de inscribirse en una institución pública, no todos tienen la facilidad de registrarse en el sistema *pre admisorio* cuando las inscripciones se realizan obligatoriamente en Internet. Ello es así, en virtud que existen poblaciones enteras en toda la República Mexicana que todavía no cuentan con tal servicio, o si lo tienen es de muy mala calidad.

Lo anterior nos ayuda a comprender dos puntos importantes: *a)* La relación existente entre el Estado y el desarrollo tecnológico; y *b)* la accesibilidad que los ciudadanos tienen a los servicios que el Estado ofrece. Es verdad que el segundo depende del primero, porque para que a un ciudadano le sean asequibles servicios tecnológicos, es necesario que el país este desarrollado tecnológicamente. Sin embargo, la existencia del primero no implica la del segundo, ya que ésta puede ser limitada para algunos. Por otro lado, si bien existen similitudes y divergencias entre el desarrollo tecnológico de los países, este no se puede cuantificar en un adelanto máximo, en virtud que aquel seguirá creciendo y perfeccionándose tecnológicamente, siempre y cuando el Estado mismo lo determine así.

Para el caso mexicano, el gobierno en turno ha promovido la Estrategia Digital Nacional cuya misión es promover e impulsar que las personas en México gocen y se beneficien del acceso a las tecnologías de la información y comunicación, así como los servicios de banda ancha e Internet (Proceso de Planeación para el Desarrollo de la Estrategia Digital Nacional y de la Política Tecnológica, 2021). Dentro de las acciones clave de la EDN encontramos que la conectividad de banda ancha e Internet será para todo el país, a través de la creación de una empresa estatal y acuerdos con la industria.

Los objetivos, si bien promueven un mejoramiento en los servicios y en la competencia; difícilmente lograrán una democratización en el acceso a las telecomunicaciones.

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

Ante ello, existen cuestiones necesarias, que deben ser satisfechas por el Estado, para posteriormente dar continuación a otras circunstancias como el desarrollo tecnológico. Alguna de las falencias de la EDN es que no explica detalladamente cómo se llevará a cabo el acceso universal de la red. En el sexenio pasado la EDN proponía un proceso de "democratización de servicio de telecomunicaciones".

Como podemos observar tenemos un problema latente entre el desarrollo tecnológico de un Estado y la influencia en el uso y disfrute de las diversas tecnologías que lo conforman, para nuestro caso en particular Internet. Además de esta situación, existen otros problemas éticos que rebasan fronteras y afectan a los usuarios en Internet y en específico sus conductas, que expondremos a continuación.

III. Problemas Éticos en la Red

Conforme crece la red de redes, también crece el número de usuarios que la conforman (Estudio sobre los hábitos de personas usuarias de Internet en México, 2022). Este incremento exponencial de los cibernautas nos hace pensar en el aumento de la comunicación entre los usuarios y las acciones que se llevan a cabo. Si bien el derecho coordina las conductas entre las personas para la protección de valores establecidos por ellas; no puede calificar las acciones como buenas o malas. Sin embargo, son aquellas quienes que realizan esta calificación y determinan el valor que tienen.

Todo ello no es excepción en Internet, ya que entre el mundo virtual y el físico, las acciones y conductas tienden a ser las mismas, y sólo cambia la forma en que se desarrollan. Sin embargo, en el presente apartado del trabajo, lo que nos atañe no es calificar las acciones en línea sino comprender la problemática que surge en estos conflictos y las posturas que han sido tomadas entre los usuarios, el Estado y en ocasiones las instituciones públicas y privadas.

Una vez expuesto lo anterior, señalaremos cuatro problemas éticos que surgen en Internet: el *Internet profundo*; la *donación de órganos*; la *ciberguerra* y *ataques en línea*; y la *pornografía infantil*.

3.1. Internet Profundo (*Deep Web*)

Internet es un espacio gigantesco lleno de todo tipo de contenidos como imágenes, videos, audio, etcétera. Esta información se encuentra almacenada en la red y, debido al gran tamaño que presenta, es imposible localizar algo en específico sin la ayuda de un motor de búsqueda. En un principio Internet era relativamente pequeño, por lo cual resultaba fácil encontrar contenidos y clasificarlos; a pesar de esto, con el paso de los años ha ido creciendo de una manera desmesurada, por lo que los buscadores se han ido especializando. Lo anterior lo podemos comparar cuando realizamos alguna búsqueda en una biblioteca y el sistema que maneja para encontrar el libro se va dividiendo en *voces*, las cuales se pueden establecer en la aplicación para realizar búsquedas más especializadas. Mientras más filtros instauremos, más limitada será la información. Internet

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

no es la excepción, y así como en las bibliotecas llegan nuevas obras, en la red también, pero esta circunstancia es constante y muy dinámica. Dado lo anterior, nos podemos imaginar el tamaño de la red y lo difícil que resultaría hacer una búsqueda, por lo cual nos preguntamos ¿cómo es tan fácil esta localización en los motores de búsqueda? La respuesta es muy sencilla, es así debido a que los buscadores han sido personalizados, el principal de ellos y más utilizado por los usuarios, Google. Aquel realiza su localización tomando como referencia datos personales (Google, Políticas de Privacidad), y de esta información obtenida y proporcionada se lleva a cabo una búsqueda eficaz.

El contenido recibido en los motores de búsqueda se queda en una superficie muy banal, manteniéndose la mayor parte de la información en un espacio adentrado y profundo de la red, un lugar donde los buscadores comunes no llegan (Chang *et. al*.,) y en el cual se encuentran bases de datos de toda índole. Es de creencia común que este espacio explorado por algunos pocos, está lleno de contenidos ilegales y antiéticos, esto es en parte cierto. Contrario a lo anterior, un estudio realizado por He, Patel, Zhang y Chang de la Universidad de Ilinois, determinaron que el contenido de la *Deep web* está divido en dos tipos de bases de datos, los *sin estructura* (textos, imágenes, audio y video); y *estructurados* (se establecen valores binarios). De un estudio de 190 bases de datos de la *deep web*, 43 fueron sin estructura, mientras que 147 estructurados.[1]

Una vez establecida la forma en que se encuentra conformada la red profunda, es importante indicar que, así como existe una gran cantidad de contenidos diversos, en su mayoría bases de datos, de igual forma se pueden dar espacios para la realización de actos ilícitos. Ello es así, en virtud a la naturaleza misma de la red y a la dificultad para llegar a esa cantidad de contenidos que se no se encuentran al alcance de cualquier usuario común. Piratería, pornografía infantil (Beckett, 2009), contrabando de armas, venta de drogas, trata de personas y sicarios por contratos son algunas de las actividades ilícitas en esta oscura red. Asimismo, estos delitos se dan debido al fácil anonimato que nos entrega; por lo cual la libertad resulta ser casi absoluta, donde podemos comprar desde narcóticos o armas, hasta órganos por encargo. A raíz de estos delitos cibernéticos,[2] la policía, tanto en México como en el mundo, ha creado cuerpos especializados para combatirlos.

Cuando nos conectamos y navegamos en la red, en ocasiones no percibimos la cantidad de conexiones que se suscitan por segundos mientras estamos frente a nuestra computadora. Internet como lo conocemos tiene una inmensidad comparado con las limitadas páginas que consultamos día a día. Por un lado, el anonimato nos protege frente a las personas conectadas permitiéndonos interactuar en los medios electróni-

1. Las 190 bases de datos de la web se clasificaron en los siguientes tópicos: Negocios y Economía; Computación e Internet; Noticias y Medios de comunicación; Entretenimiento; Deportes y Recreación; Salud; Gobierno; Regional; Sociedad y Cultura; Educación; Artes y Humanidades; Ciencia; Referencias; y Otros. Lo anterior nos demuestra una gran diversidad en la Deep Web, a diferencias de lo que pensado que en su mayoría serían sobre comercio electrónico. *Ibídem*, p. 5.

2. Con el fin de combatir estos delitos cibernéticos, en México entidades federativas como Jalisco y Yucatán cuentan con policía cibernética; por lo que respecta a Estados Unidos, el FBI es el encargado.

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

cos bajo un escudo; pero por otro lado, esta protección para algunos resulta una herramienta para cometer actos ilícitos.

No todo lo relacionado con la *Deep web* es negativo, para Etay Maor, Consejero de Cyberseguridad de IBM existen algunos aspectos que son positivos y de apoyo como por ejemplo: espacios donde pueden tener comunicación grupos vulnerables en un anonimato y sin poder se rastreados, lo cual les da una legítima razón para usarlo (Mann, 2016).

3.2. Venta de órganos en línea

Los trasplantes de órganos en la sociedad moderna han sido centro de debates partiendo de dos posturas: la primera se basa en los avances científicos y en el ánimo gratuito del acto de donación para las personas que requieren uno; y la segunda, los miles de individuos que requieren órganos alrededor del mundo, la facilidad de comunicación inmediata que otorgan las nuevas tecnologías, así como la solvencia económica de las familias de las personas que requieren de un órgano (García Arango, 2010, p. 273).

Las posturas anteriores se ven encontradas entre la donación y la compraventa de órganos. Es compartida la postura entre las legislaciones latinoamericanas acerca de la prohibición de la venta de estos órganos, y ejemplo de ello lo vemos en el derecho mexicano (Ley General de Salud, art. 327). Partiendo de lo expuesto, establecemos los argumentos a favor y en contra de estas dos posturas.

De los argumentos en contra, tenemos en primer lugar la comercialización. Ésta se refiere a la obtención de recursos económicos por medio de la venta de órganos, la cual podría convertirse en una situación de explotación. Ello es así, a causa de una persona que está en un estado de superioridad respecto de otra (Mocoroa, 2014, p. 501). Por ejemplo, un empresario podría pagar a personas con problemas económicos para que les vendan órganos vitales y éste a la vez revenderlos. Sin embargo, en esta situación se distingue el estado de necesidad en el que se encuentran las personas que deciden realizar esta venta, por lo cual como indica Juan Manuel Mocoroa "es la situación de injusticia y de miseria en la que una persona está situada lo que nos provoca la perplejidad moral." (Mocoroa, 2014) "De tal suerte, que el ejercicio de su autonomía la lleve a aceptar, necesariamente, recurrir a la venta de partes de sus órganos para intentar salir de la precariedad en la que está inmersa" (Mocoroa, 2014).

Por otro lado, los argumentos a favor estipulan dos posturas: la primera se refiere a la escasez de órganos para la realización de trasplantes; y la segunda, al derecho de propiedad sobre el propio cuerpo.

Así como en el mundo físico existe venta de órganos y esto es derivado por diversas circunstancias, tanto por problemas económicos o por el simple hecho de tener un ingreso monetario, la red cada vez es testigo de estas acciones (Bilefsky, 2012). Esta funge como un medio ideal para anunciar las ofertas establecidas por cada órgano, siendo una plataforma para personas en todo el mundo. A raíz de esta circunstancia, García Arango realizó una investigación con el objetivo de analizar las implicaciones éticas y jurídicas de la disposición con motivación económica de componentes humanos desde

IUS ET SCIENTIA • 2022
Vol. 8 • N° 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

la perspectiva de las personas que ofrecían sus órganos a través de Internet con intereses monetarios (García Arango, 2010). De los resultados obtenidos es importante señalar las siguientes conclusiones:

a) De todo el trabajo de las encuestas puede concluirse que Internet se muestra como un escenario nuevo y distinto donde se presentan situaciones particulares de repercusiones éticas y jurídicas.
b) El espacio común utilizado en Internet para ofrecer órganos y demás componentes humanos son las páginas comerciales.
c) La mayoría de los oferentes son jóvenes.
d) La mayoría de las personas apuntan a que el acto de la venta de órganos no es ético pero la necesidad es mayor.
e) Es recurrente ver la acción de vender un órgano como un beneficio mutuo, como un acto de generosidad compensado, como una ayuda altruista y meritoria.

De las conclusiones podemos desprender que, si bien es verdad que existe una necesidad económica que abre las puertas al negocio de órganos que se busca como una opción a la crisis, también es cierto que no es el único estímulo. Por otro lado, para algunas personas la venta de órganos es una acción bondadosa, que tiene más beneficios que perjuicios, en virtud que puede salvar vidas en algunos casos.

Esta situación nos demuestra que aquellas medidas tomadas por los Estados, por las supuestas intenciones comerciales y la posibilidad de explotación de órganos, puede ser que en algunos casos no exista, ya que para algún grupo de individuos el hecho de realizar una venta de sus propios órganos resulta ser una acción bondadosa y hasta cierto punto caritativa, donde ambas personas (comprador/vendedor) ganan.

3.3. Ciberguerra

Cuando escuchamos la palabra guerra, nos imaginamos soldados fuertemente armados, un grupo de terroristas, o narcotraficantes. Estas figuras las relacionamos con un espacio determinado, es decir, un campo de batalla que es el lugar donde se sitúa la conflagración. Con la llegada de las nuevas tecnologías, los equipos armamentistas crecieron de una forma desenfrenada, creando nuevas armas, más lesivas y con mayor alcance destructor. Así como los instrumentos de guerra han evolucionado, también los campos de batalla lo han hecho, pasando de lugares físicos a lugares virtuales donde los choques de intereses no se pueden percibir, pero las consecuencias materiales sí.

Resulta relevante para el presente trabajo la *ciberguerra* o *guerra informática o cibernética*, en virtud que así como en las batallas convencionales se violan infinidad de derechos fundamentales siendo uno primordial la vida, en una guerra virtual también, mismos que pueden ser violentados directa o indirectamente.

Para Dorothy Denning (2007), existen tres áreas de ciberconflicto donde las cuestiones éticas son más problemáticas:

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

a) *La ciberguer*ra. La mayoría de los ciberataques parecen ser claramente sin ética e ilegales. Existen ataques realizados por diversión, virus lanzados por curiosidad e ignorando sus consecuencias.
b) *Dilemas éticos involucrando Estados no actores cuyos ciberataques son política o socialmente motiv*ados. Esta área se refiere al hacktivismo, derivado de conflictos. Ello es una confluencia de hacker y activismo. Si el ataque esta designado a ser suficientemente destructivo y severamente perjudicial que aterroriza civiles, esto se convierte en ciberterrorismo, la integración de ciber-ataques con terrorismo.
c) *Ética de defensa*. Es llamado hackback, strickback o respuesta activa.

Otros ataques pueden ser:

a) A páginas web dirigidas solo por diversión y virus lanzados por curiosidad pero ignorando sus consecuencias.
b) Intrusión en sistemas para robar números de tarjetas de crédito o comerciar datos personales.
c) Negación de servicios pretendidos para atacar páginas web competidoras o extorsionar dinero de víctimas.
d) Que compromete y despliegan largos robos automáticos (bonets) de computadoras víctimas para emitir spam o amplificar ataques de negación de servicios.

A pesar de que no existe una definición clara de lo que representa una guerra cibernética, puede ser considerada como ataques malintencionados perpetuados a través de causes electrónicos (Wegener, 2001, p. 132), tomando como escenario principal el ciberespacio.

Para Henning Wegener (2001), los ataques que atentan contra la seguridad de la información se pueden distinguir en tres ámbitos: 1. los perpetrados contra las redes de comunicación del sector económico; 2. la política de defensa de la información respecto a los ataques perpetrados contra infraestructuras clave dentro de cualquier sociedad; y 3. cuando los ataques se dirigen contra las estructuras de seguridad nacionales e internacionales.

El primero, se refiere a espionaje industrial y a la piratería; sus repercusiones pueden extenderse hasta propiciar la falsificación de un entorno de decisión determinado y la confusión en la dirección de empresas como fraude. El segundo, se refiere a aquellos aspectos en que la sociedad está inmersa debido a la digitalización como control y gestión de ordenadores en lo relativo a sistemas bancarios, servicios hospitalarios, tráfico aéreo, etcétera. Las consecuencias podrían llegar a ser perturbadoras y devastadoras para una población. El tercero, toma el concepto de ciberguerra prácticamente toda vez que los ataques se dirigen contra las estructuras de seguridad nacional e internacional.

El Derecho Internacional de Conflictos Armados (DICA) tiene dos partes: *jus ad bellum* (ley de conflictos de administración); y *jus in bello (*ley de guerra). Estas figuras de la mencionada ley están referidas al uso de la fuerza, particularmente fuerzas armadas;

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

la primera especifica cuándo la fuerza puede ser aplicada, mientras que la última cómo puede ser empleada.

Ambas leyes están conformadas por principios éticos. Bajo las leyes internacionales, Estados y entidades soberanas, asumen obligaciones legales internacionales solo para afirmar el acuerdo a ellos. El DICA está diseñado para promover paz y minimizar el efecto adverso de la guerra en el mundo. Dentro de la misma, se establece como regla general, que los Estados no tienen permitidos a atacar a otros, excepto como un medio de autodefensa. Cuando un conflicto surge, la ley tiende asegurar que la guerra sea peleada lo más humanamente posible, minimizando daños colaterales; por lo cual se dice que tiende a prescribir ampliamente principios éticos.

Michael Schmitt ofrece siete criterios para distinguir operaciones que usan la fuerza económica, diplomática y otras leves medidas. Para cada criterio hay una gama de consecuencias del alto final, parecido al uso de fuerza leve; y el final bajo, parecido a medidas leves. Estas son las siguientes (Denning, 2007):

1. *La severidad*. Se refiere a personas asesinadas o heridos y daño en propiedad.
2. *La inmediatez*. Es el tiempo que toma para las consecuencias de una operación en causar efectos.
3. *La franqueza*. Es la relación entre una operación y sus efectos. Por un ataque armado, efectos son generalmente causados por y atribuibles a la aplicación de fuerza, mientras que medidas leves podrían tener explicaciones múltiples.
4. *La invasibidad*. Éste se refiere a si una operación involucra cruzar las fronteras en el país objetivo.
5. *La mensurabilidad*. Ésta es la habilidad de medir los efectos en una operación.
6. *La presunta legitimidad*. Se refiere a si una operación es considerada legítima dentro de la comunidad internacional.
7. *La responsabilidad*. Éste se refiere al grado de cuyas consecuencias de una acción pueden ser atribuibles a un estado opuesto a otros actores.

Estos criterios que nos presenta Schimitt, nos sirven de parámetro para determinar el grado de agresión que provoca un ciberataque dependiendo del contexto en el que se encuentra. Toda vez que las consecuencias no son las mismas entre un ataque a un robot que realiza una apendicectomía y una torre de control en un aeropuerto internacional, ya que en el primero, las pérdidas humanas y económicas son menores, en comparación con el segundo.

De lo establecido podemos determinar dos puntos que resultan favorables para las personas que realizan ciberataques: *a.* el *anonimato*; y *b.* la *efectividad*. La identidad de los individuos que realizan estos actos se ve protegida por las características de la red, pero también la efectividad de estas acciones son casi contundentes. A raíz de ello, especialistas en la materia esperan un incremento en los ciberataques en la próxima década, debido a que cada vez más nuestra vida se va moviendo en relación con la tecnología y nuestras actividades cotidianas dependen de ésta (Dredge, 2014, The Guardian). Vehí-

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

culos autodirigidos, intervenciones quirúrgicas realizadas por robots y nuevos medios de transporte son algunos ejemplos de ello.

Como ejemplo a estos ataques podemos mencionar el ciberataque global registrado el 12 de mayo de 2017, causado por el *ransomware* WannaCry, explotando las vulnerabilidades del Sistema Operativo Windows, el cual una vez instalado encriptaba documentos y pedía un pago para decriptarlo (Symantec Security Response).[3] Éste es solo una pequeña muestra de cómo un ataque de este tipo puedo paralizar a un Estado o al mundo entero.

3.4. Pornografía infantil

La pornografía infantil es toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un menor con fines primordialmente sexuales (A/RES/54/263, UNICEF, junio 2006, p. 41). Aquella ha ido en aumento en Internet debido a sus ganancias de 30 mil millones de dólares al año (Holder, 2011). Esto se debe a sus características intrínsecas, sin embargo, no todo es negativo, ya que gracias a Internet se han podido detectar redes de pedófilos. Por otro lado, existen sociedades, como la japonesa (Fackler, 2014) en donde se establecen excepciones a la pornografía infantil, debido a sus tradiciones culturales, ya que ésta se permite en dibujos (mangas). A pesar de esta excepción, la pornografía infantil es legítimamente prohibida para proteger el interés superior del menor, en virtud que involucra abuso en el acto sexual o explotación de niños, con o sin consentimiento, mismos que no son competentes para entender la naturaleza de la elección que están haciendo o comprender el impacto de sus decisiones en sus presentes y futuros intereses (West, 2011, Stanford).

Por otro lado, es importante indicar que un problema relacionado con la pornografía en general es la categorización del contenido en la red, como legal e ilegal y las consecuencias del mismo. Es evidente la ilegalidad de la pornografía infantil por lo anteriormente expuesto, sin embargo, la pornografía es legal para los mayores de edad, sin que exista una regulación del contenido y nocividad de la misma. Esta regulación de la pornografía nace de una postura conservadora que indica que aquella debe ser prohibida debido a que su contenido sexualmente explicito es obsceno y moralmente perverso, asimismo indica que el Estado está legitimado para prohibirla basado en la protección de la salud moral de las personas. Contrario a ello, la postura liberal defiende el derecho a la pornografía con fundamento en tres puntos (West, 2011): la libertad de expresión; el derecho a la privacidad; y el comparativo de daño. El *primero* se refiere a la protección de la libertad de los individuos para expresar sus opiniones y comunicarla a otros; el *segundo*, al derecho a la privacidad que tienen los individuos y la posibilidad de que el consumidor no afecte a otros, siendo el único que lo visualiza, sin afectar la esfera de los

3. Symantec Security Response, *Ransom WannaCry*, *https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99*.

IUS ET SCIENTIA • 2022
Vol. 8 • N° 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

demás; y el tercero se refiere al *principio del daño*, el cual se refiere al daño que hace la pornografía a las personas que lo consumen y a los demás, en comparación con otras acciones como violencia psicológica o violaciones de derechos.

Si bien para algunos la pornografía es una violencia o un sometimiento para la mujer, para otros es una forma de entretenimiento y un negocio muy redituable que es permitido en numerosas naciones. De igual forma, en lo que cada postura puede concordar fielmente es en la negativa sobre la pornografía infantil y sus consecuencias.

Es cierto que existe una diferencia enorme entre la pornografía en general y la infantil, sin embargo, estos contenidos se mezclan en la red, creando un problema de selección y clasificación. Podemos clasificarlos en dos tipos principales que son: el contenido legal y el ilegal. En cuanto a primero, tenemos a la pornografía que no es nueva y no siempre es vista como un problema; y el segundo la pornografía infantil, que la sociedad la percibe como un problema y es criminalizado por la Convención de los Derechos del Niño y la Convención de Cibercrímenes del Consejo Europeo. Entre estas categorías, existe el contenido acosador y amenazador, como por ejemplo el racismo y el discurso de odio. En relación a ello, Yaman Akdeniz señala que "Debe ser conocido que los cuerpos encargados de hacer cumplir la ley se preocupan sobre el uso de Internet relacionado crímenes existentes como fraude y la emergencia de cibercrímenes, tales como acceso no autorizado a redes de computadoras (hacking), distribución de virus de computadoras,…,y ataques de negación de servicios". Por lo cual las autoridades dejan a un lado acciones ilícitas como la pornografía infantil y se encargan de delitos que a su parecer resultan ser más graves.

A raíz de ello, distintas autoridades gubernamentales en el mundo han fomentado la creación de sistemas de clasificación y filtros, así como agencias de policía cibernética para la captura de grupos de pedófilos. Estas acciones son motivadas desde la vía jurídica, sin embargo no hay que pasar por alto, que una de las mejores formas de prevenir estos contenidos, es mediante el fomento de valores y una ética cívica que se puede aplicar en el mundo digital. Si bien, no podemos evitar directamente que un menor visualice en la calle una revista de contenido sexual explícito, ya que está a la vista de todos; es verdad que podemos explicarle el daño moral y los fines del mismo.

IV. Conclusión

El Estado ha sido y será la base para el desarrollo tecnológico, éste es quien promueve las políticas públicas para fomentar nuevas tecnologías o para limitarlas. Por lo cual, entre los ciudadanos es donde se reflejan las acciones y medidas que cada uno toma para sus fines.

Asimismo, es evidente la existencia de problemas éticos que se presentan en Internet y que cada vez son más comunes debido al incremento de los usuarios. La red profunda, la venta de órganos en línea, la ciberguera, y la pornografía infantil son apenas ejemplos que mencionamos para plantear algunas de las situaciones que existentes y deben ser estudiadas.

IUS ET SCIENTIA • 2022
Vol. 8 • N° 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

Finalmente podemos establecer que, tanto la injerencia del Estado en la tecnología y los problemas éticos que en la misma se suscitan, son de vital importancia para su compresión y análisis. De esta forma, no todo lo que existe en Internet es negativo, sino que éste también ha traído aspectos positivos, como una comunicación rápida entre las personas y una mayor amplitud para nuestras libertades, como la de expresión, así como una protección a nuestra privacidad e intimidad. Al final del día, somos nosotros los usuarios quienes decidimos como utilizar esta herramienta tecnológica que ha revolucionado el mundo.

Bibliografía

BECKETT, A. (2009). The dark side of the Internet, In the deep web, The Guardian, http://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet

BILEFSKY, D. (2012). Black market for body parts spread among the poor in Europe, NewYork-Times, http://www.nytimes.com/2012/06/29/world/europe/black-market-for-body-parts-spreads-in-europe.html?pagewanted=all&_r=0

Castells, M. (2011), vol. I., La era de la información. Economía, Sociedad y Cultura. La sociedad red, México, Siglo XXI,

Chang, K., *et. al.,* Accesing the deep web: a survey, University of Illinois, Computer Science Department, http://brightplanet.com/wp-content/uploads/2012/03/Accessing-the-Deep-Web-A-Survey.pdf.

Denning, D. E. (2007), The Ethics of Cyber Conflict, http://faculty.nps.edu/dedennin/publications/Ethics%20of%20Cyber%20Conflict.pdf.

Dredge, S. (2014). Internet experts see 'mayor cyberattacks' increasing over next decade, The Guardian, UK, http://www.theguardian.com/technology/2014/oct/29/major-cyber-attacks-internet-experts

Fackler, M. (2014)., Japan outlaw possession of child pornography, but comic book depictions survive, The New York Times, http://www.nytimes.com/2014/06/19/world/asia/japan-bans-possession-of-child-pornography-after-years-of-pressure.html?_r=0

García Arango, G. A. (2010), Compraventa de órganos por internet: conceptos éticos y jurídicos de los oferentes, *Revista Facultad de Derecho y Ciencias Políticas,* Colombia, núm. 113, vol. 40, julio-diciembre.

Holder Jr., E. (2011). Child Pornography, https://www.justice.gov/criminal-ceos/child-pornography

Internet World Stats, Usage and Population Statistics, http://www.internetworldstats.com/asia/kr.htm *y* http://www.internetworldstats.com/am/mx.htm

Lazcano Ponce, E. (2013), La Política de Ciencia y Tecnología en México" Secretaría de Salud, http://www.insp.mx/avisos/2872-politica-ciencia-tecnologia-mexico.html

Mann, O. (2016). Inside the darknet, Chips for everything, *The Guardian*, https://www.theguardian.com/technology/audio/2016/jun/15/inside-the-darknet-chips-with-everything-tech-podcast.

Mocoroa, J. M. (2014). XLVII, núm. 140, Venta y donación de órganos en la ley de ablación e implantes argentina: algunos problemas bioéticos, *Boletín Mexicano de Derecho Comparado.*

IUS ET SCIENTIA • 2022
Vol. 8 • Nº 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05

Plan Nacional de Desarrollo, 2013-2018, DOF 20/5/2013 (36) http://pnd.gob.mx/wp-content/uploads/2013/05/PND.pdf.

Rawls, J. (2011). Teoría de la Justicia. México. FCE

Symantec Security Response, *Ransom WannaCry*, https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99.

Tamayo y Salmorán, R. (2011). Introducción Analítica al Estudio del Derecho. 2a ed., México. Themis.

Téllez Valdés, J. (2013). Lex Cloud Computing, Estudio Jurídico del Cómputo en la Nube en México, México, UNAM-IIJ-Microsoft.

The Children's Commission on Poverty, *At What Cost? Exposing the impact of poverty in school life. Executive Summary*, UK, The Children Society, October 2014, https://www.childrenssociety.org.uk/sites/default/files/At%20What%20Cost%20Exposing%20the%20impact%20of%20poverty%20on%20school%20life%20-%20report%20summary.pdf.

WEGENER, H. (2001). La guerra cibernética, *Política Exterior*, no. 80. http://m.unibw.de/infosecur/documents/published_documents/guerra_cibernetica.

WEST, C. (2012), Pornography and Censorship, *Stanford Encyclopedia of Philosophy*, USA, revision. http://plato.stanford.edu/entries/pornography-censorship/

IUS ET SCIENTIA • 2022
Vol. 8 • N° 2 • pp. 66-79
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2022.i02.05