El estado actual del cibercrimen en Perú y el derecho alemán

The Current State of Cybercrime in Peru and German Law

Luis Alberto Jimenez Bernales

https://orcid.org/0000-0002-2555-1576
Universidad Peruana de Ciencias Aplicadas (UPC). Perú
Correo electrónico: pcdeljim@upc.edu.pe

Recibido: 7 de julio de 2023
Aceptado: 14 de marzo de 2024

DOI: https://doi.org/10.22201/iij.24484873e.2023.167.18367

Resumen: Poco más de dos décadas desde que Internet se masificó en gran parte del mundo, ya no sólo como utilidad para enviar o recibir un correo electrónico o para buscar algún dato curioso, sino también para el uso de aplicaciones que facilitan sustancialmente la vida de las personas: pagar cuentas en línea, soportes inteligentes para los múltiples dispositivos y teletrabajo; el dinamismo en esta nueva forma de interacción social no podría darse sin Internet. Sin embargo, este devenir tecnológico también implica una serie de riesgos que en los últimos años se han acrecentado en Perú y en el mundo; como la apología al terrorismo, la pornografía infantil, la piratería, la difamación, son ejemplo de los riesgos en el ciberespacio que cada día se vuelven más comunes en una sociedad posindustrial. Vista esta realidad problemática, el objetivo de este trabajo es evidenciar los riesgos a los que se encuentran expuestos los bienes jurídicos, cuando el proveedor de Internet no suministra ningún mecanismo preventivo (sistema de inteligencia artificial) para combatirlo. Al finalizar este estudio, se concluirá que las medidas de autorregulación (cumplimiento) son apropiadas para controlar las plataformas como fuentes de peligro. Se sugerirá al legislador peruano establecer una regulación que obligue a los proveedores de servicios a monitorear sus plataformas para prevenir la violación de bienes jurídicos en el ciberespacio.
Palabras clave: ciberdelincuencia, ius puniendi, política criminal, medios digitales, sociedad de riesgo.

Abstract: Little more than two decades since the Internet became widespread in much of the world, not only as a utility to send or receive an email or to search for some curious information, but also for the use of applications that substantially facilitate people's lives: paying bills online, intelligent supports for multiple devices and teleworking; the dynamism in this new form of social interaction could not happen without the Internet. However, this technological evolution also implies a series of risks that in recent years has increased in Peru and the world,

such as the apology to terrorism, child pornography, piracy, defamation, are an example of the risks in cyberspace that every day become more common in a post-industrial society. Given this problematic reality, the objective of this work is to highlight the risks to which legal assets are exposed, when the Internet provider does not provide any preventive mechanism (artificial intelligence system) to combat it. At the end of this study, it will be concluded that self-regulatory (compliance) measures are appropriate to control platforms as sources of danger. It will be suggested to the Peruvian legislator to establish a regulation that obliges service providers to monitor their platforms to prevent the violation of legal goods in cyberspace.
Keywords: cybercrime, ius puniendi, criminal policy, digital media, risk society.

I. INTRODUCCIÓN

El siglo XXI empezó con una avalancha de cambios en el ámbito tecnológico: el paso de lo analógico a lo digital. Una sociedad cada vez más predispuesta a adaptarse a los ámbitos virtuales donde Internet sirve de base para formas de comunicación no convencionales, como las redes sociales, pero también donde poco a poco empezamos a mostrar información personal como gustos, consumos, estadías y, sin darnos cuenta, estamos ofreciendo información personal que nos coloca en una posición vulnerable.

Internet ofrece ventajas para la investigación, comunicación y la economía; hace la vida mucho más fácil. También ofrece desventajas, ya que puede ser una herramienta que facilite la comisión de delitos, como la pornografía infantil, delitos contra el honor, apología del terrorismo, delitos contra la propiedad intelectual, entre otros. Por tanto, esta facilidad que se tiene con las redes digitales va asociada a riesgos que pueden lesionar bienes jurídicos, como la indemnidad sexual, la tranquilidad pública y los derechos de autor (T. Hörnle, 2002, pp. 1008-1013).

La difusión de contenidos delictivos en estas plataformas constituyen una violación a los bienes jurídicos antes mencionados y, por ende, requieren de una atención prioritaria por parte del Estado. Las personas que cometen estos ilícitos penales se valen de las deficiencias de protección que existen en el ciberespacio para obtener sus propios beneficios, permitiendo que el libre acceso y el anonimato favorezcan la aparición de estos crímenes.

Establecer la identidad del ciberdelincuente suele ser técnicamente complejo y puede resultar hasta imposible, debido a que estas personas operan utilizando servidores que proporcionan una red privada virtual,[1] encubriendo su dirección[2] y usando cualquier elemento que facilite su clandestinidad. Para el análisis se considerará el caso de las redes sociales, plataforma en la que se obtienen innumerables beneficios al utilizarlas no sólo para subir alguna foto personal que se quiera compartir, sino también como medio de comunicación cada vez más personalizado. Lamentablemente, con esta forma de comunicación, la libertad de expresión se confunde con la permisibilidad para brindar noticias sin sustento o *fake news* con el propósito de manipular o engañar a la gente.

Este ejemplo permite formular los siguientes cuestionamientos: ¿hasta dónde debe llegar la injerencia de los proveedores de servicio en Internet (ISP) para evitar la lesión de un bien jurídico?, y, además, ¿existe alguna regulación de prevención de riesgos en el uso de Internet? Estas interrogantes serán abordadas en el desarrollo del presente trabajo de investigación. En ese sentido, se identifica si el uso de estas plataformas y las medidas adoptadas por los ISP se convierten en una sociedad de riesgo y cómo debería actuar el derecho penal.

II. Consideraciones generales de la comunicación en Internet

1. Antecedentes

En su afán de seguir revolucionando el mundo entero, Estados Unidos no sólo se conformó con llevar al primer hombre a la Luna en 1969, sino que buscó la manera de fortalecer su sistema de defensa a través de una red de comunicación que le permitió conectarse y comunicarse con diferentes

[1] De acuerdo con Cisco (2024) el servidor de red privada o las siglas comúnmente utilizadas VPN, lo cual en grandes rasgos es una conexión segura que cifra el tráfico de Internet y mantiene oculta la identidad del usuario en línea. Por ende, se puede considerar una manera efectiva de ocultarse ante los demás usuarios en línea.

[2] Para ello se utiliza una dirección única denominada protocolo de Internet o las siglas comúnmente utilizadas IP, de acuerdo con Kaspersky (2023) esa dirección funciona como identificador para dispositivos en Internet o redes locales.

instituciones y departamentos a la vez. De esta manera, afianzó su poderío frente a otras potencias en plena Guerra Fría. Es así que en 1969 el Departamento de Defensa de los Estados Unidos crea *Arpanet*, un sistema de conexión diseñado con fines bélicos, el cual constituye el primer antecedente de transmisión de información entre departamentos gubernamentales de aquella época (Tolksdorf,1997, p. 2; Sieber, 1996, pp. 429-442). Este hecho marco un hito en la historia de la comunicación, pues aunque en sus inicios fue creada para codificar y transmitir información militar clasificada del gobierno estadounidense, fue la base para el sistema globalizado de redes que hoy nos es indispensable.

Este sistema pronto sería masificado y su uso llegó a algunas universidades de los Estados Unidos, logrando grandes avances para la investigación científica, la comunicación y educación del país del norte. Su expansión al resto del mundo se realizó a través de la creación de Internet en 1981 (Schmidl, 2014, p. 140; Seitz, 2004, p. 5). Un aporte importante que hizo el científico Tim Berners Lee, considerado padre de la *web*, por crear *la World Wide Web*[3] (www) quien, en 1989, logró unir el protocolo de transferencia de hipertextos (HTTP) e Internet, con lo cual consiguió interconectar los servidores *webs* de distintas partes del mundo y facilitó el acceso y búsqueda de información de una forma sencilla a través de una dirección web.

Dichos avances también se implementaron en Perú en 1991. La Red Científica Peruana[4] (RCP) se encargó de instalar la primera cabina pública de Internet en el Centro Cultural Ricardo Palma, lo cual generó un impacto en el sector académico. Su principal herramienta fue el correo electrónico. Posteriormente, las tendencias y el proceso de globalización posibilitaron que Internet sea parte crucial en la forma de interrelacionarnos, pues actualmente es una herramienta indispensable para el desarrollo de la sociedad.

Finalmente, en 2012 la libertad en Internet fue declarada un derecho humano por el Consejo de Derechos Humanos de la ONU,[5] que instó a los

[3] La World Wide Web (WWW) o red informática mundial, es un sistema que funciona a través de Internet, por el cual se pueden transmitir diversos tipos de datos a través del Protocolo de Transferencia de Hipertextos, que son los enlaces de la página web (Canal DW Español, 2022, 1m19s).

[4] Según la Red Científica Peruana (2024) la motivación principal para crear esta asociación fue la de promover el desarrollo comuntario y el acceso de los individuos a las nuevas tecnologías.

[5] De acuerdo con el Consejo de las Naciones Unidas (A. G. NU, 2012, A/HRC/20/L.13)

Estados a promover y fomentar el acceso a la red y a garantizar que los derechos a la libertad de expresión e información, tal y como se recogen en el artículo 19 de la Declaración Universal de Derechos Humanos,[6] se respeten tanto en línea como fuera de ella.

A. El concepto de información digital

El término "información" proviene del sustantivo latino "*informationis"* y del verbo *"informare",* los dos en forma conjunta significan "dar forma a la mente, enseñar". Al añadirse el adjetivo "digital", se refiere a los datos codificados en una secuencia electrónica que rodea a la sociedad producto de la globalización. De esta manera, se establece un tipo de "comunicación" entre el usuario y los diferentes sistemas informáticos.

Algunos ejemplos de servicios electrónicos de información y comunicación de acuerdo con T. Hoeren *et al.* (2019, p. 3720): ofertas en línea (oferta de datos bursátiles, grupos de noticias, salas de chat, prensa electrónica, texto de televisión/radio, televenta), video a la carta (en la medida en que no es un servicio de televisión, sino ofertas dadas por Netflix, Amazon Prime), servicios en línea que proporcionan herramientas para la búsqueda, el acceso o la recuperación de datos (por ejemplo, Internet, motores de búsqueda), la difusión comercial de información personal por correo electrónico (por ejemplo, correos publicitarios), instituciones financieras que brindan sus servicios por telebanca y también aplicativos. Los ejemplos brindados sobre dónde se encuentra la información digital serán de utilidad para el análisis posterior.

B. Anonimato, descentralización, sobrecarga de información

Dado que "los datos o la información en Internet pueden ser accesibles para todo público, esto genera una potencial vulnerabilidad en la vida de muchos usuarios" (Thiedeke, 2004, p. 15). La creación de cuentas resulta tan simple que prácticamente no se pide ninguna identificación real; así que el registro

---

el acceso a Internet fue reconocido como una herramienta para promocionar el desarrollo de los países miembros; por ende, la Asamblea General de las Naciones Unidas también enmarco algunas responsabilidades que emergen de este derecho.

6 La Declaración Universal de los Derechos Humanos de las Naciones Unidas indica en el artículo 19: toda persona tiene el derecho de expresar sus puntos de vista sin limitaciones, explorar, recibir y compartir información libremente.

en foros o grupos de chat puede ser con apodos, nombres artísticos o seudónimos. La inscripción está automatizada por orden de llegada; lo único que se comprueba es que el nombre de dominio no haya sido asignado a otra persona en otro lugar del mundo (Heß, 2005, p. 19). Pueden existir muchas razones para este anonimato: algunos temen que sus vidas o medios de subsistencia estén en peligro o que puedan sufrir desventajas políticas o económicas. Otros quieren evitar la discriminación o simplemente utilizar un nombre que sea más fácil de recordar o escribir (Hoeren, 2018, p. 670). Sin embargo, este anonimato o simple necesidad de tomar un nombre original porque el reconocimiento exclusivo de un grupo así lo exige, puede tener consecuencias negativas para la sociedad, debido a que los usuarios pueden cometer delitos gracias a este anonimato que Internet concede (Rath, 2016, p. 293).

La descentralización también se aplica en Internet, pues la red no tiene ordenadores centrales. En este sentido, cada IP puede administrar un servidor; por tanto, no hay un punto de control central. Como los ISP se comunican entre sí a través de servidores, la información fluye sin pausa; así, el servidor desencadena una avalancha de datos, debido a que siempre está conectado a Internet. Esta circunstancia se resume en las palabras clave "Flujo de información" e "información dinámica" (Rath, 2016, p. 20).

C. La red como fuente de peligro

Los avances en el campo del procesamiento electrónico de datos, las nuevas tecnologías de la información y la comunicación pueden simplificar nuestra vida, y también se muestran como un riesgo cada vez más palpable para la sociedad (Espinoza Bonifaz, 2020, pp. 10-20). Los peligros que plantea la red son: la difusión de pornografía infantil, la incitación a la violencia, las violaciones a los derechos de autor, entre otros delitos (Altenhain, 1997, p. 485).

De acuerdo con el reporte de información estadística elaborado por el Ministerio de Justicia y Derechos Humanos de Perú, entre enero de 2013 y diciembre de 2021 se registraron 14,671 delitos cometidos por medios informáticos (Ministerio de Justicia, 2022 p. 10). Asimismo, según el Ministerio Público del Perú (2023) se ha incrementado en 2,508 casos registrados en comparación con el año anterior, observando que el número de delitos perpetrados por medios informáticos ha tenido un crecimiento año con año, debido a que la población en los últimos años ha realizado operaciones en linea de forma masiva para evitar el contagio del COVID-19. No obstante,

las estadísticas antes mencionadas no reflejan el alcance real, ya que sólo una pequeña parte de los delitos en este ámbito se denuncian. El bajo riesgo de detección hace que Internet sea interesante para que los delincuentes cometan los delitos mencionados (Spindler, 1997, p. 3193).

En ese sentido, el uso de Internet constituye un mecanismo a través del cual los usuarios se exponen constantemente, y ante ello los mecanismos jurídicos no están siendo lo suficientemente eficientes.

Por consiguiente, un servidor se consideraría una fuente de peligro; asimismo, como menciona C. Pelz (2002, p. 138) Internet puede considerarse una fuente de peligro, ya que por medio de ésta se puede reenviar el mismo contenido a otros innumerables ordenadores en muy poco tiempo. De este modo, el peligro que supone el contenido almacenado se multiplica muchas veces. Puede agregarse que quien no supervisa o vigila su plataforma virtual, debería ser considerado partícipe del hecho delictivo cometido por un tercero, al coadyuvar a la realización de la violación de un bien jurídico.

En los medios de comunicación tradicionales como la prensa, la televisión y la radio, el redactor, el editor y la persona que dio la información falsa son fácilmente identificables. Por el contrario, Internet permite al creador de contenidos ilegales disfrazar su identidad o la legalidad y originalidad de sus trabajos. Esta posibilidad de anonimización de datos favorece que los usuarios utilicen Internet para cometer delitos (Heckmann, 2012, p. 2631).

2. Aproximaciones jurídicas, dogmáticas, de los delitos informáticos

A. El ciberdelincuente como enemigo de la sociedad de la información

El derecho penal del enemigo constituye un mecanismo de política criminal que regula el trato con aquellos sujetos que no pueden ser considerados ciudadanos por representar un peligro para el Estado y para la sociedad, remplazando al Estado de derecho por un Estado de excepción (Jakobs y Cancio Meliá, 2003, p. 19).

Este concepto ha sido ampliamente discutido, llegando incluso a debatirse con ahínco si es o no constitucional determinado tratamiento punitivo a personas que, de una u otra forma, han delinquido o están en posibilidad de hacerlo.

ISSN: 2448-4873
DOI: https://doi.org/10.22201/iij.24484873e.2023.167.18367

Cuando G. Jakobs y M. Cancio Meliá (2003, p. 47) mencionan que a determinadas personas por su condición de peligrosidad se les debe dar un tratamiento distinto, hacen referencia a que son enemigos de la sociedad, pero no desconocen su condición de ser humano. Para ellos hasta el más peligroso terrorista debe ser tratado y procesado con todas las garantías de un debido proceso. Se trata, por ello, de una especie de "neutralización" de personas que llamaríamos criminales en circunstancias más tradicionales, pero que se desenvuelven bajo los mismos parámetros sociológicos.

Estos juristas consideran que el Estado debe tratar a esta clase de delincuentes como enemigos que cometieron un acto ilícito y a los que hay que impedir, mediante coacción (sanción, en sus palabras) que defrauden la norma nuevamente. Independientemente del nivel de peligrosidad del criminal, se aplica la fuerza del Estado, sin perjuicio de lo mencionado. También es cierto que cuando el individuo no quiere comportarse conforme a derecho, la labor de la pena se enfoca a tratar de reformar su conducta y adecuarla de nuevo al respeto de la norma. Por ello, la idea central de su postura radica en que no se puede concebir la lucha contra la delincuencia sin imponer medidas de prevención severas, las cuales protegerán el ordenamiento jurídico y a la vez influirán en el comportamiento del delincuente (esta última manera de actuar del Estado se adecua a la prevención especial). Pero se debe respetar siempre los derechos de las personas y las garantías propias que el proceso le reconoce (Jakobs y Cancio Meliá, 2003, p. 47). Por consiguiente, el tratamiento distinto que se les da a determinadas personas por su peligrosidad no supone la vulneración de principio alguno, pues éste se fundamenta en la reacción jurídico penal del Estado.

En relación con los ciberdelincuentes (enemigos), tienen todas las herramientas para hacer colapsar al mundo. El enemigo puede estar sentado a tu lado, con su *laptop* en el restaurante al que acudes cualquier fin de semana, poniendo de cabeza la web, con la apología del terrorismo, la piratería, la propagación de pornografía infantil. Debido a esta situación, el ciberenemigo ha alcanzado una escala mundial con la revolución digital. Los riesgos son más complejos, sistémicos y difíciles de predecir por la creciente interconexión e intercambio de datos entre usuarios, empresas y gobiernos. Estos riesgos se derivan de los cambios significativos en la tecnología, como la concentración de nuestros datos en una "Nube", la democratización de los teléfonos inteligentes, las aplicaciones colaborativas y los dispositivos conectados.

En vista de esta realidad, el gobierno debería enfocarse en la autorregulación de las entidades privadas mediante programas de cumplimiento para prevenir el riesgo de datos, información y recursos alojados en un servidor. En la actualidad, es más complicado intervenir en las redes de un país como Alemania, ya que las grandes potencias cuentan con protecciones más efectivas. En consecuencia, es necesario que los gobiernos actuales fomenten una cultura de prevención antes de que se produzca la lesión de un bien jurídico.

B. Prevención punitiva en Internet

Como quiera que los avances tecnológicos han traído mejoras en la calidad de vida de las personas y la sociedad en general, éstos también han tenido íntima relación con la expansión de las nuevas formas de criminalidad (Silva-Sánchez, 2012, p. 291). Situación que ha supuesto repensar los valores orientadores mediante los cuales el legislador crea tipos penales e impone sanciones a nuevas conductas prohibidas, debido al avance de la ciberdelincuencia, hecho que atenta la confidencialidad, la integridad, la reserva de datos y genera espacios para el uso fraudulento de los sistemas informáticos.

Tan es así, que este flagelo social según L. Zúñiga Rodríguez (2020, p. 96) se convirtió en un problema de orden global al comprender los ámbitos empresariales, económicos y políticos. Además, el anonimato, la red y la globalización le son útiles a los ciberdelincuentes para no ser detectados e identificados con facilidad.

Es evidente que, ante lo precedentemente expuesto, el legislador considere necesario prevenir y aumentar las barreras punitivas para así evitar que este tipo de conductas puedan significar, en un momento dado, un grave peligro para la sociedad. Por ejemplo, después de los hechos acaecidos en los Estados Unidos el 11 de septiembre de 2001, se vivió un cambio fundamental en la forma como se afronta el terrorismo. Podría afirmarse que, desde este punto emblemático para nuestras sociedades, la labor del reconocimiento de información tendenciosa o vulnerable fue de vital importancia, y desde allí parte la necesidad de combatir estos riesgos.

Ha de entenderse mejor la idea que postulaba U. Beck (1998, p. 238), cuando hacía referencia a las sociedades de riesgo: en la actualidad es prácticamente imposible prever todas las situaciones de peligro ya que, debido al desarrollo tecnológico, la criminalidad encuentra nuevas y más comple-

jas formas de delinquir. A raíz del COVID-19 y la consecuente cuarentena, la nula interacción social obligó a todo público que quería mantenerse como un individuo productivo se alineara a la virtualidad y, sin saberlo, formar parte de un grupo vulnerable. Resulta frecuente la apología del terrorismo, la pornografia infantil, la pirateria, a partir de los dispositivos móviles y otros mecanismos, lo cual constituye una nueva forma de criminalidad que era impensable hace treinta años, época en la que U. Beck ideó su teoría.

En consecuencia, la fuerza punitiva del Estado está plenamente justificada en estos casos, a pesar que se configura como un inevitable adelantamiento de la barrera de punibilidad. En este sentido, con ello no se quiere decir que el Estado deba actuar vulnerando derechos fundamentales, sino que su marco de actuación deberá estar enmarcado en mecanismos y estrategias contundentes en defensa de la multiplicidad de bienes jurídicos que se ponen en peligro con estos nuevos tipos de delitos (Beck, 1998, p. 20).

C. Medidas de cumplimiento adecuadas para hacer frente al cibercrimen

Dado que no se puede exigir al ISP que adopte medidas preventivas o de salvamento en un servidor externo que no le pertenece, sí se le puede exigir que tome las medidas preventivas o de salvamento en su propio servidor para evitar el resultado lesivo (Rengier, 2019, p. 475).

Una de estas medidas adecuadas es el control de los datos almacenados en su propio servidor mediante el sistema de filtrado. Otra medida adecuada es eliminar los contenidos ilegales tan pronto como sean detectados. El ISP es el único, aparte del emisor de los datos, que podría impedir, a través de las contramedidas necesarias, que estos contenidos ilegales se remitan a terceros y sean así accesibles a un amplio público a través de Internet. Si el ISP no impide o bloquea el transporte automatizado de los datos ilegales, estaría contribuyendo a la comisión de actos delictivos. Asimismo, según R. Rengier (2019, p. 475), la inacción del ISP constituye un incumplimiento de la acción objetivamente requerida.

Se debe precisar como menciona M. Becker (2018) que la aplicación del sistema de filtrado se remonta a muchos años antes de la entrada en vigor de la nueva Directiva de la Unión Europea (UE) sobre Derechos de Autor (UE, 2019) o del Reglamento de la UE sobre la Lucha contra la Distribución de Contenidos Terroristas en Línea (UE, 2021). Sus antecedentes son la

Ley alemana sobre el Mejoramiento de la Aplicación de las Normas en las Redes Sociales (*Netzwerkdurchsetzungsgesetz* [NetzDG], 2017) y del Tratado Interestatal alemán sobre la Protección de los Menores frente a los Medios de Comunicación (*Jugendmedienschutz-Staatsvertrag* [JMSTV], 2002). Esta realidad hace que los ISP actúen de forma proactiva para proteger sus servidores de la difusión de contenidos ilegales.

En la práctica, se utiliza un *software* "inteligente" muy desarrollado que trabaja con redes neuronales (*deep learning*) para reconocer el contenido. Estos filtros de carga, que ya están integrados en el propio *software* del servidor, se aplican antes de la publicación, es decir, mientras el contenido está todavía en la memoria interna. Si se detecta un contenido ilegal, no se publica y se evita una violación del bien jurídico, ya que el filtrado tiene lugar antes de que el contenido se almacene realmente y se ponga a disposición del usuario (Sieber, 1997, p. 655; Koch, 2005, p. 602). Tanto el bloqueo del acceso y la eliminación de la información ilícita de terceros, como la interrupción del proceso de transmisión de datos respectivos, no plantean grandes dificultades técnicas y son físicamente posibles en términos reales.

Sin embargo, se podría argumentar aquí que el ISP no puede impedir completamente el almacenamiento o la difusión de los contenidos ilegales. La razón es que el control automatizado para detectar estos contenidos puede fallar en determinadas situaciones. Este argumento no es convincente, ya que como es de apreciar en la nueva Directiva sobre Derechos de Autor, que se va a explicar más adelante, se obliga al proveedor a tomar todas las medidas necesarias para evitar las lesiones. Una medida adicional con la que puede contar el ISP para encontrar contenidos ilegales y luego eliminarlos de su servidor es el control manual. Esta posibilidad debe ser utilizada en caso necesario, por lo que está obligado a mitigar las lesiones de los bienes jurídicos en este marco.

D. Razonabilidad del acto

Además de la posibilidad de evitar el éxito en la propagación de contenidos ilegales, también es necesario que la acción a realizar sea razonable para el prestador de servicios (Lackner *et al.*, 2023, Rn. 5; Schönke y Schröder, 2019, Rn. 155). Para evaluar lo que es lógico y razonable (Wessels *et al.*, 2019, Rn. 1216; Fischer, 2024, Rn 82) es necesaria una ponderación caso por caso. En esta situación hay que sopesar el peso y el grado del peligro inminente

para los intereses en conflicto (Stadler, 2005; Spindler *et al*., 2018; Sobola y Kohl, 2005, pp. 443-448); es decir, por un lado, el interés de la víctima o de la sociedad en proteger sus bienes jurídicos, y por el otro, los intereses del proveedor de servicios. En principio, cuanto mayor sea la amenaza para los bienes jurídicos, mayor será el grado de control que se puede exigir al proveedor.

Los críticos se quejan de una restricción irrazonable de la libertad de expresión e información y temen la "cancelación" por medios. Como menciona M. Scheppe (2018) el abogado Christian Stahl, criticó que la NetzDG hace más daño que bien. Como las empresas querían evitar multas millonarias, tomaban la precaución de borrar todo lo que pudiera ser peligroso para ellas, independientemente de que fuera sancionable o ilegal.[7] Esto violaría "claramente" la libertad de expresión de los usuarios. J. M. Balkin (1999, pp. 2295-2298) llama a este fenómeno "censura colateral", que supone que el intermediario tiene un incentivo para censurar en privado porque no es su propia expresión de opinión y quiere escapar de la responsabilidad. Por otro lado, en la sesión 235 del *Budenstag* (2019) la diputada representante de izquierdas (*die linke*), Petra Sitte, criticó la Ley por poner "en manos de particulares" la valoración de la punibilidad de los contenidos, que en realidad es competencia de los tribunales.

Pero no cabe duda de que Internet libre sin ningún tipo de regulación alberga riesgos considerables, como lo ya antes mencionado, la difusión de propaganda terrorista y pornografía, que vulnera la intimidad de las personas. Los críticos olvidan que incluso la libertad de expresión garantizada por la Constitución no se aplica sin excepción, sino que encuentra sus límites en los derechos de los demás.

En este contexto, el Tribunal Constitucional Federal (2010) subrayó que el artículo 5 (1) de la Ley Fundamental no contiene ninguna garantía para las informaciones falsas, la propaganda y la incitación al pueblo.[8] Por el

---

[7] De acuerdo con M. Scheppe (2018), es la postura que dio a entender el jurista alemán Stahl en razón de la NetzDG, además de que está en favor de abolir la ley. De la misma forma véase G. Spindler (2017, pp. 171-173) *Notice and take down*. Teniendo en cuenta el riesgo de multas de hasta cincuenta millones de euros en caso de no borrado, es probable que éste sea el camino preferido para un operador de red que actúe por razones exclusivamente económicas –M. Liesching (2018)--. Esto establece efectivamente un sistema de "*Löschung im Zweifelsfall*", ya que las empresas que actúan económicamente no pueden actuar de otra manera (p. 27).

[8] Véase también M. Liesching (2010); sin embargo, el Tribunal Constitucional de Alemania (BverfG) también declaró que es legítimo sancionar las vulneraciones a los bienes jurídicos. En concreto, es posible impedir la libertad de opinión que "supere un peligro concretamente

contrario, la libertad de opinión y la libertad de prensa terminan cuando el honor de terceros y las leyes generales exigen que se detenga (artículo 5, párrafo. 2, GG). Por tanto, la aplicación de la ley y el orden no es un ataque, sino, al revés, la garantía de la libertad de expresión. Como dijo el entonces ministro federal de Justicia, Heiko Maas (SPD), en la sesión 244 del *Bundestag* (2017): "Con esta Ley ponemos fin al derecho del más fuerte en la red y protegemos la libertad de expresión de todos los que están en la red y que también quieren expresarse en ella". Asimismo, Schiff subraya que la NetzDG es una reacción legislativa legítima a las tendencias de asunción de poder de los proveedores a hacerse más poderosos, que como "*Gatekeeper*" del discurso público, se han convertido en una parte indispensable de la sociedad en red.

Por otra parte, las obligaciones de control para evitar la vulneración de los derechos de los particulares en el ámbito de los medios de comunicación no son en absoluto una excepción oscura, como demuestra un vistazo a las funciones de diligencia debida en el marco de la ley de prensa. Esta comparación se sugiere porque el proveedor de servicios, al igual que el editor de un medio tradicional, difunde contenidos o información. Aquéllas están explícitamente normativizadas en la mayoría de las leyes de prensa de los distintos estados alemanes federados. Por ejemplo, el artículo 6o. de la LPG-*Baden-Württemberg* estipula que los medios deben comprobar la veracidad, el contenido y el origen de todas las noticias con el cuidado que exigen las circunstancias antes de difundirlas. Por ejemplo, las cartas al director donde recibía improperios e incluso amenazas (S. Waschatz, 2014, p. 65; M. Löffler *et al*., 2023, Rn 155). En cuanto al alcance y la intensidad de los deberes de diligencia según el derecho de prensa, éstos no deben determinarse en abstracto, sino en función de cada caso concreto (Damm y Wolfdieter Kuner, 1991, Rn 214; M. Löffler *et al*., 2023, Rn 163). Por ejemplo, el editor tiene una mayor obligación de examinar los anuncios de terceros si hay una razón particular para dudar de la permisibilidad del contenido en cuestión, como en el caso de ilegalidad reconocible o efectos particularmente perjudiciales para el individuo afectado por la respectiva contribución (BHG,

tangible de violación de la ley" y que "en forma de apelación a la violación de la ley, la emocionalización agresiva o la disminución de los umbrales de inhibición pueden desencadenar directamente consecuencias que pongan en peligro los bienes jurídicos".

1987, p. 2225; BHG, 1992, pp. 3093 y 3094; BverfG, 2009, p. 565; Wenzel *et al*., 2018, p. 803).

Al igual que la obligación de la prensa de controlar la difusión de noticias por parte de otros, también se ha de esperar que el proveedor de servicios controle los contenidos o la información de terceros. Si, por ejemplo, el proveedor tiene un servidor que almacena opiniones de terceros, debe comprobar si los archivos recibidos están dentro del marco legal antes de publicarlos. En este caso, existe el peligro latente de que se traspase la frontera del contenido punible al incluir en la oferta, por ejemplo, la incitación al pueblo, o bien si el proveedor almacena archivos pornográficos en su servidor, se debe comprobar si los archivos recibidos están dentro del marco legal y debe garantizar, especialmente, que los menores no puedan acceder a estos contenidos.

El tráfico mundial de datos es indispensable en la actualidad y representa un factor económico considerable. Pero encuentra un límite en la importancia de los bienes jurídicos afectados en vista de los peligros potenciales amenazantes (D. Barton, 1999, p. 239). Estos elementos ilícitos no deberían ser ignorados, sobre todo porque un gran número de personas tiene la posibilidad de percibir las violaciones de los bienes jurídicos. Es así que el proveedor de servicio puede apoyar a la difusión de contenidos ilegales, dado que el usuario utiliza dicho servidor para su actividad delictiva. Por tanto, el interés económico tiene que pasar a un segundo plano frente al interés de la protección de los bienes jurídicos (OLG, HH, 2006, p. 756; OLG, Munich, 2007, p. 104; Feldmann, 2006, pp. 744-748).

En cuanto a la cuestión de la razonabilidad, no sólo importa el momento en que se conoció la información o el acto ilícito (medidas *ex post*). Sería óptimo que el proveedor de servicios cree de forma preventiva una infraestructura técnica que le permita bloquear la información ilícita (medidas *ex ante*) (Eberle *et al*., 2003; Heckmann *et al*., 2019). Como se menciona en la jurisprudencia del Tribunal Europeo de Derechos Humanos (2015), estas medidas sirven para proteger los derechos e intereses de los demás y de la sociedad.[9] Por último, pero no por ello menos importante, el proveedor de servicios tiene un gran interés en ello, ya que evita quedar bajo el "fuego" penal o, al menos, ser objeto de comentarios negativos en la esfera pública, lo que no es bueno

[9] *Cfr*. Sentencia del Tribunal Europeo de Derechos Humanos (2015): ...Responsabilizar a los portales de noticias de Internet sin violar el artículo 10 del CEDH si no toman medidas para eliminar sin demora los comentarios claramente ilícitos, incluso sin notificarlo a la víctima o a terceros.

para su reputación; es decir, retirar contenidos indebidos es absolutamente legal y razonable.

3. Legislación en materia de prevención de delitos informáticos en Perú y en Alemania

En los últimos años, la "ciberdelincuencia" se ha convertido en el centro de atención de las autoridades de seguridad y también de la política. En este contexto, se dará a conocer un análisis general sobre las legislaciones existentes en Perú y Alemania, con respecto a la prevención de los ciberdelitos. Alemania brinda un análisis genealógico de los ciberdelitos, con la finalidad de legitimar el poder punitivo en la sociedad de riesgo, habilitando el *ius puniendi* sobre conductas que afectan sistemas, datos informáticos y bienes jurídicos relacionado a las tecnologías de la información y comunicación (TIC). A continuación, se procederá con el análisis de las legislaciones.

A. Alemania

La ciberseguridad se rige por varias leyes, entre ellas tenemos la Ley de Telemedios (*Telemediengesetz* [TMG], 2007), así como el JMSTV y la NETZDG, que sirven para prevenir las violaciones de los bienes jurídicos e imponen medidas preventivas en la lucha contra la ciberdelincuencia.

La TMG asume que la persona que crea su propia información es también responsable de ella. Así, el artículo 7(1) de la TMG estipula que los proveedores de servicios son responsables de su propia información, la cual ponen a disposición de los usuarios para su uso, de acuerdo con las leyes generales. Sin embargo, se puede considerar un privilegio de responsabilidad si un proveedor de servicios almacena información de terceros. En este sentido, el artículo 7(2) de la TMG no impone una obligación general de supervisar y controlar la información de terceros. Al respecto, debo precisar que este privilegio de responsabilidad que otorga la TMG al ISP está perdiendo terreno en la actualidad, especialmente en los delitos contra la propiedad intelectual como se puede ver en la Directiva sobre Derechos de Autor —RL UE, 2019/790—, que fue aprobada por el Parlamento de la Unión Europea y el Consejo (UE, 2019).[10] Esta Directiva, en su artículo 17, obliga

[10] Los gobiernos de los respectivos Estados miembros de la UE tienen ahora que

a los ISP a realizar todos los medios técnicos necesarios para la protección del bien jurídico y fomentar de esta manera el buen funcionamiento del mercado de obras protegidas por derechos de autor, y eliminando la inseguridad jurídica más allá de las fronteras nacionales a nivel europeo. Este cambio, refleja que el ISP controle el contenido de terceros que almacena en su servidor, dando origen a la posición de garante de vigilancia por una fuente de peligro,[11] por lo que el ISP estaría sujeto a deberes de cuidado al respecto.

El JMSTV tiene como objetivo principal la protección de los menores del riesgo que existe en Internet. La protección de los menores, tal y como se menciona explícitamente en el artículo 5(2) de la Constitución alemana, no sólo significa una restricción de la libertad de opinión e información prevista en la Constitución, sino que también incluye un mandato de protección por parte del Estado. En este sentido, el objetivo de esta norma de derecho fundamental es garantizar el desarrollo sin perturbaciones de los menores y evitar los peligros que los amenazan mediante las medidas preventivas. Por tanto, el ISP debe cumplir su obligación de control con medios técnicos o de otro tipo que hagan imposible o considerablemente más difícil que los niños o adolescentes del grupo de edad en cuestión perciban ofertas lesivas. Por ejemplo, el ISP puede proporcionar la oferta con una calificación de edad que pueda ser fácilmente identificable por los usuarios. Otra forma de cumplir con la obligación de control es permitir el acceso del contenido sólo en horarios establecidos. Si el ISP incumple sus obligaciones, será sancionado en virtud del artículo 23 del JMSTV. El legislador ha creado así una disposición penal especial para la protección de los niños y los adolescentes. De acuerdo con esta disposición, quien actúa en contra de lo que indica el artículo 4o. del JMSTV (2003),[12] será castigado con una pena de prisión de hasta un año y con multa.

La NetzDG introduce normas de cumplimiento en las redes sociales que deben ser aplicadas por el ISP para evitar delitos penales, como la incita-

---

incorporar la Directiva sobre Derechos de Autor a su legislación nacional, desde el 15 de abril de 2019.

[11] Un garante de vigilancia es aquel que se convierte en el gobernante de una fuente potencial de peligro, al que se dirige la expectativa razonable de que lo controlará y evitará consecuencias perjudiciales (Rengier, 2019, § 50, Rn. 45).

[12] Quien distribuya o ponga a disposición ofertas que sean manifiestamente capaces de poner en grave peligro el desarrollo de los niños y adolescentes, será castigado con una pena de prisión de hasta un año y con multa.

ción a la violencia, la difamación o la perturbación de la paz pública. A raíz de ello, los ISP están obligados a retirar o bloquear los contenidos ilegales, pues Facebook y Twitter (hoy X) no sólo crean nuevas oportunidades para la expresión de opiniones y el debate, sino también para la difusión de noticias falsas dirigidas a la propaganda y la incitación al terrorismo. De acuerdo con G. Nolte (2017), los usuarios de redes utilizan estos medios porque es más fácil difundir sus mensajes de forma anónima o bajo un seudónimo, debido a que Internet hace que la difusión sea más rápida y accesible a un amplio círculo de destinatarios. Esto supone un gran peligro para nuestra sociedad, no sólo por la facilidad de difusión de forma anónima de contenidos ilícitos, sino porque los ciberenemigos tienen las VPN a su alcance, lo que hace que sean doblemente difíciles de interceptar por la justicia.

B. Perú

No existe un régimen de *notice and take down* en Perú tal como en Alemania. Si bien el Tratado de Libre Comercio (TLC) firmado con Estados Unidos nos impone tener un sistema de responsabilidad de los ISP, en la actualidad aún no ha sido implementado.

La Oficina de Derechos de Autor, a través del régimen de medidas cautelares, ejerce una suerte de *notice and take down* contra los ISP de Internet que proporcionan el acceso a contenidos que podrían ocasionar lesiones contra bienes jurídicos protegidos relacionados con la propiedad intelectual. Debe precisarse que la Oficina de Derechos de Autor realiza una protección fundada en los presupuestos procesales para interponer una medida cautelar, por lo cual no se pueden tomar como un reemplazo a la responsabilidad penal de los ISP.

Finalmente, es importante una propuesta normativa que delimite la responsabilidad penal del ISP por su contribución en la lesión o puesta en peligro de los bienes jurídicos.

III. Conclusiones

La intención de esta investigación no es poner en duda el devenir de los avances tecnológicos y las nuevas formas de comunicación entre personas o entre entidades jurídicas, es innegable la diversidad y la relevancia de estos apor-

tes a la vida cotidiana de cada persona. Sin embargo, no debemos olvidar que estamos expuestos a nuevos riesgos que origina una sociedad posindustrial. Si bien el Estado peruano ha implementado normas que sancionan los delitos informáticos, es de apreciar la falta de regulación normativa en la prevención de estos delitos, como sí la hay en Alemania. Este rol de prevención debería ser asumido por el ISP a través de su programa de *compliance*, puesto que éste se encuentra en un punto determinante para filtrar el contenido (puerta de entrada). De esta manera, se podría contribuir aún más en la mitigación de los riesgos contra los bienes jurídicos de terceros. Por tanto, es necesario que el Estado peruano regule normativamente las obligaciones y deberes que le corresponden a los ISP.

Por otro lado, es comprensible que el público se pueda sentir invadido o quizá rechace la formalidad a la que no están acostumbrados cuando usan Internet, pero es necesario concienciar a los individuos, sobre la importancia de tomar medidas enérgicas y coherentes por parte de los ISP. Pues la falta de acción de su parte podría ayudar a la expansión de los delitos expuestos. Ante las nuevas formas de delinquir es necesario desarrollar y aplicar nuevos mecanismos de prevención.

IV. Recomendación

Los ISP de contenido deberían tener mayores responsabilidades puesto que ha sido confirmada la posibilidad de evitar la lesión de los bienes jurídicos expuestos en el medio digital, los cuales deben protegerse con todas las herramientas de las que se dispone; por otro lado, porque se ha comprobado también la razonabilidad de la realización de aquel acto de control de su plataforma. No se puede omitir la responsabilidad y dejar que un riesgo potencial se acrecenté.

Los ISP deberían situar en segundo plano las ganancias económicas que dejan los medios digitales cuando se está frente a la afectación de bienes de mayor gravedad, colocando medidas de prevención en donde no sólo se tenga en cuenta el interés de la víctima, sino también se cuide la imagen y reputación del mismo proveedor respecto a diversas sanciones.

Los ISP deberían tener en cuenta que la libertad de expresión es sin duda un gran bien, pero termina donde empieza el derecho penal. Todo el mundo puede utilizar las redes sociales para influir en el discurso social y en la forma-

ción de la opinión pública, pero nadie puede insultar y menospreciar a otras personas ni difundir mentiras sobre ellas.

V. Referencias

Altenhain, K. (1997). *Die strafrechtliche Verantwortung für die Verbreitung mißbilligter Inhalte in Computernetze.* CR: Computer und Recht.

Balkin, J. M. (1999). Free Speech and Hostile Environments. *Columbia Law Review*, *99*(8), 2295-2320. https://doi.org/10.2307/1123612

Barton, D. (1999). *Multimedia-Strafrecht: Ein Handbuch für die Praxis*. Hermann Luchterhand Verlag.

Beck, U. (1998). *La sociedad del riesgo: hacia una nueva modernidad.* Barcelona: Paidós.

Becker, M (2018). *Mehr Kontrolle im Internet. Die Diskussio in Deutschland.* Recuperado el 7 de enero de 2024. https://www.swr.de/swr2/wissen/article-swr-17782.html

Bundesgerichtshof (1987). *Neue Juristische Wochenschrift*.

Bundestag alemán (2017). Informe taquigráfico. 235a. sesión. https://dserver.bundestag.de/btp/18/18235.pdf

Bundestag alemán (2017b). Informe taquigráfico. 244a. sesión. https://dserver.bundestag.de/btp/18/18244.pdf

Ceffinato, T. (2017). *Die strafrechtliche Verantwortlichkeit von Internetplattformbetreibern. JuS: Juristische Schulung*.

Children's Online Privacy Protection Act (1998) (Estados unidos). https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim

Cisco (22 de febrero de 2024). *What is a Virtual Private Network (VPN).* Recuperado el 11 de marzo de 2024. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Damm, R. (2001). *Widerruf, Unterlassung und Schadensersatz in Presse und Rundfunk.* C. H. Beck.

Damm, R. y Kuner, Wolfdieter (1991). *Widerruf, Unterlassung und Schadensersatz in Presse und Rundfunk*. C. H. Beck.

Degen, T. (2007). *Freiwillige Selbstkontrolle der Access – Provider*, Boorberg.

DW español (6 de junio de 2022). *Tim Berners-Lee: creador de la World Wide Web* [Vídeo]. YouTube. https://www.youtube.com/watch?v=SNw4m1m_2GE

ISSN: 2448-4873
DOI: https://doi.org/10.22201/iij.24484873e.2023.167.18367

Eberle, C., Rudolf, W., Wasserburg, K. (2003). *Mainzer Rechtshandbuch der Neuen Medien.* Müller, C F in Hüthig Jehle Rehm *en Internet*. Recuperado el 11 de febrero de 2024. https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf

Espinoza Bonifaz, R. (2020). *Hacia una criminología indoamericana*.

Feldmann, J. (2006). OLG *Hamburg: Haftung des Betreibers von Internetforen -- heise.de Urteil vom 22.08.2006 - 7 U 50/06*. MMR.

Fischer, T. (2024). *Strafgesetzbuch: StGB* (71a. ed.). C. H. Beck.

Galetzka, C. y Krätschmer, M. (2016). Rassismus und Terrorismus im Netz --Strafrechtliche Verantwortlichkeit der Betreiber von sozialen Netzwerken. *MMR: MultiMedia und Recht.*

García Cavero, P. (2019). *Derecho penal. Parte general* (3a. ed.). Ideas.

Heckmann, D. (2012). Persönlichkeitsschutz im Internet -- Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderungen für Ehrschutz und Profilschutz. *NJW: Neue Juristische Wochenschrift.*

Heckmann, D., Stadler, T. y Roggenkamp, J. D. (2019). *Juris Praxiskommentar Internetrecht*. Juris.

Heß, M. (2005). *Die Verantwortlichkeit von Diensteanbietern für Informationen im Internet nach der Novellierung des Teledienstgesetzes.* LIT Verlag.

Hoeren, T. (2018). *Internet – Rderecht* (3a. ed.). De Gruyter.

Hoeren, T., Sieber, U. y Holznagel, B. (2019). *Handbuch Multimedia – Recht* (48a. ed.). C. H. Beck.

Hörnle, T. (2002*).* Pornographische Schriften im Internet: Die Verbotsnormen im deutschen Strafrecht und ihre Reichweite. *NJW: Neue Juristische.*

Hoven, Elisa (2018). Die strafrechtliche Verantwortlichkeit der Betreiber von Social -- Media – Plattform. *ZWH: Zeitschrift* für *Wirtschaftsstrafrecht und Haftung im Unternehmen*.

Jakobs, G. y Cancio Meliá, M. (2003). *Derecho penal del enemigo*. Cuadernos Civitas.

Kaspersky (19 de diciembre de 2023) *What is an IP Address – Definition and Explanation.* Recuperado el 11 de marzo de 2024. https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address

Koch, F. (2005). *Internet -- Recht* (2a. ed.). Oldenbourg.

Krol, E. (1995). *Die Welt des Internet*. Oreilly.

Lackner, K., Kühl, K. y Heger, M. (2023). *Strafgesetzbuch: StGB* (30a. ed.). C. H. Beck.

Ley de Telemedios (2007)(Alemania). https://www.gesetze-im-internet.de/tmg/

Ley sobre la Mejora de la Aplicación de la Ley en las Redes Sociales (2017) (Alemania)

Liesching, M. (2010). *Hausverlosung im-Internet*. MMR.

Liesching, M. (2018). *Die Durchsetzung von Verfassungs-und Europarecht gegen da NetzDG*. MMR.

Löffler, M., Wenzel, K. E., Sedelmeier, K., Burkhardt, E. H., Achenbac, H., Adam, M., Altenhain, K., Berger, K., Bölke, D., Boorberg, W., Buck, H., Cornils, M., Gomille, C., Grimm, S., Grund, U., Heilmann, S., Kudlich, H., Kühl, K., Lauber-Rönsberg, A.,... Steffen, E. (2023). *Presserecht Kommentar* (7a. ed.). C. H. Beck.

Ministerio de Justicia (2022). *Ciberdelincuencia en el Perú*. Reporte de información estadística. https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf?v=1661790352

Ministerio Público Fiscalía de la Nación (2023). *Fiscalía de Ciberdelincuencia recibió más de 17 mil denuncias y logró 78 sentencias en los últimos 2 años.* https://www.gob.pe/institucion/mpfn/noticias/778658-fiscalia-de-ciberdelincuencia-recibio-mas-de-17-mil-denuncias-y-logro-78-sentencias-en-los-ultimos-2-anos

Naciones Unidas (2012). *Promoción, protección y disfrute de los derechos humanos.*

Naciones Unidas (2019). *La Declaración Universal de los Derechos Humanos.* Recuperado el 11 de febrero de 2024. https://www.un.org/es/about-us/universal-declaration-of-human-rights#:~:text=Art%C3%ADculo%2019,por%20cualquier%20medio%20de%20expresi%C3%B3n

Nolte, G. (2017*).* Hate-Speech, Fake-News, das »Netzwerkdurchsetzungsgesetz« und Vielfaltsicherung durch Suchmaschinen. *Zeitschrift für Urheber- und Medienrecht*.

Pelz, C. (1999). *Die Strafbarkeit von Online-Anbietern.* Wistra.

Popp, M. (2002). *Die strafrechtliche Verantwortlichkeit von Internet – Providern*. Duncker & Humboldt.

Rath, C. (2016). *Das Recht ist kein justizfreier Raum. Der verborgene Teil des Internets bietet nicht nur Schutz für Dissidenten und Whistleblower, sonder auch Drogen Waffen und andere ilegale Waren*. C. H. Beck.

Red Científica Peruana (2024). Recuperado el 11 de marzo de 2024. https://rcp.pe

Rengier, R. (2019). *Strafrecht Allgemeiner Teil* (11a. ed.). C. H. Beck.

ISSN: 2448-4873
DOI: https://doi.org/10.22201/iij.24484873e.2023.167.18367

Scheppe, M. (4 de enero de 2018*). Fragen und Antworten: NetzDG – das umstrittene Gesetz.* WirtschaftsWoche. Recuperado el 11 de febrero de 2024. https://www.wiwo.de/politik/deutschland/fragen-und-antworten-netzdg-das-umstrittene-gesetz/20814742.html
Schmidl, Michael (2014). *IT-Recht von A-Z* (2a. ed.). C. H. Beck.
Schönke, A. y Schröder, H. (2019*). Strafgesetzbuch: StGB* (30a. ed.). C. H. Beck.
Seitz, N. (2004). *Strafverfolgungsmaßnahmen im Internet.* (vol. 19). Ius informationis.
Sieber, U. (1996). Strafrechtliche Verantwortlichkeit *für den* Datenverkehr in internationalen Computernetzen. *JZ: Juristenzeitung*, *LI*(9), 429-442.
Sieber, U. (1997). *Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen*. CR Computer und Recht.
Silva-Sánchez, J. (2012). *Aproximaciones al derecho penal contemporáneo* (2a. ed.), Bdef.
Sobola, S. y Kohl, K. (2005). *Haftung von Providern für fremde Inhalte.* Computer und Recht.
Spindler, G. (1997). *Haftungsrechtliche Grundprobleme der neuen Medien*. Nueva Jersey: Neue Juristische.
Spindler, G. (2017). *Internet Intermediary Liability Reloaded – The New German Act on Responsibility of Social Networks and its (In-) Compatibility with European Law*. https://www.jipitec.eu/archive/issues/jipitec-8-2-2017/4567
Spindler, G., Schmitz, P. y Liesching, M. (2018). *Telemediengesetz: TMG* (2a. ed.). C. H. Beck.
Stadler, T. (2005). *Haftung für informationen im-internet.* Responsabilidad por la información en Internet (2a. ed.). Erich Schmidt.
TEDH (2015). DELFI AS v. Estonia. *NJW*, 2015, 2863 (2868).
The Digital Millennium Copyright Act (1998) (Estados Unidos). https://www.copyright.gov/legislation/dmca.pdf
Thiedeke, U. (2004). *Soziologie des Cyberspace: Medien*, Strukturen und Semantiken. Kindle.
Tolksdorf, Robert (1997). *Internet-Aufbau und Dienste*. International Thomson Publishing.
Tratado Interestatal sobre la Protección de los Menores frente a los Medios de Comunicación (2002) (Alemania).
Tribunal Constitucional Federal (2009). 565. ZUM-RD.
Tribunal Constitucional Federal (2010). BVR 369/04. Recuperado el 11 de febrero de 2024. https://www.hrr-strafrecht.de/hrr/bverfg/04/1-bvr-369-04.php

Tribunal Federal de Justicia de Alemania (1987). 2225. *NJW*.
Tribunal Federal de Justicia de Alemania (1992). *NJW*. pp. 3093 y 3094.
Tribunal Regional Superior de Munich (2007). 104. K&R
Tribunal Superior de Justicia de Hamburgo (2006). 756. ZUM
Unión Europea. Directiva (UE) 2019/790 del Parlamento Europeo y el Consejo, del 17 de abril de 2019, que modifica las Directivas 96/9/CE y 2001/29/CE sobre los Derechos de Autor y Derechos Afines en el Mercado Único Digital. *Diario Oficial de la Unión Europea*.
Unión Europea. Directiva (UE) 2021/784 del Parlamento Europeo y el Consejo, del 29 de abril de 2021, sobre la Lucha contra la Difusión de Contenidos Terroristas en Línea. *Diario Oficial de la Unión Europea*.
Waschatz, S. (2014). *Haftungsfalle Behördeninformation*. Nomos.
Wenzel, E. K., Burkhard, H. E., Gamer, W., Peifer, N. K. y Strobl-Albeg, J. (2018). *Das Recht der Wort- und Bildberichterstattung* (6a. ed.). Otto Schmidt.
Wessels, J., Beulke, W. y Helmut, Satzger (2023). *Strafrecht Allgemeiner Teil* (53a. ed.). C. F. Müller.
Zúñiga Rodríguez, L. (2020). *Fundamentos de la responsabilidad penal de las personas jurídicas*. Instituto Pacífico.

ISSN: 2448-4873
DOI: https://doi.org/10.22201/iij.24484873e.2023.167.18367