ARTICULO
Revista Derecho - Año 2 edición 3: 233 - 245

Web: http://www.revistaderecho.pe E-mail: editorial@revistaderecho.pe
ISSN 2313-6944

EL DERECHO PENAL INFORMÁTICO HUMANO COMO CAUTELA FRENTE AL PODER PUNITIVO EN LA SOCIEDAD DE CONTROL

*Michael Espinoza Coila**

INFORMACIÓN DEL ARTICULO

Art. Recibido: 04/02/16
Art. Aceptado: 01/06/16
Art. Publicado: 18/12/18

PALABRAS CLAVE:
Derecho Penal
Informática
Poder punitivo
Control
Vigilancia

RESUMEN

El presente artículo sintetiza la tesis de pregrado "Derecho Penal Informático: Deslegitimación del poder punitivo en la sociedad de control", el cual estudió la problemática del poder de vigilancia del poder punitivo habilitado con los delitos informáticos, para ello nos planteamos como objetivos: explicar los limites u horizonte de proyección del Derecho Penal Informático, la interdisciplinariedad del Derecho Informático y el Derecho Penal, señalar las fuentes del Derecho Penal Informático, definir el Delito Informático, describir el tratamiento de los Delitos Informáticos en el Derecho Penal peruano y comparado, explicar la aplicación espacial y temporal de los Delitos Informáticos, por último señalar las consideraciones de política criminal sobre los Delitos Informáticos; la mencionada tesis concluyó que el Derecho Penal Informático Humano, es el saber jurídico penal que mediante la interpretación de leyes penales sobre Delitos Informáticos, propone a los agentes jurídicos un sistema reductor del poder de vigilancia del poder punitivo en la sociedad de control, para impulsar el poder jurídico con el fin de preservar los espacios de libertad y privacidad de las personas, además se explica la interdisciplinariedad del Derecho Informático y el Derecho Penal, como correspondencia secante entre saberes jurídicos, sus fuentes de conocimiento y de información, también se sostiene varias definiciones de manera formal, material y analítica de los delitos informáticos que en el Perú, se encuentran en la Ley N° 30 096 "Ley de Delitos Informáticos" y diversas leyes de Estados Unidos, Alemania, Francia, España, Chile, Argentina, y Ecuador, también concluimos que los delitos informáticos requieren de los principios de aplicación temporal del Código Penal, finalmente señalamos algunos problemas con el poder

* Abogado. Universidad Nacional del Altiplano de Puno (Perú). Círculo de Investigación Líderes Optimistas Revelando Derecho (CILORD). micnous@gmail.com

punitivo partiendo desde la Criminología cautelar expuesto por el jurista Eugenio Raúl Zaffaroni y pautas a considerar para la prevención de los delitos informáticos y del poder de vigilancia.

THE HUMAN COMPUTER CRIMINAL LAW AS A CAUTION TO PUNITIVE POWER IN THE CONTROL SOCIETY

ARTICLE INFO

Article Received: 04/02/16
Article Accepted: 01/06/16
Article Published: 18/12/18

KEY WORDS:
Criminal Law
Informatics
Punitive power
Control
Surveillance

ABSTRACT

This article synthesizes the undergraduate thesis "Computer Criminal Law: De-legitimization of punitive power in the control society", which studied the problem of the power of vigilance of punitive power enabled with computer crimes, for this we set ourselves the following objectives: the limits or horizon of projection of Computer Criminal Law, the interdisciplinarity of Computer Law and Criminal Law, to point out the sources of Computer Criminal Law, to define Computer Crime, to describe the treatment of Computer Crimes in Peruvian and Comparative Criminal Law, to explain the spatial and temporal application of Computer Crimes, finally pointing out the considerations of criminal policy on Computer Crimes; The aforementioned thesis concluded that the Criminal Human Rights Law, is the criminal legal knowledge that through the interpretation of criminal laws on Computer Crimes, proposes to the legal agents a system that reduces the power of vigilance of punitive power in the control society, to promote the legal power with the purpose of preserving the spaces of freedom and privacy of the persons, in addition the interdisciplinarity of the Computer Law and the Penal Right is explained, like drying correspondence between legal knowledge, its sources of knowledge and of information, also it is sustained several formal, material and analytical definitions of computer crimes that in Peru, are found in Law No. 30 096 "Computer Crime Law" and various laws of the United States, Germany, France, Spain, Chile, Argentina, and Ecuador, we also conclude that computer crimes require the principles of temporary application of the Penal Code, finally we pointed out some problems with the punitive power starting from the precautionary Criminology exposed by the jurist Eugenio Raúl Zaffaroni and guidelines to consider for the prevention of computer crimes and the power

1. INTRODUCCIÓN

El viernes 12 de octubre de 2018, la empresa Facebook reconoció que 29 millones de cuentas quedaron descubiertas con el ciberataque realizado el 28 de setiembre que aprovechando un agujero de seguridad en los tokens dentro de las funciones "Ver como"(DW, 2018a, 2018b); las vulnerabilidades y las puertas traseras de los sistemas informáticos son asuntos casi cotidianos para la prensa internacional superando los guiones de película como WarGames (Filmaffinity, 1983); en nuestro país, el gobierno peruano ha establecido un marco de seguridad digital del Perú con los delitos informáticos desde el año 2 000 y con el Decreto Legislativo N.º 1 412 se ha insuflado un gobierno digital, que se viene lentamente impregnando en las estructuras sociales que producen y consumen información en un entorno digital, donde vive el ciudadano digital, quien hace uso de las tecnologías digitales, ejerciendo sus deberes y derechos gozando de una identidad y domicilio digital (Poder Ejecutivo del Perú, 2018), todo este ambiente nos ha permitido discurrir algunas razones que parten desde el derecho penal humano y la criminología cautelar, y exponer nuestros resquemores sobre la sociedad de control y la vigilancia del poder punitivo a través de la tecnologías de la información y comunicación.

Con la filosofía sabemos que somos objeto de vigilancia en medio de una sociedad de control (Foucault, 2002; Gilles, 1999), quizá antes los medios fueron rudimentarios o analógicos, en este siglo XXI de la goblocolonización, son las leyes y las tecnologías de control las herramientas mas enjudiosas para los gobiernos y las empresas que pretenden controlar a la población.(Lessig, 2005; Stallman, 2013); el tráfico de datos de nuestra vida digital son ahora bienes valiosos de intercambio comercial entre países y empresarios puesto que el mercado internacional y la intervención de comunicaciones son expresiones de soberanía global que determina quién es el centro del mundo, el dominante, el productor, el punto de referencia para los dominados.

2. LÍMITES U HORIZONTE DE PROYECCIÓN DEL DERECHO PENAL INFORMÁTICO HUMANO

Para la limitación y explicación del horizonte de proyección, fue menester formular en la tesis una definición del derecho penal informático humano, como: saber jurídico penal que, mediante la interpretación de leyes penales sobre delitos informáticos, propone a los agentes jurídicos un sistema reductor del poder de vigilancia del poder punitivo en la sociedad de control para impulsar del poder jurídico con el fin de preservar los espacios de libertad y privacidad de las personas en el entorno digital.(Espinoza Coila, 2017)

Si la definición, es la exposición de la caracterización y diferenciación de algo material o inmaterial (Real Academia Española, 2014) correspon-

de presentar las siguientes proposiciones conforme a nuestra tesis(Espinoza Coila, 2017), siguiendo al maestro E. Raúl Zaffaroni:

a) Es un saber jurídico penal, porque es un programa técnico-político del derecho penal humano, que primero estudia los delitos informáticos para formular discursos que orientan las decisiones judiciales en un marco de poder político y económico, y segundo aspira a ser doctrina que se convierta en jurisprudencia sobre delitos relacionados a las Tecnologías de la Información y la Comunicación (TIC).

b) La interpretación de leyes penales sobre delitos informáticos, se realiza con el método dogmático deslegitimante del derecho penal humano, con el cual se construye un sistema orientador a los jueces para dictar sentencias judiciales, a los fiscales y abogados para la formulación de tesis de imputación y de defensa, con la finalidad de limitar el poder de vigilancia del poder punitivo que es ejercido por las agencias ejecutivas (policías) y políticas (parlamentarios), y preservar el Estado Constitucional de Derecho.

c) La Sociedad de Control, como binomio de sociedad digital y vigilancia (Alcántara, 2008), es manifestación del poder punitivo, legitimada por la mayoría de la población que sabe que es vigilada pero lo acepta porque se siente protegida (Eugenio Raúl Zaffaroni, 2016), y se justifica con la doctrina de la seguridad nacional(Mattelart, 2002, 2009) lo que le interesa a la poder político y económico es reducir la privacidad, controlar a la población mediante las tecnologías de control.

d) La reducción del poder de vigilancia mediante la dogmática desligitmante del derecho penal informático humano, permite reducir los efectos nocivos del poder punitivo que se alimenta de la cultura del terrorismo (Chomsky, 1998) que preconizan la vigilancia con el discurso de la seguridad nacional, fomentando la criminalización de la vida digital de la personas con los delitos informáticos.

e) Finalmente, el Derecho Penal Informático Humano, no es igual a al Derecho Penal de la Seguridad(Kindhäuser, 2014) y Derecho Penal Preventivo(Sieber, 2015) que solo legitiman y fortalecen al poder punitivo habilitando los estados de excepción y la restricción permanente derechos mediante el control judicial, que permiten una buena convivencia, mismo Estado Utópico, desconociendo la realmente como funciona la estructura básica del poder punitivo que nos hacen cavilar cuando leemos la Cautio Criminalis (Spee, 2017), de modo que me permito afirmar

que el resto es solo Derecho Penal Inhumano.

f) El derecho penal informático humano, tiene como objeto de estudio a la seguridad jurídica de los delitos informáticos, y como objeto de interpretación a las leyes penales sobre delitos informáticos.

g) Su función es reducir o recortar la intensidad del poder de vigilancia del poder punitivo y fortalecer el poder jurídico para mantener la vigencia del Estado Constitucional de Derecho donde se puede cautelar la vida digital de las personas, garantizando sus espacios libertad y privacidad.

h) El Derecho Penal informático es Público (derecho público), Represivo (reprime al poder punitivo), Continuo y Fragmentador (del poder punitivo) y Normativo (delitos informáticos).

3. INTERDISCIPLINARIEDAD SECANTE ENTRE DEL DERECHO INFORMÁTICO Y EL DERECHO PENAL

La interdisciplinariedad secante del Derecho Informático y el Derecho Penal Humano (Espinoza Coila, 2015), permite que cada saber confluya para total comprensión del fenómeno informático, por ejemplo la informática nos informa que los humanos o PEBKAC somos la pieza que falla en los mecanismos de seguridad (Ward & Wall, 2018) por otro lado el Derecho Penal nos advierte de la existencia del Poder Punitivo; esta interrelación superpuesta de estos saberes hacen que la actividad del agente jurídico sea racional y tecnificada, pues no hay otra manera tratar a los *big data*, *data center*, inteligencia artificial, virus, Internet entre otros términos técnicos, tampoco es posible sin el Derecho Penal, entender que las leyes penales son instrumentos de control o de vigilancia y que mediante su interpretación podemos contener al poder punitivo.

De la confederación de saberes, nace el Derecho Penal Informático Humano; a primera vista, pareciera que me adscribo a la tendencia de desintegrar el Derecho Penal, como sucede con el Derecho Penal Económico, cabe aclarar que no se pretende demandar autonomía para este saber jurídico penal, tan solo vinculo dos saberes: el Derecho Informático y el Derecho Penal Humano, para construir un sistema interpretativo para que los ciudadanos digitales pervivan en la sociedad de control, y también ofrezco una respuesta a todos quienes creen que existe un Derecho Penal Informático autónomo, la cual consiste en establecer una prelación con la dogmática deslegitimante del Derecho Penal Humano en la labor interpretativa de los delitos informática, pues se trata de excogitar una visión racional y real del tratamiento de los delitos relacionados a las TIC, puesto que un alejamiento de los principios rectores del Derecho Penal Humano, nos conduciría a legitimar al Poder Punitivo por ende a la vigilancia de la Sociedad de Control, lo cual suscitaría

un Derecho Penal Informático Inhumano o propiamente un Derecho Penal Inhumano; el discurso emancipatorio del Derecho Penal es un táctica recurrente del Poder Punitivo, pues no otra manera de eximirse del Poder Jurídico de contención, que decir que lo que se legisla, enseña o dictamina no es Derecho Penal o que se trata de delitos especiales (como los delitos informáticos) y que por tal motivo, no debemos considerar al Derecho Penal; cuestión errónea, por el contrario el Derecho Penal es ineludible para el tratamiento de las leyes penales manifiestas, eventuales y no manifiestas.

4. FUENTES DEL DERECHO PENAL INFORMÁTICO HUMANO

El Derecho Penal Informático Humano, que estriba en el Derecho Penal Humano del egregio maestro Raúl Zaffaroni, requiere también de datos reales y especializados, por ello tiene dos fuentes: a) Conocimiento, que comprende a todas las leyes sobre delitos informáticos que habilitan el ejercicio del poder punitivo (incluye a las inconstitucionales), y otros datos aportados por la interdisciplinariedad con el Derecho Constitucional, Derecho Internacional, Derecho Informático, Derecho Administrativo, Derecho Civil, Jurisprudencia, Filosofía, Historia, Política, Economía, Sociología, Antropología y otros datos de la realidad, para entender el efecto real de las normas penales, su funcionamiento y críticas ideológicas; y b) Información, que comprende la bibliografía sobre delitos informáticos, dado que es importante conocer el estado de desarrollo doctrinario sobre lo delitos informáticos y el Derecho Penal. (Espinoza Coila, 2017; Eugenio Raúl Zaffaroni, Alagia, & Slokar, 2002)

5. EL DELITO INFORMÁTICO

El Delito Informático (computer crime / computerkriminalität), es definido de manera (a) *formal*, como acción u omisión prohibida por la ley penal sobre delitos informáticos; (b) *material*, como conducta final que ofenden bienes jurídicos relacionados a las Tecnologías de la Información y la Comunicación (TIC), y (c) *analítica*, como conducta típica, antijurídica y culpable que tiene como medio u objeto de protección a las T.I.C.(Espinoza Coila, 2014, 2017)

Entre todas las definiciones, la analítica es la mas adecuada, pero no esto resuelve totalmente el problema más patente del cual el poder punitivo se aprovecha para sembrar confusión e inseguridad, pues al revisar la doctrina, notamos que no hay uniformidad de las definiciones ni en las clasificaciones.(Espinoza Coila, 2017) Por esta cuestión fue necesario establecer, en la tesis, una función y características a los delitos informáticos a modo de presentar una antípoda al poder punitivo.

Los delitos informáticos, asumen una doble función en la sociedad de control: a) Habilitar el ejercicio del poder punitivo, y a la vez b) Limitar al poder punitivo mediante la interpretación del tipo con una dogmática

deslegitimante y estableciendo los caracteres propios del delito que han de acreditarse para dejar pasar las aguas menos turbias o intensas del poder punitivo.(Espinoza Coila, 2017)

Los delitos informáticos o delitos cibernéticos, siguiendo la doctrina(Acosta Patroni, 2003; Téllez Valdés, 2008), se caracterizan: (1) Conductas criminales de cuello blanco, porque sólo determinado número de personas con ciertos conocimientos técnicos pueden cometerlas; (2) Acciones ocupacionales porque se realizan cuando el sujeto está trabajando; (3) Acciones de oportunidad, porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico; (4) Provocadoras de serias pérdidas económicas; (5) Se realizan con facilidad de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física, (6) Difícil averiguación y comprobación, porque sus autores actúan de forma anónima; (7) Sofisticados y relativamente frecuentes en el ámbito militar; (8) Dificultades para su comprobación; (9) Dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales; (10) Ofrecen a los menores de edad facilidades para su comisión, (11) Proliferación; (12) De mera actividad y con permanencia del hecho, pueden repetirse continuamente en el tiempo, en razón que son de comisión instantánea, se perfeccionan con la acción u omisión, no es necesario el daño, sus efectos son permanentes; (13) Pluriofensivos y masivos, porque pueden afectar varios bienes jurídicos y a varios sujetos pasivos; y (14) Transfronterizos, porque se valen del Internet, por lo que puede tener efectos en varios países.(Espinoza Coila, 2017)

El sujeto activo de los Delitos Informáticos, es cualquier persona, con dominio técnico como lenguajes de programación, hardware de ordenadores, redes de informática, sistemas operativos, Ingeniería Social, etc. y el sujeto pasivo, también es cualquier persona, natural y jurídica (asociaciones, empresas y entidades públicas), titulares de los bienes jurídicos, sobre los cuales recae la actividad típica.(Espinoza Coila, 2017)

6. TRATAMIENTO DE LOS DELITOS INFORMÁTICOS EN EL DERECHO PERUANO Y COMPARADO

Los delitos informáticos en el Perú, están previstos en la Ley N.º 30 096 "Ley de Delitos Informáticos" del 2 013, modificado por la Ley N.º 30 171 del 2014; y en el Derecho Comparado, se encuentran regulados por diversas leyes especiales o en el mismo Código Penal de países como, Estados Unidos, Alemania, Francia, España, Chile, Argentina y Ecuador. (Espinoza Coila, 2017)

Ahora bien procedemos a la concreción de este punto de la tesis, enumerando los delitos informáticos y a describirlos a grosso modo, los delios regulados en Perú son: a) Acceso Ilícito, b) atentado a la integridad

de datos informáticos, c) atentado a la integridad de sistemas informáticos, d) proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos (grooming), e) interceptación de datos informáticos, f) fraude informático, g) suplantación de identidad y h) abuso de mecanismos y dispositivos informáticos,

Los mencionados delitos tiene por común origen genealógico fechado el 12 de octubre de 1 984, con la promulgación de la Ley "Counterfeit Access Device and Computer Fraud and Abuse Act", que incorporó la §1 030 en el Código Federal de los Estados Unidos de Norteamerica, se forjaron en medio de la guerra fría, la legislación pretendía evitar la fuga de información confidencial del Gobierno y de las empresas hacia manos de los enemigos, el resto de países, importaron los tipos penales con una afinación en los *nomen juris* y las formulas legales sin un saneamiento ideológico que lo recusara, porque los gobiernos receptores también pretendían usar el discurso de la seguridad nacional implementando sistemas de inteligencia so pretexto de combatir el terrorismo y el espionaje con las tecnologías de información, cuando en realidad solo les importo amplificar el poder de vigilancia del poder punitivo, en la actualidad está permeando el orbe el Convenio de Budapest "Convenio sobre la Ciberdelincuencia" que influencio para emitir una ley especial sobre delitos informáticos en el ordenamiento jurídico peruano.(Espinoza Coila, 2017)

El sujeto activo, por lo general, con excepción de delitos cometidos contra la indemnidad sexual, es cualquier persona natural, en cuanto al sujeto pasivo, éste puede ser una persona natural o jurídica; en cuanto al agente del delito, nos parece conveniente que este posea real y efectivamente los conocimientos técnicos para realizar las conductas típicas. Las conductas son dolosas, de mera actividad, se admite la participación, es posible el concurso con otros delitos, y los bienes jurídicos son: confidencialidad de datos y sistemas informáticos, integridad y disponibilidad de los sistemas informáticos, indemnidad sexual, disponibilidad de datos de los sistemas informáticos, patrimonio, fe pública, disponibilidad e integridad de datos y sistemas informáticos(Espinoza Coila, 2017)

7. DIMENSIÓN ESPACIAL Y TEMPORAL DE LOS DELITOS INFORMÁTICOS

Los delitos informáticos son transnacionales, cuando la acción se ejecuta en un país y el resultado en otro país, y más cuando la transferencia de datos es internacional, esto eleva ubicuidad, los riesgos y la complejidad en su investigación, por ello necesario que el Perú y los países de Latinoamérica suscriban un instrumento internacional de cooperación y persecución de la ciberdelincuencia. En cuanto a la aplicación temporal de la ley penal, esto, no pasa de lo ordinario, si el delito se dio en nuestro país, se debe emplear los Principios de aplicación temporal del Código Penal, y si es en el exterior procedemos se-

gún el Derecho Penal internacional, de igual modo para la aplicación espacial. (Acurio Del Pino, 2007; Espinoza Coila, 2017; Reyna Alfaro, 2002; Sieber, 2008)

8. CONSIDERACIONES DE POLÍTICA CRIMINAL SOBRE LOS DELITOS INFORMÁTICOS

La Criminología Cautelar, nos indica que criminalización mediática, considera los conflictos sociales como delitos, para denotar que se está solucionando el problema con ello se potencia más el poder punitivo, y se legitima la sociedad de control, denominándola Sociedad de la Información o Sociedad del Riesgo, donde el poder de vigilancia del poder punitivo con los delitos informáticos se proyecta a la vida digital de las personas, esto es, que policías, fiscales, servicio de inteligencia, etc. tienen licencia para vigilar lo que sucede en el mundo digital, por otro lado, los efectos nocivos de la selectividad del poder punitivo alimentan un estereotipo de hacker en los niños y adolescentes que son nuevo chivo expiatorio, para abrir camino al Estado de Policía en una aparente seguridad y la confianza de los habitantes en que no serán víctimas de fraude informático, acceso ilícito, etc., frente a este problema, solo nos queda deslegitimar al poder punitivo en la sociedad de control con el Derecho Penal Humano, o digamos el Derecho Penal Informático Humano, ésta sería una forma jurídica de limitar la selectividad y los efectos nocivos del poder punitivo. Finalmente para prevenir la comisión de delitos informáticos, sugerimos seguir la "Mini guía de seguridad informática " de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), que en síntesis prescribe: (a) Tener cuidado con la información que se publica en Internet, (b) No compartir videos e imágenes comprometedoras por chat o redes sociales, (c) No usar la webcam con desconocidos, (d) No responder mensajes que solicitan información personal, como cuentas de usuario, contraseñas y otros datos, (e) No hacer clic en enlaces, ni descargar archivos adjuntos de mensajes sospechosos; por último sugerimos difundir y observar los "Principios Internacionales de Derechos Humanos sobre Vigilancia de las Comunicaciones". (Electronic Frontier Foundation y otras organizaciones, n.d.; Espinoza Coila, 2017; UNODC, n.d.; Eugenio Raúl Zaffaroni, 2011)

9. CONCLUSIONES

Los límites u horizonte de proyección del Derecho Penal Informático Humano, se explica por su propia definición como saber jurídico que interpreta delitos informáticos con el método dogmático deslegitmante del Derecho Penal Humano expuesto por el maestro Eugenio Raúl Zaffaroni, para reducir los efectos del poder de vigilancia del poder punitivo en la sociedad de control; este saber tiene por objeto estudio a la seguridad jurídica, y las leyes penales sobre delitos informáticos como objeto de interpretación; tiene la función de reducir el poder de vigilancia del poder pu-

nitivo; se caracteriza por ser público, represivo, continuo, fragmentador y normativo.

La interdisciplinariedad del Derecho Informático y el Derecho Penal, se explica por su correspondencia de saberes jurídicos, que es de forma secante por la superposición en sus horizontes de proyección para la adecuada interpretación de los delitos informáticos.

El Derecho Penal Informático, como *saber jurídico penal*, tiene (a) Fuente de conocimiento, que son todas las leyes sobre delitos informáticos y (b) De información que se refiere a la bibliografía penal y de otros saberes, y *como legislación penal*, tiene (a) Fuentes de conocimiento, que son las leyes penales constitucionales (lícitas) sobre delitos informáticos y (b) De producción, que se refiere a instituciones u órganos constitucionalmente habilitadas para la sanción de leyes penales.

El Delito Informático es definido de manera analítica, como conducta, típica, antijurídica y culpable que tiene como medio u objeto de protección a las Tecnologías de la Información y Comunicación (TIC).

Los delitos informáticos en el ordenamiento jurídico peruano, están previstos en la Ley N.º 30 096 "Ley de Delitos Informáticos", modificado por la Ley N.º 30 171 que se inspiró en el Convenio sobre la Ciberdelincuencia; también se encuentran tipificados en varios países, como lo Estados Unidos de Norte América, Alemania, Francia, España, Chile, Argentina, y Ecuador.

Sobre la aplicación espacial de la ley, los Delitos Informáticos son transnacionales, cuando la acción se ejecuta en un país y el resultado en otro país, y cuando la transferencia de datos se da en redes informáticas internacionales. En cuanto el aspecto temporal de la comisión de los delitos informáticos, se deben emplear los principios de aplicación temporal del Código Penal.

La criminalización mediática, ha fomentado los delitos informáticos, y con ella se potencia el poder punitivo, se legitima la sociedad de control y su poder de vigilancia, puesto que el poder punitivo se proyecta a la vida digital de las personas, permitiendo que agencias ejecutivas tengan posibilidad de vigilar en el mundo digital; esto tiene efectos nocivos como alimentar un estereotipo de hacker en los jóvenes de generación digital, abrir camino al Estado de Policía, y corrupción con todos los datos recopilados. Para la prevención de los delitos informáticos y del poder de vigilancia, proponemos seguir la "Mini guía de seguridad informática" de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), también difundir y observar los "Principios Internacionales de Derechos Humanos sobre Vigilancia de las Comunicaciones".

10. BIBLIOGRAFÍA

1. Acosta Patroni, A. (2003). *Hacking, cracking y otras conductas ilícitas cometidas a través de internet*. Universidad de Chile. Retrieved from http://reposi-

torio.uchile.cl/bitstream/handle/2250/114475/de-acosta_a.pdf?sequence=1&isAllowed=y

2. Acurio Del Pino, S. (2007). *Delitos Informáticos: Generalidades*. Retrieved from http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
3. Alcántara, J. F. (2008). *La sociedad de control Privacidad, propiedad intelectual y el futuro de la libertad*. Barcelon, España. Retrieved from https://www.versvs.net/wp-content/libros/la-sociedad-de-control/jose-alcantara-la-sociedad-de-control.pdf
4. Chomsky, N. (1998). *La cultura del terrorismo*. Barcelona, España: Editorial Popular.
5. DW. (2018a, September 28). Facebook: 50 millones de cuentas afectadas por hackeo masivo. Retrieved from http://dw.com/es/facebook-50-millones-de-cuentas-afectadas-por-hackeo-masivo
6. DW. (2018b, October 12). Facebook dice que los hackers accedieron a datos de 29 millones de cuentas. Retrieved from http://dw.com/es/facebook-dice-que-los-hackers-accedieron-a-datos-de-29-millones-de-cuentas/
7. Electronic Frontier Foundation y otras organizaciones. (n.d.). *NECESARIOS & PROPORCIONADOS PRINCIPIOS INTERNACIONALES SOBRE LA APLICACIÓN DE LOS DERECHOS HUMANOS A LA VIGILANCIA DE LAS COMUNICACIONES*. Retrieved from https://necessaryandproportionate.org/files/2016/03/04/spanish_principles_2014.pdf
8. Espinoza Coila, M. (2014). Los delitos informáticos en el Perú: Panóptico del poder punitivo. *Taripaña*, *6*, 13–16.
9. Espinoza Coila, M. (2015). LA NECESIDAD DE UNA INTERDISCIPLINARIEDAD SECANTE ENTRE EL DERECHO PENAL Y EL DERECHO INFORMÁTICO. Retrieved from http://www.unap.edu.pe/web4/la-necesidad-de-una-interdisciplinariedad-secante-entre-el-derecho-penal-y-el-derecho-informatico
10. Espinoza Coila, M. (2017). *Derecho Penal Informático: Deslegitimación del poder punitivo en la Sociedad de Control*. Universidad Nacional del Altiplano. Retrieved from http://renati.concytec.gob.pe/
11. Filmaffinity. (1983). Juegos de guerra. Retrieved from https://www.filmaffinity.com/es/film553168.html
12. Foucault, M. (2002). *Vigilar y castigar : nacimiento de la prisión*. Buenos Aires, Argentina: Siglo Veintiuno.
13. Gilles, D. (1999). Post-scriptum sobre las sociedades de control. Valencia: Pre-Textos. Retrieved from http://www.oei.org.ar/edumedia/pdfs/T10_Docu1_Conversaciones_Deleuze.pdf

14. Kindhäuser, U. (2014). Derecho penal de la seguridad. Los peligros del derecho penal en la sociedad del riesgo. *Revista Pensamiento Penal*, 2027–1743. Retrieved from http://www.pensamientopenal.com.ar/system/files/2014/10/doctrina40016.pdf

15. Lessig, L. (2005). *Cultura libre. Como las grandes meios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad*. Estados Unidos: Traficante de sueños. Retrieved from freeculture.cc/freculture.pdf

16. Mattelart, A. (2002). *Historia de la sociedad de la información*. Barcelona, España: Paidós.

17. Mattelart, A. (2009). *Un mundo vigilado*. Barcelona, España: Ediciones Paidos Iberica. Retrieved from https://books.google.com.pe/books/about/Un_mundo_vigilado.html?id=PPsrsS4e5LMC

18. Poder Ejecutivo del Perú. (2018, September 13). Decreto legislativo que aprueba la ley de gobierno digital [Decreto Legislativo].

19. Real Academia Española. (2014). *Diccionario de la lengua española* (23rd ed.). Madrid, España. Retrieved from http://dle.rae.es

20. Reyna Alfaro, L. M. (2002). *Los delitos informáticos : aspectos criminológicos, dogmáticos y de política criminal*. Jurista Editores.

21. Sieber, U. (2008). Límites del Derecho Penal. Fundamentos y desafíos del nuevo programa de investigación jurídico-penal en el Instituto Max-Planck de Derecho Penal extrajero e internacional. *Revista Penal*. Retrieved from http://www.uhu.es/revistapenal/index.php/penal/article/viewFile/366/357

22. Sieber, U. (2015). Risk Society and Preventive Criminal Law [Ponencia en la Universidad Nacional del Altiplano de Puno/Perú]. Puno: Instituto Max Planck para el Derecho penal extranjero e internacional de Friburgo.

23. Spee, F. (2017). *Cautio Criminalis*. Buenos Aires, Argentina: EDIAR.

24. Stallman, R. (2013). ¿Cuánta vigilancia puede soportar la democracia? *Boletín «Free Software Supporter»*. Retrieved from https://www.gnu.org/philosophy/surveillance-vs-democracy.es.html

25. Téllez Valdés, J. A. (2008). *Derecho informático* (4th ed.). México: McGraw-Hill Interamericana.

26. UNODC. (n.d.). *Mini guía de seguridad informática*. Retrieved from http://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Safety_Guide_Spanish.pdf

27. Ward, M., & Wall, M. (2018, November 2). Cómo dejar de ser un "ciberidiota" (y qué consecuencias puede traer serlo).

BBC. Retrieved from https://www.bbc.com/mundo/noticias/46072087

28. Zaffaroni, E. R. (2011). *La palabra de los muertos*. Buenos Aires, Argentina: EDIAR.
29. Zaffaroni, E. R. (2016). *Derecho penal humano y poder en el siglo XXI* (1st ed.). Bogotá, Colombia: Grupo Editorial Ibañez. Retrieved from http://www.pensamientopenal.com.ar/system/files/2016/10/doctrina44188.pdf
30. Zaffaroni, E. R., Alagia, A., & Slokar, A. (2002). *Derecho penal: parte general*. Buenos Aires, Argentina: EDIAR.