CIBERCRIMINALIDAD & POSTMODERNIDAD: LA CIBERCRIMINOLOGÍA COMO RESPUESTA AL ESCENARIO CONTEMPORÁNEO

Julio César García Luna[1]
Daniel Ernesto Peña Labrin[2]

RESUMEN: *En la sociedad informática de la postmodernidad, con motivo del advenimiento de las nuevas tecnologías de comunicación e información (TICs), y el acceso masivo a Internet como parte de la interactividad cibernética que vivimos, ha permitido la multiplicación de delitos y conductas desviadas que pululan en el ciberespacio, obligando a que los profesionales de la criminología se enfoquen en lo que hoy se conoce como Cibercriminología trabajando principalmente en su prevención, en tal sentido urge el conocimiento especializado de la dimensión de la problemática considerando los "espacios virtuales vs los físicos", que es la comunicación en tiempo real y globalizada de los migrantes y nativos del siglo XXI.*
PALABRAS CLAVE: *Cibercriminología, Delitos Informáticos, Internet, Nuevas Tecnologías de Información y comunicación; Código Penal.*

ABSTRACT*: In the post-modern information society, the appearance of new information and communication technologies (ICTs) and mass access to the Internet as part of the cybernetic interactivity which we live in, have allowed the increase of crimes and deviant behavior that swarm cyberspace, forcing Criminology professionals to focus on what is now known as Cyber Criminology, working mainly on its prevention. In this regard, it urges the specialized knowledge of the dimension of the problems within, considering the "virtual vs physical spaces", which is the telematic and globalized communication in real time for migrants and natives of the XXI century.*
KEYWORDS: *Cyber Criminology, Cybercrime, Internet, New Information and Communication Technologies; Penal Code.*

SUMARIO: *I. Aspectos Generales: Modernidad y Postmodernidad II. Cibercriminología en Latinoamérica: la necesidad de estudios regionales III. Extensión de la criminalidad informática IV. Reflexiones finales V. Conclusiones VI Recomendaciones VII Referencias bibliográficas VIII. Webgrafía*

I. ASPECTOS GENERALES: MODERNIDAD Y POSTMODERNIDAD

La nueva realidad en que vivimos desde diferentes puntos de vista, social, cultural, económico y jurídico deben guiar al Estado para que intervenga activamente en la prevención y sanción de los delitos, analizando sus causas y consecuencias; puesto que día a día se incrementan conductas desviadas y

[1] ***Criminólogo Presidente-Administrador Zona Sureste, Licenciatura de Criminología de la Benemérita Universidad Autónoma de Puebla, Miembro G.L.I.E. Email:*** crimimex@gmail.com
[2] ***Abogado & Sociólogo, Magíster en Derecho Penal, Segunda Especialidad en Derecho Informático, Profesor de Grado y Postgrado; Docente de la Facultad de Derecho y Ciencias Políticas de la Universidad Inca Garcilaso de la Vega - Lima- Perú. Vice Presidente de la Comisión Consultiva de Criminología del Ilustre Colegio de Abogados de Lima 2016. Email:*** oficinacist@yahoo.es

delictuosas, catalogadas como dañinas, que afectan al Estado y a la sociedad en su conjunto, a menudo motivadas por factores y etiologías que se encuentran implícitos en el ambiente donde nace y se desarrolla el ser humano como ser bio-psico-social.

No obstante, como producto del vertiginoso cambio tecnológico que ha redundado en las diferentes formas de interactuar y propiamente del fenómeno social que antes se situaba únicamente en la interacción social física y hoy vemos como ésta ha sido reemplazada ostensiblemente por la hiper conectividad telemática, y con trascendencia global. [3]

En consecuencia, las nuevas tecnologías de información y comunicación (TICs), han abierto un campo de posibilidades inimaginables de conductas con relevancia penal y criminógena, aprovechado dicha situación, para modernizar sus actividades criminales y valiéndose de las herramientas que la web 2.0 brinda en el siglo XXI. [4] Evocando a Terceiro Morón Lerma[5], nos habla del pasaje del *"homo sapiens"* a *"homo digitalis"* y destaca que, en el ciberespacio, cada individuo es potencialmente un emisor y un receptor en un medio cualitativamente diferenciado, en el que todos se comunican con todos pero, los internautas, no se localizan principalmente por su nombre, posición social o ubicación geográfica, sino a partir de centros de intereses, por lo que puede hablarse de una suerte de *"mundo virtual segregado por la comunicación, lo que obliga a la Criminología intentar ponerse al día para formular nuevos perfiles criminales que respondan a las características*

[3] El sociólogo francés ***Edgar Morín***, afirma que nos encontramos en la actualidad en la *"era de la información"* y que el gran reto que el hombre tiene delante de él, es ser capaz de poder pasar a la *"era del conocimiento"*. Las informaciones, dice Morín, son datos dispersos. Hoy en día estamos inundados de información por todas partes (Internet, los más media, etc.), incluso el máximo especialista de la disciplina más específica es incapaz de estar al corriente de todas las informaciones que sobre su tema salen diariamente. Cada vez más, la gigantesca proliferación de información escapa del control humano. El conocimiento, en cambio, es la organización de la información, la puesta en contexto y en relación de las informaciones. Sólo la información convertida en conocimiento sirve para alimentar un pensamiento capaz de entender la realidad, cuestionándosela y buscando soluciones y alternativas. Véase: **NOGUERA FERNÁNDEZ, Albert (2014)** *Prólogo de la Obra de* ***PEÑA LABRIN, Daniel****, Curso online de Sociología Jurídica*, Edit. vLex-International, Barcelona, Pág. 09

[4] **CAMPOS DELGADO Norma y Esteban RAMIREZ VILCHEZ (2013)** *Necesidad de proponer se legisle en relación al Grooming o Cyber acoso sexual infantil como delito independiente y su proposición de incorporarlo en el Código Penal Peruano*. Tesis de Grado de Abogado, Facultad de Derecho, Universidad Señor de Sipan, Pimentel, Pág.18

[5] **RIQUERT, Marcelo (2014)** *Cyberacoso sexual infantil ("Cybergrooming")*, Edit. Revista Asociación Pensamiento Penal Nº 167 de fecha 21/04/2014, Bs As, Pág. 01

suigéneris, de esta nueva criminalidad que avasalla el planeta".[6]

Al respecto, Ulrich Beck, explicaba que en un principio, la utilización de dicho concepto estuvo remitida, principalmente, al ámbito de las ciencias básica, en términos del análisis y de la evaluación del desarrollo de las nuevas tecnologías. No obstante el hecho que este tipo de evaluación avanzó mucho en términos de refinanciamiento y precisión de manera inevitable surgieron los conflictos sociales derivados de los peligros asociados al desarrollo de nuevas tecnologías.[7]

Por un lado el aspecto positivo, las TICs, admiten herramientas útiles de interconexión y desarrollo resaltando la inteligencia artificial que antes era propia el cerebro humano, sin embargo desde un punto de vista negativo trae consigo una serie de potenciales peligros para adultos y sector empresarial, principalmente a niños, niñas y adolescentes quienes son posibles víctimas de la demencia digital, a menudo por falta de capacidad y suficiencia para discernir las verdaderas intenciones de las personas con quienes sostienen relaciones virtuales y vulneración de sistemas de seguridad, de tal forma que analizando este tema podremos entender y conocer las verdaderas dimensiones y desarrollo de los medios informáticos (cibernética), el uso del internet y las computadoras, con las que día a día nos relacionamos tal vez sin percibir sus consecuencias.[8]

Por lo tanto, el progreso de la informática es una de las características primordiales y destacada del presente milenio, por lo que su utilización comprende un abanico de posibilidades que es indispensable delimitar a fin de combatir los excesos que se vienen apreciando[9]. Empero el desarrollo de las TICs, han revolucionado la forma de comunicarnos y permitiendo que sean hoy

---

[6] **PEÑA LABRIN, Daniel (2015)** *Delitos Informáticos contra la Indemnidad y Libertades Sexuales: Ley N°30096,* Edit. Instituto Pacífico. Actualidad Penal, Febrero N°8 Lima

[7] Citado por: **PAULUS SANTIBAÑEZ, Nelson (2004)** Del Concepto de Riesgo: Conceptualización del Riesgo de Luhmann y Beck, Edit. Revista Mad.N°10, Mayo. Departamento de Antropología. Universidad de Chile. Santiago de Chile,Pág.01

[8] Nos hemos convertido en ciudadanos *"adictos a la seguridad pero siempre inseguros de ella",* lo aceptamos como si fuera lógico, o al menos inevitable hasta el punto que en opinión de *Zygmunt Bauman*, contribuimos a *"normalizar un estado de emergencia*". Citado por VÁZQUEZ ROCCA, Adolfo (2008) *Zigmunt Bauman: Modernidad Liquida y Fragilidad Humana*. Edit. Revista Crítica de Ciencias Sociales, Madrid, Pág.05

[9] **BLOSSIERS HÜME, Juan (2004)** *Criminalidad Informática*, Edit. Portocarrero, Lima.Pág.271

cada vez más las personas que poseen acceso a las mismas acordando la brecha digital que aun constituye un óbice al desarrollo. Si bien la utilización de éstas trajo ventajas significativas, también vino aparejado del surgimiento de sucesos delictógenos por el mal uso de las mismas no existiendo límites de lo permitido o no en la red. De aquí surge el cuestionamiento: ¿Existen el tiempo y el espacio en el ciberespacio? Evidentemente no, cualquier persona desde cualquier lugar del mundo puede cometer un delito o conducta desviada contra otra *online,* basta con que tenga una conexión a Internet, asimismo ¿las víctimas son más vulnerables?, también la respuesta es que sí, porque el ciberespacio es un lugar desconocido, un lugar en el que se puede engañar mejor, porque existe el anonimato, la posibilidad de ser cualquier persona y sobre todo, la eventualidad de hacer creer cualquier cosa a cualquiera en cualquier lugar del mundo[10]. Verbigracia: El *phishing*[11], *pedofilia, pornografía infantil, grooming, usurpación de identidad y amenazas por medio de correos electrónicos y redes sociales, sexting*[12] *entre otros*. Son ejemplos planteados con un cristalino examen de la realidad pluricausalista y multifactorial en la que estamos viviendo y a lo que nos enfrentamos cotidianamente. En palabras de Susana Tomasi[13] : *" El crecimiento, desarrollo y expansión de los sistemas de la información ha comenzado a plantear nuevas temáticas y desafíos respecto a la seguridad informática, ya que empresas, organismos de gobiernos, e individuos adaptados a la era digital, se han encontrado con que personas inescrupulosas se aprovechan de dicha tecnología, para cometer delitos, conductas desviadas, fraudes o apropiarse de información almacenada y usufructuarla en su provecho, por lo cual se hacen*

[10] **GONZALES GARCIA**, **Abel (2013)** *Cibercriminalidad: Secuestros virtuales como nueva modalidad delictiva*. Edit. Revista Cambio 16,02/12/13, Madrid, Pág.40

[11] **PHISHING:** Técnica utilizada para captar datos bancarios de los usuarios a través de la utilización de la imagen de la entidad bancaria. Cuando se faciliten datos bancarios a través de Internet es fundamental comprobar que se trata de páginas web con protocolos de seguridad válidos. El phishing es una técnica de captación ilícita de datos personales (*principalmente relacionados con claves para el acceso a servicios bancarios y financieros*) a través de correos electrónicos o páginas web que imitan/copian la imagen o apariencia de una entidad bancaria/financiera (*o cualquier otro tipo de empresa de reconocido prestigio*). Disponible en Internet: http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=125

[12] ***SEXTING:*** Consiste en el envío de contenidos de tipo sexual (principalmente fotografías y/o videos) producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles. http://www.sexting.es

[13] **TOMASI, SUSANA Noemí (2011)** Pericias *Informáticas de Sistemas y Computaci*ón. Compilado en Tratado Jurisprudencial y Doctrinario. Derecho Informático. Tomo II. Edit. La Ley, Bs As.

necesarios nuevos tipos de investigaciones". [14]

Reflexionar en torno al horizonte de sentido entre la modernidad y la postmodernidad es reconocer una compleja transición, se trata así mismo de un tiempo histórico de usencia de luz que nos permitiera al menos de alguna manera advertir hacia donde se orienta dicha transición o tendencia histórica.[15]

Asimismo, la posmodernidad, también llamada postmodernidad, es un concepto muy amplio que se refiere a una tendencia de la cultura, el arte y la filosofía que surgió a finales del siglo pasado. A nivel general, puede decirse que lo postmoderno se asocia al culto de la individualidad, la ausencia del interés por el bienestar común y el rechazo al racionalismo, el movimiento postmoderno, a grandes rasgos sostiene que la modernidad falló al pretender renovar las formas de pensamiento y expresión. Por eso se asocia al desencanto y la apatía ya que parte de lo entiende como un fracaso de la sociedad.[16]

De otro lado, el termino postmodernidad explica Bernardo del Rosal[17] es ambiguo y sujeto a gran controversia, hasta el extremo que hay quien ha sugerido que su uso excesivo lo ha vuelto en exceso frágil, lo postmoderno hace referencia a algo nuevo y diferente que ha sucedido en los últimos tiempos y que ya no puede ser explicado en términos de *"modernidad"*. En tal sentido, más que obsesionarnos con definir el contexto vigente, quizás la clave de bóveda esta en describir si las recientes o, incluso, las inminentes reformas penales son continuidades del pasado o, por el contrario, asistimos a verdaderas discontinuidades que rompen con ese pasado y que están dando

---

[14] Se llama ***GROOMING***, a la acción deliberada de un adulto de acosar sexualmente a un niño o niña mediante el uso de Internet. Siempre es un adulto quien ejerce el grooming. Estos adultos suelen generar un perfil falso en una red social, sala de chat, foro u otro, en donde se hacen pasar por un chico o una chica y entablan una relación de amistad y confianza con el niño o niña que quieren acosar. El mecanismo del grooming suele incluir un pedido de foto o video de índole sexual o erótica (pedido por el adulto, utilizando el perfil falso). Internet es una herramienta que brinda nuevas posibilidades a problemáticas previamente existentes. Véase: **MINISTERIO DE JUSTICIA Y DD.HH. Presidencia de la Nación (2014)** Grooming. *Guía Práctica para Adultos, Información y Consejos para entender y prevenir el Acoso a través de Internet*, Bs.As. Pàg.35

[15] **GARCIA FLORES José y Omar REYES PEREZ (2008)** *La Problemática del Horizonte de Sentido entre la Modernidad y la Postmodernidad, Temas de Ciencia y Tecnología*, Volumen 12 número 34 enero-abril. Edit. Universidad del Mar, Campus Huatulco, Pág.01

[16] Véase: Definición de postmodernidad, http://www.definicion.de/postmodernidad, Pág.01

[17] **DEL ROSAL BLASCO (2009)** Bernardo, *¿Hacia el Derecho Penal de la Postmodernidad?, Edit. Revista Electrónica de Ciencia Penal y Criminología*. http://www.criminet.ugr.es/reepe , Pág.57

origen a algo nuevo, a algo distinto, frente a lo que, por tanto, tenemos que adoptar un enfoque analítico y una estrategia diferente ante la modernización de la criminalidad. El discurso de la modernidad en Derecho Penal, a lo largo de todas sus fases de desarrollo, ha significado, básicamente, el discurso de la convicción en que el comportamiento criminal es una conducta anormal e indeseable, pero evitable y el discurso de confianza en que a través del adecuado soporte o de las adecuadas técnicas de intervención, el ser humano es capaz de modificar, reorientar o inhibir sus comportamientos criminales. Situación que es necesario reforzar en aras del control formal e informal de la cibercriminalidad.

En suma, estamos hablando lo que Blossiers Hüme[18] denominaba: *"Criminalidad Globalizada",* que es en definitiva la criminalidad en el mundo globalizado, policentrico, frio y pragmático o sea la criminalidad tal como se presenta en nuestros días y como se proyecta hacia el futuro más próximo.

II. CIBERCRIMINOLOGIA EN LATINOAMERICA: LA NECESIDAD DE ESTUDIOS REGIONALES

Desde hace casi una década el tema de las Criminologías específicas o especializadas ha tenido cabida en las discusiones entre colegas para determinar los enfoques de investigación, especialmente en México. Sin embargo, algunos de los temas particulares que atañen a nuestra ciencia, se han venido desarrollando de manera lenta pero continua, conocidos también como líneas de investigación tanto a niveles de tesis académicas como en estudios de carácter profesional en América Latina. [19]

En lo que refiere al desarrollo de la Cibercriminología, podemos aclarar que este tema ha tenido un escaso avance en publicaciones en español que permitan orientar al estudiante o investigador iniciado con las referencias suficientes para tener un panorama claro en su trabajo y que complementen los

[18] Véase: **ZAFFARONNI, Eugenio Raúl (2010)** *En Prólogo Póstumo de la Obra de* **BLOSSIERS HÜME***, Juan José, Criminalidad Globalizada y sus efectos en el Mundo*, Edit. Edimarff, Lima, Pág. 13.

[19] México recibió en los últimos cuatro años 30 mil reportes telefónicos ligados a delitos cibernéticos de los cuales el 53% fueron contra dependencias de los tres niveles de gobierno 26% contra ámbitos académicos y 21% contra el sector público o empresarios. Estas cifras colocan a México en el tercer lugar mundial con víctimas por crímenes cibernéticos sólo por debajo de China y Sudáfrica con 85 y 84% de nuevos usuarios de manera respectiva. http://www.crimimex.com.mex

textos que ya se han desarrollado desde otros campos de conocimiento a esta área aportando elementos como los análisis legislativos a inicios de la presente década[20] o aspectos de investigación de cibercriminalidad técnicos que pueden resultar útiles para criminalistas y analistas forenses[21].

Verbigracia, con respecto al acoso sexual infantil a través de la web, en el Perú como en México[22], no existía el tipo penal sub materia, vale decir a esta nueva forma de abuso sexual virtual, contándose con numerosos casos que presentan estas características y que eran denunciados por la prensa en sus noticias de *"tinta roja"*, sin embargo, en Perú el año 2013 se promulgó la Ley Nº 30096 y su modificatoria la Ley Nº 30171 en el año 2014[23], Ley de Delitos Informáticos, siendo forzoso adaptar las normas de fondo a la utilización de herramientas informáticas para cometer delitos, habiendo el legislador nacional reconocido la velocidad de la innovación de las redes, pero el tema no se agota allí hace falta políticas de información, promoción y difusión que se traduzcan en la prevención de estos execrables delitos que manchan las crónicas del orden interno y que alimentan a las agencias del control social formal e informal cotidianamente en la región[24].

Cabe aclarar que el presente ensayo, no pretende únicamente establecer deficiencias comparativas frente a otras latitudes, por el contrario se plantea que sea parte de las contribuciones que sirvan como aliciente a la

[20]**CÁMPOLI, Gabriel Andrés. (2005)** *Delitos informáticos en la legislación mexicana*. Edit. Instituto Nacional de Ciencias Penales, México.

[21]**LIRA ARTEAGA, Oscar Manuel. (2010)** *Cibercriminalidad: Fundamentos de investigación en México*, Edit. Instituto Nacional de Ciencias Penales, México.

[22] Aunque en México (2015) otros delitos informáticos como fraude digital, phishing, robo de identidad o ingreso a sistemas informáticos ajenos están tipificados en el Capítulo segundo del Código Penal Federal, artículos 211 bis 1 al bis 7, están limitados en investigación, pues casi 80% de estos ataques se realizan desde fuera del país, razón por la cual se frena estos casos. Véase. http://www.crimimex.com.mex

[23] Las fotografías o vídeos de contenido sexual, en manos de la persona inadecuada, pueden constituir un elemento para extorsionar o chantajear al protagonista de las imágenes. Se llama sextorsión al chantaje en el que alguien (*menor o mayor de edad*) utiliza estos contenidos para obtener algo de la víctima, amenazando con su publicación. Se trata de una situación delicada y difícil de abordar por un menor de edad. El adolescente, temeroso ante la posibilidad de que su sextorsionador pueda dar difusión a imágenes sensibles que le comprometerían públicamente, puede tomar la decisión de acceder a su chantaje, que normalmente consiste en seguir enviándole fotografías o vídeos de carácter sexual, y, en casos extremos, realizar concesiones de tipo sexual con contacto físico. De esta manera, el adolescente puede entrar en una espiral cuya salida pasa por no acceder a las pretensiones del hostigador, y comunicar la situación a un adulto y el ***Ciberbullyin o Cyberacoso*** entre iguales supone el hostigamiento de un menor hacia otro menor, en forma de insultos, vejaciones, amenazas, chantaje, etc., utilizando para ello un canal tecnológico. Véase: Instituto Nacional de Tecnologías de Comunicación *(2012) Pantallas Amigas, Guía sobre Adolescentes y Sexting ¿qué es y cómo prevenirlo?*, Madrid, Pág,12

[24] A pesar que el Perú no ha suscrito la Convención de Budapest del 2001, sobre Cibercriminalidad, sin embargo la Ley 30096 (2013) y su modificatoria 30171(2014) se inspiro en ella.

generación de nuevo conocimiento, advirtiendo tanto de las restricciones legales que se tienen al ser investigadores independientes a las instituciones policiales, como de las recomendaciones básicas que deben seguir para realizar análisis sólidos y de alto rigor informativo salvaguardando al mismo tiempo la integridad de posibles víctimas involucradas y la del propio intelectual, siendo el inicio de una base de experiencias que formen un criterio específico de consideración a los diversos temas disponibles para su abordaje.

Por su parte, el bloque Latinoamericano[25] ha representado para los cibercriminales una enorme oportunidad de obtener altas ganancias debido a que en dicha región existen economías que se encuentran entre las veinte más importantes del mundo y al mismo tiempo el bajo riesgo que representa ser identificados, procesados y sentenciados por la escasa criminalización informática versus la efectiva criminalización que existe en EE.UU y en la Unión Europea, redundando en la migración de la delincuencia informática a esta parte del planeta a nivel local, regional y supranacional. Sin embargo, en la mayoría de estos sectores no existe una adecuada capacitación en la investigación de conductas antisociales en el ciberespacio y tampoco cuentan con el equipo tecnológico y logístico suficientes para hacer frente a individuos con conocimientos e infraestructura que son constantemente actualizados. El Perú cuenta con la División de Investigación de Delitos de Alta Tecnología de la DIRINCRI-PNP, pero su trabajo pese a sus esfuerzos es insuficiente por la falta de apoyo logístico, presupuesto y posicionamiento en la sociedad, unido a ello la cifra negra que aún pesa en esta gama de delitos.[26]

Al mismo tiempo los congresistas han encontrado una gran cantidad de problemas para decidir si la tipificación de estas conductas debe realizarse o por el contrario es preferible ajustarlas a las ya previstas en los códigos penales sin tener que discutir la creación de nuevas leyes corriendo el riesgo de no poder sancionar aquellas que no logren encuadrarse a delitos

---

[25] **MARTIN, Paul (2015)** *Inseguridad Cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos*. Edit. Instituto Español de Estudios Estratégicos. Documento Opinión.iee.es,Pág.01

[26] Consúltese: http://www.policiainformatica.gob.pe. En la actualidad, en México la Comisión Nacional de Seguridad es quien, a nivel federal puede recibir denuncias de incidentes, para posteriormente hacer las investigaciones para ubicar y procesar a ciberdelincuentes para evitar incidentes futuros. Asimismo, la Secretaria de Seguridad Pública (SSPCDMX), ha puesto en marcha a la Policía de Ciberdelincuencia Preventiva, que tiene por objetivo el monitoreo de redes sociales y sitios web en general. https://mattica.com,Pág.01

tradicionales[27]. En esta situación, como indicamos *ultrasupra*, cibercrímenes como el *grooming y* el *sexting,* difícilmente podrían ser perseguidos por la policía hasta que tuvieran un desenlace de consecuencias dañinas contra la integridad de la víctima (fase externa del delito); en esta discusión no puede dejarse de lado que algunas legislaciones se han esforzado por redactar las primeras iniciativas para que los cibercrímenes sean considerados delitos informáticos, sin embargo nos encontramos con una atención preferencial a aquellos que afectan las actividades económicas de empresas de gran valor comercial como instituciones bancarias, esto tiene una simple explicación: las víctimas de delitos económicos suelen ser agentes de una significativa influencia política.

III.EXTENSION DE LA CRIMINALIDAD INFORMATICA

Para entender el espectro que analizamos es forzoso referirnos a lo que Bauman[28] describe como el paso a la modernidad liviana como la nueva irrelevancia del espacio, disfrazada como aniquilación del tiempo. En primer lugar, el desarrollo de unos medios de comunicación que permiten, para quien los maneja, la *"casi instantaneidad"* a escala global, así como la invisibilidad de esos usuarios para con quien no tiene acceso a dichos medios. En segundo lugar, implica la pérdida de valor del territorio en sentido estricto, el espacio tiene un valor fetiche, en términos del George Simmel, el espacio vale lo que cuesta y hoy en día puede neutralizarse miles de kilómetros en horas es la magia del tiempo real que si bien es cierto trajo innumerables satisfacciones para las demandas sociales también éstas fueron aprovechas en los últimos tiempos según Fernando Miró Linares, por los delitos informáticos y/o cibercrimenes, en referencia al vocablo anglosajón *cybercrime*, procedente de la unión entre el prefijo cyber, derivado del termino *cyberspace*, y el termino crime, como concepto que sirve para englobar la delincuencia relacionada con el uso de las Tecnologías de Información y Comunicación. En los estudios criminógenos y jurídicos llevados a cabo en ingles, ya aparece haberse

[27] **RODRIGUEZ FLOREZ, María Eugenia (2013)** *América Latina, ¿debe crear un sistema de normas armonizadas para el cibercriminal?*. Edit. Trabajos de Investigación de Políticas Públicas. Departamento de Economía Universidad de Chile, Santiago de Chile,Pág,01

[28] Citado por **MATEO GIRON, Javier (2008)** Zygmunt Bauman: Una lectura Liquida de la Postmodernidad. Revista Académica de Relaciones Internacionales, número.9, Octubre, Edit. GERI-UAM, México. http://www.relaciones internacionales.info, Pág.11

impuesto este término frente a otros que ocupan generalmente el mismo o similar espacio de significado, tales como computercrime y otros en lo que se utilizan prefijos como *virtual, onlin, high-tech,digital,computer-related,Internet-related,electronic, y e-crimes*. [29]

El internet como medio de comunicación utilizado por los ciudadanos del mundo, ha dado lugar a múltiples tendencias, una de ellas es la proliferación como dijimos de conductas desviadas y delictivas donde los cibernautas se comunican en línea a todo nivel, sin embargo, diversos comportamientos están orientadas a ocasionar daño a cuantiosas empresas, personas, jóvenes y menores de edad que a menudo interactúan sin conocimiento o ingenuidad.[30]

Es un problema real que surge del uso de información electrónica y medios de comunicación en la tierra, a consecuencia del incremento de la tecnología informática y de comunicación: Internet, correo electrónico, facebook, instagram, twuiter, whatsapp, blogs, websites, y democratización universal de los smartphone, etc. Pudiendo ser el móvil para acercarse y dañar a un individuo o grupo social, mostrando un comportamiento deliberado, repetitivo y hostil, valiéndose de las TICs, para la comisión de cualquier delito cibernético.

En Criminología existe una especialidad (cibercriminología) que se ocupa de conocer cómo influyen las actividades online en la vida offline, habiéndose celebrado en la Universidad Miguel Hernández del Elche (España: 2013), el encuentro internacional con los máximos expertos en esta materia, llegados de Australia, EE.UU. Argentina, Inglaterra y España, la temática se centró en averiguar cómo influye el ciberespacio en la configuración de la delincuencia, si es un facilitador de determinadas tipologías delictivas y que características aporta en la delincuencia.[31]

---

[29] **MIRO LINARES, Fernando (2011)** *La Oportunidad Criminal en el Ciberespacio*. *Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen*. Edit. Revista Electrónica de Ciencia Penal y Criminología. http./criminet.urg.es/recpe, Pág.07

[30] Aquí urge la necesidad impostergable de maximizar el soporte y entrenamiento de sistemas de información, implementación, análisis, optimización, localización de averías y documentación de sistemas de redes.

[31] **GONZALES GARCIA**, **Abel (2013)** Pág.41

Sin embargo, pensar que la especialización en Cibercriminología permitirá al experto lograr entender todos los cibercrímenes es una ambición desmedida, si bien muchas actividades se encuentran relacionadas (por ejemplo el *phishing, tráfico de base de datos* y el *spoofing*[32]*)* la complejidad de cada uno de los cibercrímenes existentes así como la dinámica de estos para evolucionar a través de un continuo proceso de aprendizaje de sus autores, obliga al investigador a elegir un sector específico (por ejemplo cibercrímenes sexuales, acoso contra menores, acceso a la privacidad de figuras públicas, ataques políticos, etc.) y tener acercamientos con otros sectores cuando una situación específica requiera de análisis más extensos.

Actualmente podemos observar que los ataques más comunes siguen centrándose en intereses económicos contra sectores financieros de uso diario por la clase media[33]. Por ello los intentos iníciales en crear acciones preventivas son enfocados a clientes y cuentahabientes de las instituciones bancarias, notándose una inversión económica significativa en años recientes por parte del sector privado, mientras que la parte de las autoridades han invertido fuertes cantidades de tiempo y diseño en campañas de advertencia en el uso de la información que se proporciona por medios no físicos para su identificación, con el fin de hacer uso de sus cuentas financieras personales. [34]

Estos esfuerzos con buenas intenciones probablemente han hecho más cautelosos a miles de potenciales víctimas, sin embargo mientras las campañas mantenían un mismo formato a través de los años, el uso de internet

---

[32] **SPOOFING:** En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos de investigación, es decir, un atacante falsea el origen de los paquetes haciendo que la victima piense que estos son de un host de confianza o autorizado para evitar la victima lo detecte. **GARCIA CIYI, Carlos** (2010) *"Hablemos de Spoofing-Hacking Ético"*, Blog de Seguridad informática, https://hacking-etico.com,Pág.01

[33]**PÉREZ, Ramón (2015)** *Los 10 delitos informáticos más frecuentes*. Recuperado de http://pro. giztab. com/2015/10/20/los-10-delitos-informaticos-mas-frecuentes/

[34] **hacking ético:** Suelen realizarlo expertos informáticos o consultores en esta materia para advertir a las empresas de la vulnerabilidad de sus sistemas, como forma de prevención de hackeos de carácter malicioso que pueden provocar algún tipo de perjuicio a la empresa. Estos hackers, también llamados "**white hat hackers**" ayudan a encontrar los puntos débiles del entramado web de la empresa para evitar ataques a sus redes y así encontrarse en un constante estado de prevención que aumentará la seguridad de la empresa.Esta figura es la contrapuesta a la que entendemos inicialmente por hacker, una persona que intenta constantemente acceder a datos privados de la web de una empresa o institución para sacar un beneficio económico, político o estratégico de la información sustraída. Esta figura se conoce como "**black hat hacker**". http://www.delitosinformaticos.com/03/2014/noticias/claves-del-hacking-etico Pág.01,

se intensificaba de manera progresiva llegando a la era de la conexión permanente a través de dispositivos móviles, generando un nuevo problema que ha tomado su tiempo identificar: el ingreso del cibercriminal a equipos de uso diario donde la información personal y profesional se encuentra almacenada en un mismo lugar, comprometiendo no solo la seguridad financiera de quien pierda el control (material o digital) también su integridad física y es lo que ocurre con el ciberespacio como ámbito social que tiene como caracteres intrínsecos una concreta configuración de las coordenadas espacio/tiempo, frente a la que tiene en el que podríamos denominar espacio real o físico.[35]

Es en este nuevo panorama, se suelen utilizar como sinónimos de *ciberespacio* el concepto de *"espacio virtual*", como antitético al espacio "*real".* La simultaneidad, la unicidad de momentos, puede llevar a la impresión de que el ciberespacio es la ausencia de espacio, quizás fruto del equívoco de asimilar la idea de espacio a la distancia. No obstante, el ciberespacio es real en el sentido que existe, pero se trata de una "*especie nueva"* de espacio, invisible a nuestros directos sentidos y en el que las coordenadas de espacio y tiempo adquieran otro significado y ven redefinidos su alcance y limites.[36]

La volatilidad del web 2.0, traducidas en la evolución las redes inalámbricas y del propio hardware móvil, las cámaras digitales y los videos grabadoras son cada más accesibles para los cibernautas de las grandes mayorías, así como de los sistemas de defensa bancario y financiero han creado una nueva faceta de cibercrimen que debe identificarse rápidamente para hacerle frente a la mutación del delito[37].

Es en este punto donde la participación de la Cibercriminología se vuelve crucial, ya que mientras los equipos tecnológicos mantienen un avance constante el investigador solo se ha especializado en la operación de estos, sin prestar atención de forma prioritaria al comportamiento criminal en el ciberespacio y considerando que pueden identificarse de forma previa algunas conductas que ayudarían a su prevención antes de que el hecho sea

[35] **MIRO LINARES, Fernando (2011)** Pág.05
[36] Ibidem,Pág.06
[37] **PEÑA LABRIN, Daniel (2012)** *Delito, Sexo e Internet*, Edit. Loza Avalos Abogados. Alerta Informativa, Lima Pág.144

amenazado y/o vulnerado, afectando los bienes jurídicos tutelados por la ley penal y las leyes especiales.

IV. REFLEXIONES FINALES

Ante esto, Klaus Tiedemann[38] indica: "*La tarea del Derecho no es la de quedarse atado a viejas categorías teóricas que nada sirven sino más bien de adaptarse y proveerse de nuevas formas de prevención y protección a la sociedad"*. Es por ello que el Derecho Penal informático debe revisarse así mismo, y encuadrase en estas situaciones que protejan a las personas y no esconderse en vacíos legales que no nos benefician absolutamente. [39]

Desde el ámbito internacional, hoy hablar de delitos en internet, sin un enfoque de estas características es imposible, toda vez que las redes sociales, atraviesan el globo terráqueo y no existiendo fronteras, cohabitando como dijimos una cifra negra, en esta gama de nuevos delitos. Los países más industrializados entendieron que era necesario armonizar sus leyes y establecer medios técnicos y procedimientos de cooperación para combatir los delitos cometidos por internet, América latina aún sigue siendo un reto en este milenio. [40]

Esa fue la génesis de la Convención de Ciberdelito y de otros instrumentos internacionales, tales como Protocolo adicional contra la Xenofobia en Internet; Protocolo relativo a la venta de niños que complementa

---

[38] **TIEDEMANN, Klaus (2000)** *Derecho Penal y Nuevas Formas de Criminalidad*, Edit. Idemsa, Lima, Pág. 267.

[39] Recordemos que entre los países que han adoptado medidas penales para hacer frente al acoso sexual infantil a través de la web, podemos mencionar a *Alemania, Australia, Estados Unidos, Escocia, Inglaterra*, y también *España*, con la entrada en vigor de la reforma del Código Penal, el **23 de diciembre de 2010**,se incorpora el artículo 183 bis, que introduce un nuevo tipo penal, el contacto con menores de trece años a través de las nuevas tecnologías con la intención de acercarse a dicho menor para cometer delitos de índole sexual, tales como agresiones, abusos sexuales, exhibicionismo, provocación, prostitución y corrupción de menores.

[40] ***Cifra Negra de la Criminalidad****:* Entendida como la tasa de delito desconocido y que, en consecuencia, no aparece reflejada en la estadística. Incluye dos grandes grupos. ***La Cifra Oscura*** La tasa de delitos que, habiendo sido cometidos, no se han descubierto. Aquello que no se han dictado una sentencia condenatoria, por falta de pruebas. La cifra negra se divide a su vez en dos más: ***La Cifra Oculta:*** Aquel volumen de delitos que no aparece en las estadísticas, aun conociéndose al autor por la falta de denuncia de la víctima la criminalidad oculta: Hace referencia al volumen de delitos que aparecen en las estadísticas oficiales por que la víctima desconoce que el suceso fuera un hecho delictivo. Véase en **RUEDA ROMERO, Paulino (2011)** *Sociología del Derecho* Edit. Fondo Editorial De la USMP, Lima, Pág.277

la Convención de las Naciones Unidas sobre los Derechos del Niño. Todo ello ha demostrado que la localidad del derecho debía ceder frente a la globalidad de la red, incluso en un ámbito como el derecho penal y procesal que siempre estuvo tan ligado a la soberanía de carácter territorial.[41]

Los Estados miembros del Consejo de Europa y los otros Estados firmantes del Convenio de Budapest (*redactado en el año 2001*), habían tenido experiencia en casos transnacionales y cometidos a través de internet, y coincidieron en la necesidad de llevar a cabo una política penal común destinada a prevenir la criminalidad mediante internet, a través de una legislación apropiada de cada Estado.[42]

A nivel mundial, México se ubicó como el sexto país más atacado por los cibercriminales durante el 2015[43], Si bien México y Perú aún no se adhieren a la convención y el resto de los países de la región no suscribieron inicialmente al tratado internacional por no ser parte del Consejo de Europa, nada frena que adoptemos sus ideas y sugerencias como forma de optimizar nuestras leyes, para las nuevas fronteras: el internet y el ciberespacio. Además, es cardinal reformar las normas procesales[44]. No es lo mismo la recolección de la evidencia digital que de la recolección de prueba física a la que se requiere la mayoría de casos en la reforma procesal del nuevo sistema garantistas adversarial que se viene implementando en México, Perú y otros países de la región.

---

[41] **MINISTERIO PUBLICO FISCAL (2013)** *Informe Final, Desafíos para la investigación de Delitos Informáticos*, Buenos Aires, Pág.03

[42] El Grooming, ***No estaba incorporado en la Convención de Budapest***, sino proviene del proyecto2520/2012-PE, enviado directamente por el poder Ejecutivo, iniciativa legislativa del Presidente de la República. Este proyecto de Ley planteaba un texto alternativo llamado Ley de Represión de la Cibercriminalidad y propone una serie de nuevos delitos y agravantes en nuestro Código Penal, para casos en los que se afecte la integridad de los sistemas informáticos para cometer un delito.

[43] Señaló la Directora Jurídica de Seguridad Digital y Propiedad Intelectual de Microsoft México, Jimena Mora. Véase: **EL FINANCIERO (2016)** *En Alianza con Bloomberg*. https://m.elfinanciero.com.mex, Pág.01

[44] Panamá se convirtió en el 2014 el segundo país latinoamericano, tras República Dominicana, en ratificar el convenio europeo sobre cibercriminal, primer tratado internacional sobre infracciones penales cometidas en internet. Hasta antes de este hecho, sólo cuatro países No Miembros del Consejo de Europa no eran parte del Convenio de Budapest: USA, Canadá, Japón y República Dominicana. El número de ataques perpetrados con programas maliciosos se han triplicado en los últimos dos años. En 2014, la firma de seguridad informática rusa Kaspersky reportó que se creaban 14.400 piezas de código dañino por hora, lo que redundaba en cuatro por segundo. Entre agosto de 2015 y agosto 2016, la cifra llegó a 45.833 por hora, es decir doce por segundo. Véase: App.eltiempo.com.novedades.tecnologia,30/08/2016.Pág.01

Sin embargo, existen una serie de temas susceptibles, al menos, de ser discutidos para analizar la posibilidad de introducirlos en los códigos, verbigracia, la solicitud de preservación y obtención de datos, la validez de la prueba obtenida en otro país, el registro de cosas físicas versus el registro de datos; la posibilidad de aplicar un software judicial a distancia, cuestiones de competencia, utilización de tecnología de cifrado, entre otras.[45]

En tanto, estas cuestiones abordadas y discutidas, presentan diferentes aristas que requieren ser expresamente tratadas en las leyes de la materia. De esta manera, es substancial fortalecer los mecanismos de Cooperación Internacional. En numerosos casos los procesos de transferencia de datos afectan a varios países. Cuando el presunto delincuente no se encuentra en el mismo lugar que la víctima, la investigación requiere la cooperación entre las autoridades competentes de todas las naciones que resulten afectados.

Empero, el principio de soberanía nacional no permite que un país lleve a cabo investigaciones dentro del territorio de otro país sin el expreso permiso de las autoridades locales. Además, las investigaciones deben realizarse con el apoyo interinstitucional de las naciones involucradas. En la mayoría de los casos se dispone de un sumario tiempo para que la indagación sea exitosa. Sin embargo, el clásico régimen de asistencia mutua presenta evidentes dificultades cuando se trata de investigaciones de ciberdelitos, pues los procedimientos son muy largos y tediosos sumado a ello la obsolescencia de los sistemas de protección de datos y además la judicatura desconoce la dinámica y técnica de los delitos informáticos.

Todavía queda largo camino por recorrer para lograr una legislación equivalente en todas las jurisdicciones principalmente contra el abuso sexual virtual (*Grooming*), de los niños, niñas y adolescentes[46]. Uno de los grandes problemas que surgen en torno a los Delitos Informáticos, es saber si el legislador tiene el conocimiento técnico adecuado para tipificar éstos y si

[45] Con fecha 26 de septiembre del 2015, mediante D. Leg.1234, se incorporo al Código Penal Peruano el Artículo 162-B: *"Interferencia de comunicaciones electrónicas de mensajería instantánea y similares"*.
[46] **CUENCA ESPINOSA, Alexander (2012**) El delito Informático. Una Nueva Tendencia Criminal del Siglo XXI. Su Evolución, Punibilidad y Proceso Penal, Edit. Pontificia Universidad Católica del Ecuador, Quito, Pág.02

existen las herramientas y/o actualizaciones necesarias para que los jueces puedan juzgar este tipo de ilícitos, siendo la respuesta NO[47]. Vemos que en caso de tipificar y juzgar este tipo de ilícitos quedan en la total ineficacia, ya que no contamos con profesionales a fines a estos temas que puedan, de manera idónea y garantizada, hacer punible y efectiva la justicia en estos actos antijurídicos.[48] Las discrepancias pueden causar dificultades para las investigaciones tanto a nivel nacional como internacional y, aunque la tipificación penal de estas actividades es esencial, pero la capacitación de los administradores de justicia es vital, para garantizar el éxito de los resultados de investigación punitiva, en la procura de acercarnos a los cambios que las tecnologías de información y comunicación han aportado en la aparición de estas nuevas conductas delictivas.

Urge en nuestros países de la región[49], crear, promocionar y difundir una cultura tecnológica, en la cual, a las anteriores y nuevas generaciones de ciudadanos, se les guíe y eduque sobre los mecanismos de protección para no ser víctimas de delitos informáticos, dando prioridad al empleo de personas idóneas en seguridad informática, para proteger el sistema integral y tecnológico del Estado nacional.

No obstante, tal como sostiene Santiago Mir Puig[50]: *"Sólo cuando ningún mecanismo administrativo o civil sea suficiente, entonces estará legitimado el recurso de la pena o de la medida de seguridad".* En consecuencia, las funciones del acceso y tránsito de la red y sistemas informáticos resultan ser

---

[47] Un caso sugerente revisando los programas de estudios de la Facultades de Derecho de Perú, sólo en muy pocas existe el curso de Derecho Informático, lo que deviene en un óbice jurídico, en el conocimiento y dominio de esta temática por parte de los Abogados que egresaran a finales de la segunda década del siglo XXI.

[48] El 13 de diciembre de 2011, en el seno de la Unión Europea, sea probó la Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, por la que se sustituye la ***Decisión marco 2004/68/JAI del Consejo*** acabada de mencionar. Tal y como se refleja en el considerando sexto de la misma, el delito de pornografía infantil exige la adopción de un enfoque común que abarque la acción judicial contra los delincuentes, la protección de las menores víctimas y la prevención del fenómeno. El interés superior del menor debe ser consideración primordial a la hora de poner en práctica las medidas para combatir estos delitos con arreglo a la Carta de Derechos Fundamentales de la Unión Europea y la Convención de las Naciones Unidas sobre los Derechos del Niño.

[49] Al respecto en Perú la **Ley Nº 28119 del 12/12/2003**, que prohíbe desde hace casi dieciséis años, el acceso de menores de edad a páginas web de contenido pornográfico, si bien fue un avance significativo en la tendencia de prevención general, está se volvió ineficaz al no existir la fiscalización de las *Municipalidades y de la Policía Nacional* en velar por su estricto cumplimiento.

[50] **MIR PUIG, Santiago (1996)** *Derecho Penal – Parte General*, Edit. PPU, Barcelona, Pág.189.

las pautas sobre las que deberá construirse la regulación acorde a la realidad que el derecho exige, para ubicar, perseguir, enjuiciar y punir a los responsables de estos delitos, hasta ahora premunidos del cálido manto de la impunidad, y que la legislación nacional enlace sus limitados brazos naturales y las persecuciones se programen, ejecuten y consumen en colaboracionista forma supranacional, reflejando decisiones efectivas de intervenirlos.

Por último, el tema no está agotado por el contrario lo que nos motivó abordar esta nueva problemática, son las innumerables situaciones atípicas, donde nuestros niños, niñas, adolescentes, empresas y población en general están involucrados conviviendo con la cifra negra y oculta, de esta nueva cibercriminalidad que ha rebasado los paradigmas clásicos de la sociología, derecho penal y la criminología del siglo XXI[51]. **In fine.**

V. CONCLUSIONES

PRIMERA: Debemos reconocer el amplio camino aún para lograr una legislación equivalente en todas las jurisdicciones contra la cibercriminalidad, debiendo ser claros al respecto, no se tratan de nuevos delitos propiamente dicho sino la actualización del modus operandi acorde a luz del término acuñado por Adam Staff: *"la sociedad informática* que vivimos. En tal sentido, las divergencias legales originan a menudo atipicidad para las investigaciones tanto a nivel nacional como supranacional.

SEGUNDA: Urge en la región latinoamericana informar, promover y difundir los alcances del modus operandi y perfilación criminal de la criminalidad informática a través de los medios de comunicación y redes sociales, para que la población en general conozca los alcances de lo que está

[51] **PEÑA LABRIN, Daniel (2011)** *Incorporación del tipo: Acoso Sexual infantil a través de la Web al Código Penal Peruano*, Edit. Gaceta Penal & Procesal Penal. Gaceta Jurídica, Tomo 29 Noviembre, Lima,Pág.351

prohibido y permitido en esta amplia gama de delitos. Resaltando el rol del Poder Judicial, el Ministerio Público, Defensoría del Pueblo y sus operadores jurídicos logren comprender con profundidad los parámetros de lo regulado en material criminal, a fin de construir la predictibilidad y especialidad penal, garantía constitucional que debe contener las resoluciones judiciales.

CUARTA: Se torna indispensable que la comunidad latinoamericana tome conciencia social sobre esta gama de delitos y aquí juega un papel importante la familia, la escuela y las redes sociales sobre las consecuencias nefastas de las interacciones online, los internet pertenecen a todos y a nadie, trascendiendo la vida real. Por lo tanto, los agentes de socialización y el Estado, deben informar, promover y difundir sobre las situaciones comunes que nos ponen en riesgo de los cibercriminales y que la ciudadanía por lo general no advierte, por ejemplo, informaciones delicadas tales como: otorgar datos personales: usurpación de identidades falsas, ataques a empresas, el uso de fotografías de niños o jóvenes con fines inadecuados, niños que acosan a otros niños, adultos a niños, pornografía infantil, etc. Promoviendo una política de concientización de tolerancia cero.

QUINTA: El Poder Ejecutivo mediante el Ministerio de Educación y los entes involucrados, implementen Programas de prevención, donde el eje medular se circunscriba en la creación de campañas audiovisuales que tengan como receptores a la sociedad en su conjunto y paralelamente, con cruzadas telemáticas, y que tengan como destinatarios en primer lugar a todo el círculo familiar y en segundo lugar con el compromiso de crear conciencia sobre el uso seguro de Internet en el hogar, la calle y en las empresas.

SEXTA: La universalización del Internet ha conllevado al nacimiento de distintos fenómenos y conductas, que a menudo pueden vulnerar a la capa más sensible de nuestra sociedad: nuestros niños, niñas y adolescentes. Concebimos que sea importante que estén preparados para protegerse frente a estos potenciales peligros; y que se eduquen sobre las formas en que sus derechos pueden ser vulnerados y que conozcan los patrones sanos para interactuar en la web, Además aprender a diferenciar los contenidos convenientes de los que no lo son, en una época en la cual la tecnología está condicionando al hombre en sus diferentes facetas, dicha realidad no se puede seguir soslayando.

SETIMA: La relevancia social es que se usaría la red del ciberespacio con responsabilidad, previniendo las amenazas que acechan constantemente al usar el ciberespacio y la internet o cualquier sistema informático o cibernético con responsabilidad y ética social que reivindique los valores ontológicos que son el sustento intrínseco de la persona humana como fin supremo de la sociedad y el Estado.

VI. RECOMENDACIONES

PRIMERA: Hoy en día hablar de cibercriminalidad es evocar una realidad cotidiana que nos involucra como sociedad y si bien es cierto nuestras actividades están rebasadas por la informática, más aún la sociedad civil debe formular estrategias a todo nivel para protegerse de esta nueva lacra social como lo son los delitos informáticos, aquí la criminología tiene un rol protagónico en el tema de prevención.

SEGUNDA: Vivimos en una época antropocéntrica postmoderna donde el individualismo y el placer pasajero es una de las características de este milenio, y donde el hombre ya no necesita habilidades sociales por las hiperconectividad en el

fenómeno social del siglo XXI, donde es hegemónica la interactividad telemática, dejando atrás la interacción social física del siglo XX, bajo este espectro la cibercriminología tiene el reto de la especialización en esta amplia gama de delitos y conductas desviadas que demanda el tejido social para preservar holísticamente los derechos fundamentales inspirados en el derecho natural y que hoy son de interés global por nuestras naciones. **In fine.**

VII. REFERENCIAS BIBLIOGRÁFICAS

1. **BLOSSIERS HÜME, Juan (2004)** *Criminalidad Informática*, Edit. Portocarrero, Lima.
2. **CÁMPOLI, Gabriel Andrés (2005)** *Delitos informáticos en la legislación mexicana*. Edit. Instituto Nacional de Ciencias Penales, México.
3. **CAMPOS DELGADO, Norma y Esteban RAMIREZ VILCHEZ (2013)** *Necesidad de proponer se legisle en relación al Grooming o Cyber acoso sexual infantil como delito independiente y su proposición de incorporarlo en el Código Penal Peruano*. Tesis de Grado de Abogado, Facultad de Derecho, Universidad Señor de Sipan, Pimentel
4. **CUENCA ESPINOSA, Alexander (2012)** *El delito Informático*. *Una Nueva Tendencia Criminal del Siglo XXI* .Su Evolución, Punibilidad y Proceso Penal, Edit. Pontificia Universidad Católica del Ecuador, Quito.
5. **DEL ROSAL BLASCO (2009)** Bernardo, ¿Hacia el Derecho Penal de la Postmodernidad?, Edit. Revista Electrónica de Ciencia Penal y Criminología. http://www.criminet.ugr.es/reepe
6. **EL FINANCIERO (2016)** *En Alianza con Bloomberg*. https://m.elfinanciero.com.mex
7. **GARCIA CIYI ,Carlos (2010)** *"Hablemos de Spoofing-Hacking Ético",* Blog de Seguridad informática, https://hacking-etico.com
8. **GARCIA FLORES José y Omar REYES PEREZ, (2008)** La Problemática del Horizonte de Sentido entre la Modernidad y la Postmodernidad, Temas de Ciencia y Tecnología, Volumen 12 número 34 enero-abril. Edit. Universidad del Mar, Campus Huatulco
9. **GONZALES GARCIA**, **Abel (2013)** *Cibercriminalidad: Secuestros virtuales como nueva modalidad delictiva*. Edit. Revista Cambio 16,02/12/13, Madrid.
10. **INSTITUTO NACIONAL DE TECNOLOGÍAS DE COMUNICACIÓN *(2012)*** *Pantallas Amigas, Guía sobre Adolescentes y Sexting ¿qué es y cómo prevenirlo?*, Madrid.
11. **LIRA ARTEAGA, Oscar Manuel. (2010)** Cibercriminalidad: Fundamentos de investigación en México, Edit. Instituto Nacional de Ciencias Penales, México.
12. **NOGUERA FERNÁNDEZ, Albert (2014)** *Prólogo de la Obra de **PEÑA LABRIN, Daniel**, Curso online de Sociología Jurídica*, Edit. vLex-International, Barcelona.

13. **MARTIN, Paul (2015)** *Inseguridad Cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos*. Edit. Instituto Español de Estudios Estratégicos. Documento Opinión.iee.es
14. **MATEO GIRON, Javier (2008)** Zygmunt Bauman: Una lectura Liquida de la Postmodernidad. Edit. Revista Académica de Relaciones Internacionales, número.9, Octubre, Edit. GERI-UAM, México, http://www.relaciones internacionales.info
15. **MINISTERIO DE JUSTICIA Y DD.HH. PRESIDENCIA DE LA NACIÓN (2014)** *Grooming*. *Guía Práctica para Adultos, Información y Consejos para entender y prevenir el Acoso a través de Internet*, Buenos Aires.
16. **MINISTERIO PUBLICO FISCAL (2013)** *Informe Final, Desafíos para la investigación de Delitos Informáticos*, Buenos Aires.
17. **MIR PUIG, Santiago (1996)** *Derecho Penal – Parte General*, Edit. PPU, Barcelona.
18. **MIRO LINARES, Fernando (2011)** *La Oportunidad Criminal en el Ciberespacio*. *Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen*. Edit. Revista Electrónica de Ciencia Penal y Criminología. http./criminet.urg.es/recpe
19. **PAULUS SANTIBAÑEZ, Nelson (2004)** Del Concepto de Riesgo: Conceptualización del Riesgo de Luhmann y Beck, Edit. Revista Mad.N°10, Mayo. Departamento de Antropología. Universidad de Chile. Santiago de Chile
20. **PEÑA LABRIN, Daniel (2011)** *Incorporación del tipo: Acoso Sexual infantil a través de la Web al Código Penal Peruano,* Edit. Gaceta Penal & Procesal Penal. Gaceta Jurídica, Tomo 29 Noviembre, Lima.
21. **PEÑA LABRIN, Daniel (2012)** *Delito, Sexo e Internet*, Edit. Loza Avalos Abogados. Alerta Informativa, Lima
22. **PEÑA LABRIN, Daniel (2015)** *Delitos Informáticos contra la Indemnidad y Libertades Sexuales: Ley N°30096,* Edit. Instituto Pacífico. Actualidad Penal, Febrero N°8 Lima
23. **PÉREZ, Ramón (2015)** ***Los 10 delitos informáticos más frecuentes*.** Recuperado de http://pro. giztab. com/2015/10/20/los-10-delitos-informaticos-mas-frecuentes/
24. **RIQUERT, Marcelo (2014)** *Cyberacoso sexual infantil ("Cybergrooming")*, Edit. Revista Asociación Pensamiento Penal Nº 167 de fecha 21/04/2014, Buenos Aires.
25. **RODRIGUEZ FLOREZ, María Eugenia (2013)** América Latina, ¿debe crear un sistema de normas armonizadas para el cibercriminal?. Edit. Trabajos de Investigación de Políticas Públicas. Departamento de Economía Universidad de Chile, Santiago de Chile.
26. **RUEDA ROMERO, Paulino (2011)** *Sociología del Derecho* Edit. Fondo Editorial De la USMP, Lima.
27. **TIEDEMANN, Klaus (2000)** *Derecho Penal y Nuevas Formas de Criminalidad*, Edit. Idemsa, Lima, Pág. 267.
28. **TOMASI, SUSANA Noemí (2011)** Pericias *Informáticas de Sistemas y Computació*n. Compilado en Tratado Jurisprudencial y Doctrinario. Derecho Informático. Tomo II. Edit. La Ley, Bs As.
29. **VÁZQUEZ ROCCA, Adolfo (2008)** *Zigmunt Bauman: Modernidad Liquida y Fragilidad Humana*. Edit. Revista Crítica de Ciencias Sociales, Madrid.

30. **ZAFFARONNI, Eugenio Raúl (2010)** *En Prólogo Póstumo de la Obra de* **BLOSSIERS HÜME***, Juan José, Criminalidad Globalizada y sus efectos en el Mundo*, Edit. Edimarff, Lima, Pág. 13.

VII. WEBGRAFIA

1. http://www.microsoft.com/business/eses/Content/Paginas/article.aspx?cbcid=125
2. http://www.sexting.es
3. http://www.definicion.de/postmodernidad
4. http://www.crimimex.com.mex
5. http://www.relaciones internacionales.info
6. http://pro.giztab.com/2015/10/20/los-10-delitos-informaticos-masfrecuentes/
7. http://m.elfinanciero.com.mex
8. https://hacking-etico.com
9. https://mattica.com

Puebla/Lima, Febrero 2017