Tesis

Ius et Praxis, Revista de la Facultad de Derecho
N.º 46, 2015
ISSN 1027-8168
pp. 225-240

Ciberterrorismo: amenaza fulminante. Resumen de la tesis "El delito de terrorismo informático como figura jurídica en el código penal vigente. Propuesta para su inclusión en la Ley sobre Delitos Informáticos en el Perú"

David Alonso Santiváñez Antúnez

1. Introducción

Hablar de ciberterrorismo en el mundo contemporáneo es hablar de una de las vertientes criminales más peligrosas del mundo. Rampante como ninguna, su amenaza ha proliferado en todas las vertientes, y hoy, las proyecciones que denotaba la CIA para el año 2030, en su reconocido Global Trends, no juegan más que a un desatinado presagio casi irreversible, y digo casi porque aún contamos con el tiempo de poner las cartas sobre la mesa y jugar nuestra partida en favor de la sociedad, la seguridad y el desarrollo.

El mundo globalizado cada día mejora su interconectividad. Ya nada ni nadie puede concebirse fuera de los medios electrónicos y la sociedad digital. Los medios de comunicación son cada vez más voraces y de fácil acceso para la población, las redes sociales han dejado de ser simplemente mundos alternos de sociabilización –valga la redundancia– y se han vuelto mercados con clientes abiertos a las estrategias de *marketing* –partícipes de la misma–. Qué decir de la educación a distancia, las facilidades del *cloud computing*, el *e-commerce* y las ventanas de peligrosidad que han generado las *e-drugs*. La tecnología trae aspectos buenos y malos, la web y la deep web, las *bitcoins* y otras generalidades, el ciberdelito y la

destrucción social física y digital. El mundo globalizado no se imaginó con dos caras tan bien marcadas, al igual que la concepción de Internet no se imaginó para fines sociales o comerciales, sino militares.

La discusión de las principales organizaciones mundiales sobre el tema solo nos lleva al margen de la preocupación y la preparación para enfrentar una de las amenazas más terribles para la sociedad y la humanidad. Expertos en materia de ciberseguridad, ciberdefensa y seguridad ciudadana no han desacreditado su existencia, y el aspecto legal, en algunos grupos minoritarios y sectorizados, tampoco. El mundo es cambiante, y así como cambia la sociedad cambian la vida, la economía y el delito.

Bajo todo aquello señalado, y tras una ardua investigación de cerca de tres años, nace la tesis *El delito de terrorismo informático como figura jurídica en el código penal vigente. Propuesta para su inclusión en la Ley de Delitos Informáticos del Perú*, que propone la tratativa de penalizar dicha conducta en el código penal vigente. La iniciativa de comprender que el mundo entero cada día llega más y más al ciento por ciento de la implementación digital nos lleva al alcance de ver reflejado el delito a través de la estructura digital y sus componentes. Ataques de denegación de servicio, redes *botnet* o sustracción de información a través de la minería de datos, son temas que no son ajenos al terrorismo informático, pero que no son en sí tal conducta delictiva, sino parte de un ejercicio para los fines reales del ciberterrorismo, como la destrucción de la sociedad y el colapso de las estructuras políticas.

Este es un resumen de la tesis presentada en el año en curso, tesis que busca generar conciencia en la sociedad y el ambiente jurídico y político, para iniciar un trabajo de penalización de dicha conducta, antes que siga avanzando en el ambiente real y digital, y volvamos a cometer los mismos errores que en la década de los ochenta con el terrorismo, cuando nos negamos a aceptar su existencia y pagamos las consecuencias con el capítulo más cruento de nuestra historia republicana. El terrorismo informático o ciberterrorismo está vigente en el mundo. Este texto es prueba de ello.

2. Hablando de ciberdelito antes que de ciberterrorismo

Quizás uno de los factores dignos de ser un "talón de Aquiles" en el ambiente del derecho informático sea nada más y nada menos que la definición de delito informático o ciberdelito, y es que las comparacio-

nes con la definición tradicional vertida por el derecho penal generan conjeturas cada vez más confusas en vez de soluciones prácticas. De antemano se puede decir que no existe una definición única para referirse al delito informático *per se*, por lo que se generó un nuevo concepto durante el desarrollo de la tesis, tomando el precepto del concepto tradicional de delito, marcando de esa manera que el ciberdelito, en el sentido jurídico, es "aquel delito cometido a través de medios tecnológicos o de componentes/instrumentos que puedan utilizarse con los medios tecnológicos, ya sea un *pendrive*[1], CD, entre otros". En un sentido social y evolutivo, diremos que el ciberdelito es "la evolución misma del delito a los nuevos tiempos".

El delito informático es un delito cuya arma letal es una computadora o elemento electrónico, o componentes-instrumentos que acompañen al elemento en sí, el mismo que permitirá al usuario perpetuar aquella conducta punible como si se tratase de un delincuente común; es decir, como aquellos que la normativa penal ya ha señalado. Con lo expuesto, debe considerarse que los componentes tecnológicos llevan consigo una serie de elementos que pueden aportar nuevos matices para el análisis del espacio jurídico del delito en el mundo moderno. Sin embargo, en nuestra realidad nacional, aún no hemos comprendido el poderío y la realidad que generan los ciberdelitos, mucho menos siquiera hemos comprendido su concepto o lo hemos relacionado a otros términos necesarios para comprender su magnitud, conceptos tales como ciberataque, ciberguerra, ciberdefensa, seguridad informática, informática forense o *ethical hacking*, entendiendo por tanto que a la ignorancia vertida concebimos una deficiente Ley de Delitos Informáticos en el Perú[2], incomprensible e irreal en todo contexto. Pero eso es otro tema de discusión; sin embargo, es importante entender qué es un delito informático antes de hablar de terrorismo informático o ciberterrorismo.

3. Terrorismo informático: amenaza mundial fulminante

Definir terrorismo informático resulta tan complicado como lo es el ciberdelito; esto no se debe a una cuestión generacional, sino a que resulta igual de complicado definir el concepto de terrorismo, punto

1 Dispositivo de almacenamiento.

2 Ley n.º 30096 y Modificatoria Ley n.º 30171.

de partida para entender el terrorismo informático, pues aún no existe un concepto único.

Entre los tantos conceptos que se emplearon para el desarrollo de la tesis para conceptualizar el término "terrorismo", resalta el de la Unión Europea (UE), el cual lo señala como:

> Los actos intencionados que por su naturaleza o contexto, pueden atentar gravemente contra un país o una organización internacional, intimidar gravemente a una población y obligar indebidamente a los poderes públicos o a una organización internacional a hacer o a abstenerse de hacer algo, o a desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales. (Santiváñez, J., 2013)

Igualmente, calificaron a "grupo terrorista" como "la asociación estructurada de más de dos personas, establecida en el tiempo y que actúa de forma concertada para cometer delitos terroristas" (Santiváñez, J., 2013, pp. 103-104)[3].

Como cualquier otro delito, el terrorismo informático solo se diferencia de su antecesor por el uso sistemático del terror e implementación del mismo a través de medios informáticos y electrónicos, que también son utilizados para captar partidarios para el movimiento terrorista, engañar e implantar el terror en la sociedad, ya sea a través de noticias falsas, correo electrónicos, redes sociales y acciones diversas ejecutadas por este medio. No obstante, no deja de ser un delito peligroso, no solo por la repercusión que tienen estos medios en la actualidad, y por su alcance de comunicación mundial gracias a las redes sociales. El verdadero peligro radica en la mayor proyección y en el mayor alcance de ataque, a nivel internacional, que puede llegarse a cumplir de desarrollarse por completo este delito.

Comprendemos que el delito de terrorismo siempre ha constituido peligro para la seguridad pública y del Estado, y que es prioridad de este último velar por la protección de la sociedad y su desarrollo. Sin embargo, solo los países desarrollados han empezado a centrarse en el ciberterrorismo, ubicándolo desde ya como "una amenaza sin precedentes" y cuyo avance, cada vez más veloz, amenaza con desestabilizar

3 Citando texto del diario *La Vanguardia* en su edición del 7 de diciembre de 2001.

a la sociedad por diversos flancos, en especial el generacional. Solo algunos países del continente americano ya han empezado a trabajar en políticas que les permitan enfrentar esta amenaza que está presente en la sociedad real y virtual desde hace más de diez años, y el Perú no se encuentra en la lista de los países de avanzada, a pesar de que este tema viene siendo discutido en foros internacionales en donde nuestro país está presente. Claro ejemplo de ello se muestra en nuestra actual Ley de Delitos Informáticos y en los tres anteproyectos a la norma, en donde nunca se tocó el tema para la inclusión y estudio sobre el ciberterrorismo, existiendo no solo antecedentes de hechos sino también informes de las principales organizaciones sobre el tema. A la fecha, el Pleno sigue sin proponer y debatir sobre esta posición.

3.1 Tres vertientes de una amenaza

Para comprender su presencia y tener información sobre cómo actúa el terrorismo informático, es indispensable comprender tres flancos de acción que les han dado resultados hasta la fecha.

3.1.1 Como apología del terrorismo

La apología del terrorismo es uno de los ejercicios más usados desde sus inicios y que en el ambiente de Internet ha encontrado un mayor alcance y proyección. La barrera territorial no existe, así que su accionar es más efectivo y de mayor alcance. Se ensalzan "valores" de figuras criminales –entiéndase valores por actos malignos o deplorables– para incitar al pueblo a un determinado fin, o alterar parte de la historia nacional para convencer a las masas, como lo vemos día a día, fruto del desconocimiento de las nuevas generaciones sobre las atrocidades cometidas por grupos subversivos tales como Sendero Luminoso o el MRTA[4].

Internet les ha dado la "ventaja" de expresar sus "opiniones" avalando la libertad de expresión que la misma web ampara desde sus inicios como fuente de información. Redes sociales como Facebook© o Twitter©, incluso algunas páginas como Ask.fm, son utilizadas para captar toda clase de personas e invitarlas, a través de engaños, a formar parte de grupos subversivos, aplicando la demagogia y la psicología. Uno de los casos más

4 Movimiento Revolucionario Túpac Amaru.

recientes es el reportado por la cadena de noticias CNN sobre el accionar del grupo terrorista ISIS en Internet y sus tácticas de reclutamiento a través de la página Ask.fm e Instagram©, tácticas muy bien maquinadas y que han sabido pasar desapercibidas en dichos ambientes de la web, reclutando a un gran número de jóvenes (Segall, 2014).

3.1.2 Como medio de implantación del terror

La psicología empleada por los ciberterroristas no solo tiene como fin el reclutamiento, sino también la implantación del terror. Muchos casos se dan a diario y pasan desapercibidos en la web o son tomados únicamente como *spam*[5] en nuestros *mails*, cuando en realidad se trata de casos de implantación del terror, algunos más efectivos que otros.

Si se es precavido al inspeccionar redes sociales como Facebook©, se podrá encontrar algunas sedes de grupos terroristas que ya han invadido este ambiente. En ella no solo incentivan el movimiento terrorista, sino que además utilizan las mencionadas cuentas para publicar imágenes que recuerdan aquella época dolorosa de los peruanos, en donde se mataba a gente, a los traidores a su desagradable e incomprensible *movimiento*, y otras acciones que incontables veces enlutaron al país. Niños armados, cadáveres de personas sangrando en el suelo, apologías, nombramientos de regresos y libertades de camaradas senderistas harían pensar que esto es parte de una mente sin sentido y sin comprensión alguna del dolor de la población, pero es una realidad dañina que ellos buscan reimplantar.

3.1.3 Como arma de ataque contra la sociedad y otros medios informáticos y electrónicos

El implemento de *hardware* y *software* en el accionar terrorista ha llevado a los más elaborados ataques percibidos por el hombre. Ya diría Chema Alonso, experto en seguridad informática, que "ante la complejidad de

5 *Spam* es el término utilizado para los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo). En algunos casos son de tipo publicitario o de tipo juego (enviado por desconocidos con ciertos mensajes tales como *para enamorar, cadena de dinero*, etc.), enviados en grandes cantidades (incluso, masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina *spamming*.

los ciberataques, más compleja debe ser la ciberdefensa"[6]. Si pretendemos recordar un ejemplo de ciberataque "perfecto", me atrevería a decir que el ejecutado en el año 2010 a una planta nuclear en Irán es considerado uno de los ciberataques "más efectivos de la historia"; y es que la introducción del virus denominado Stuxnet no solo significó el fin de los planes de energía nuclear en Irán, sino que además demostró el poderío de los virus informáticos a nivel mundial[7].

Si de ataques ciberterroristas hablamos, el producido en Australia en el año 2000 no solo es considerado como el primer caso de ciberterrorismo, sino que sigue siendo el más recordado cuando se habla del tema. Según informa Brian Boeting, miembro del FBI de San Francisco, en el año 2000, una persona obtuvo el control de una planta de tratamiento de desagüe cloacal y liberó un millón de litros de desechos en los ríos, causando el mayor pánico en la historia de dicha nación (Graña & Ini, 2007).

El terrorismo informático es una amenaza real. Su accionar ya ha afectado a muchos países, y los ciberataques son cada vez más constantes y perfeccionados. *Softwares* especiales, *malwares*, redes *botnet*, firmas irreconocibles, cada vez son más complejos y cada vez es mayor la responsabilidad de los países en referencia al tema; es por ello que la CIA coloca al terrorismo informático como el delito más poderoso que existirá para el año 2030; esto se deberá a que el terrorismo, de continuar en vigencia y en ataque, tomará más fuerza en la realidad mundial, y verá en los medios informáticos o electrónicos, y en las principales redes sociales, un nuevo campo no solo de captación de partidarios, sino también de ataque y destrucción, afectando a las sociedades y sus principales economías, desatando una ciberguerra sin límites (Office of The Director of National Intelligence, 2012). Solo es cuestión de tiempo para que la amenaza adquiera mayor fuerza.

6 Palabras de Chema Alonso, experto en seguridad informática, durante la clase maestra "Seguridad empresarial contra *insiders*", llevada a cabo en la Universidad Europea de Madrid, el 1 de octubre de 2014.

7 Palabras de Lorenzo Martínez Rodríguez, CTO de SECURIZAME©, experto en seguridad informática, durante el desarrollo del debate "Ángeles vs. demonios: hackers vs. abogados", llevado a cabo durante el XVII Congreso Iberoamericano de Derecho e Informática. Santa Cruz de la Sierra, Bolivia. Miércoles 16 de octubre de 2013.

3.2 Responsabilidad del Perú ante la amenaza ciberterrorista

Como se ha resaltado en el punto anterior, Perú ya se ha visto afectado por movimientos terroristas tales como Sendero Luminoso y MRTA en el ambiente de la web. No es de extrañar que su poderío se maneje en las redes sociales, principal lugar de captación de jóvenes, foco desconocedor de hechos lúgubres de las décadas de los ochenta y noventa. Es por esos mismos hechos que el país tiene la responsabilidad de combatir una vez más contra las huestes terroristas y extirparlas del país, una responsabilidad que se ve reflejada en tres aspectos que se fusionan en uno solo.

Primero, guardamos una *responsabilidad moral*, pues no podemos permitir que el terrorismo siga vigente aunque dé la apariencia de no estarlo, y pretenda ser parte de la convivencia social que tenemos nosotros, los peruanos.

Segundo, se trata de una *responsabilidad social*, pues tenemos un compromiso u obligación con la sociedad, en donde debemos velar tanto por la seguridad y desarrollo de la misma, como por la educación de la sociedad en temas sobre los tocados en este resumen.

Finalmente, mencionemos la *responsabilidad histórica*, que deriva del trabajo efectuado en la época de la máxima expresión terrorista y nuestros esfuerzos por eliminar aquel mal social que amenaza con regresar a nuestros nuevos cimientos. Debemos incentivar la responsabilidad histórica en el factor educación para no olvidar el pasado cruento y la lucha constante en nuestra nueva generación, ignorante del terror vivido en Perú, y empezar a trabajar en una mejor legislación que sancione actos terroristas, ya sean físicos o informáticos. No podemos permitir que la paz que tanto nos costó conseguir nos sea arrebatada una vez más.

4. Marco teórico: ¿cómo se avaló la veracidad de la tesis?

A este punto de avance se ha comprendido qué tan efectivo y peligroso puede llegar a ser el terrorismo informático; sin embargo, no se conoce trabajo doctrinario que pretenda tratar siquiera la superficie de este tema. Para el desarrollo de la tesis, a falta de un sustento legal, los estudios y opiniones de las principales organizaciones mundiales han avalado la presente investigación, asegurando, desde sus respectivos flancos, que la peligrosidad y existencia del terrorismo informático a nivel mundial se encuentra más latente que nunca.

Para el enfoque nacional, en primer lugar, es indispensable resaltar que, legalmente hablando, y en la actuación práctica de nuestras autoridades, *no contamos con las armas necesarias para combatir el delito de terrorismo informático*, porque es jurídicamente inexistente en nuestra normativa actual, pero no es inexistente en el mundo.

Brian Boeting, miembro del FBI de San Francisco, expuso en una entrevista la importancia de que los países empiecen a preocuparse por la ciberdefensa de sus naciones para combatir todo tipo de cibercrimen, en especial contra el terrorismo informático, al que ya consideran una amenaza emergente en el mundo entero.

Para la Organización de las Naciones Unidas, el delito cibernético evoluciona constantemente, y aquellas conductas de las que antes no se hablaba o que no eran consideradas peligrosas, hoy se visten como las amenazas más propensas en el mundo, siendo una de ellas el terrorismo informático (ONU, 2010). De igual modo, la Organización del Tratado del Atlántico Norte (OTAN) declaró, en el 2008, a través del diario inglés *The Guardian*, que "se dispone a adoptar una estrategia de defensa mundial frente al ciberterrorismo, al que considera una amenaza global similar a la estrategia militar con misiles" (Iarnoticias, 2008). De forma semejante, Sulyman Anil, máximo encargado de la OTAN para la defensa de los ataques informáticos, señaló que "la defensa cibernética ha alcanzado un nivel tan elevado como la pueda tener la defensa militar y la seguridad energética" (Iarnoticias, 2008).

Para la Organización de Estados Americanos (OEA), "los recursos disponibles en la Internet pueden ser usados para atacar sistemas militares de los países". Además, instan a los países miembros a que demuestren progresos tangibles en la lucha contra el ciberterrorismo (Elsalvador, 2003). En la página 68 de su informe[8], en el análisis denominado "The Future of Terrorism", la CIA señala que los medios digitales serán las armas y metas del futuro para los terroristas informáticos o ciberterroristas. Su peligrosidad se detallará con el paso del tiempo, y los grupos terroristas, para aquel entonces, habrán comprendido la fuerza de los *medios digitales* y del desbalance social y económico que pueden causar. Como hemos analizado en el transcurso de este texto, no solo ya ha sido comprendido en toda su magnitud, sino que en el pre-

8 Entiéndase por *informe* el documento denominado "Global Trends 2030: Alternative Worlds. A publication of the National Intelligence Council"

sente año se ha visto un manejo más progresivo de sus prácticas sucias a través de medios digitales.

Con la labor de seguir sustentando la veracidad del terrorismo informático en el mundo presente, se consultó personalmente a diversos expertos en materia legal, informática y seguridad ciudadana, cada uno con una particularidad, pero cuyo resultado siempre iba en la misma dirección: la peligrosidad del avance constante del terrorismo informático y la problemática social que generaría su meta de inestabilidad.

Para el doctor Alexander Díaz García, autor de la Ley de Delitos Informáticos de Colombia, considerada la mejor ley de delitos informáticos en el mundo, la presencia del terrorismo informático a nivel mundial no está descartada, y nuestra misión de prepararnos y estar pendientes de sus avances y planes debe ser prioridad nacional en materia de defensa (Díaz, comunicación personal, 14 de octubre de 2013).

Según el ingeniero español Lorenzo Martínez Rodríguez, CTO de SECURIZAME©, implementar medidas de seguridad informática es algo vital para mitigar los riesgos, pues la seguridad al ciento por ciento nunca se podrá obtener. Trasladado esto al ambiente del ciberterrorismo, de no tomar las medidas necesarias no solo para el combate sino para la defensa y protección, seremos un blanco fácil del accionar delictivo (Martínez, comunicación personal, 11 de noviembre de 2013).

Certificando la explicación de Martínez se encuentra el ingeniero colombiano Jhon César Arango, gerente de Proyectos de ITForensic LTDA©, quien afirma, con su vasta experiencia, que tanto las empresas como los países del Primer Mundo han tomado como prioridad la ciberseguridad, pues conocen perfectamente la amenaza que se produce día a día en el ambiente informático (Arango, comunicación personal, 11 de noviembre de 2013).

En el enfoque nacional, la opinión vertida por el experto en seguridad ciudadana, coronel PNP (R) Juan José Santiváñez Marín, resalta la falta de interés por parte del Estado peruano en los temas relacionados con la informática, el delito y su problemática; en especial, ante la presencia del delito de terrorismo informático en el Perú. Agrega que en temas de seguridad ciudadana, importantes también en el ambiente del ciberterrorismo,

> […] no existe una política de Estado en dicho aspecto, y que cada gobierno cree hacer lo mejor para hacer frente a la inseguridad existente, en donde el ciudadano común es la víctima permanente de la

> delincuencia común y organizada, sin entender que el problema de la inseguridad ciudadana no solo debe ser visto por el Poder Judicial, Ministerio Público, Policía Nacional o Ministerio de Justicia, sino que éste es un problema mucho más grande. (Santiváñez, J., 2013)

El Perú ha carecido durante muchos años de un adecuado plan para combatir la criminalidad en el ambiente informático, y prueba de su desconocimiento es la misma ley actual de delitos informáticos en el Perú, donde no solo han condicionado al extremo la conducta delictiva con los términos "ilegítimo" y "deliberado", sino que además se proyecta una imagen no acorde con la realidad ni con el ejercicio delictivo de algunas personas en la web. A eso debemos agregar que no han tenido proyecciones con la ciberseguridad, ciberguerra ni planes de ciberdefensa ante amenazas informáticas, penalizando más la actividad *hacker*, siendo una de sus vertientes necesarias e indispensables para combatir los peligros de la red y hacer más funcional el ejercicio de la seguridad y la lucha contra el terrorismo informático, el *ethical hacking*. De igual manera, el Estado peruano no se ha preocupado en educar a su población sobre los problemas que vivió el país en las épocas más oscuras del terrorismo, buscando de algún modo, con o sin intención, eliminar aquel capítulo de nuestra historia republicana, y cuyas consecuencias se ven reflejadas en el desconocimiento de una población joven y propensa a ser captada por los grupos terroristas, como así lo demuestra un "estudio estadístico" elaborado por quien redacta, durante el desarrollo de la tesis, el mismo que arrojó resultados negativos y desconcertantes al momento de cuestionar sobre los hechos de aquella época, conocimiento del accionar terrorista en ese entonces y en la época actual, sobre nuevas modalidades de apología y proyección de su ideología como son el Movadef y otras actividades. El Estado ha educado a ignorantes que no tomarán conciencia una vez estos grupos tomen fuerza de su resurgimiento actual, cuando debería enfocarse en evitar que levanten sus pilares una vez más.

En conclusión, el Estado peruano parece no ver la peligrosidad que se puede llegar a causar en el ambiente de la informática y de la sociedad en sí, cuando sus elementos se encuentren en malas manos, y que este accionar puede repercutir en la sociedad real. Un experto en el manejo de elementos informáticos y electrónicos puede llegar a robar un banco incluso en cuestión de segundos, sin la necesidad de encontrarse en el mismo país; sujetos como éste, solo con uno de estos ele-

mentos y su habilidad, causa pérdidas económicas al Estado, a los bancos y a los ciudadanos[9]. Por más que el Gobierno quiera dar la apariencia de gran inversión con los millones aplicados a la implementación de tecnologías de la información y de la comunicación (TICS), dichos avances no se pueden percibir ni en las principales instituciones del gobierno ni en la sociedad, siendo considerada una inversión pobre y carente de proyección en seguridad y en la sociedad (Santiváñez, D., 2014), incluso la más baja en comparación con sus pares como Brasil y Chile, quienes invierten cinco veces más en temas de TICS. No estamos preparados para afrontar la amenaza, pero tampoco se le está dando la importancia debida.

5. Un mundo no perdido: propuestas legales para combatir el ciberterrorismo

Luego de demostrar y reafirmar la presencia del terrorismo informático en la sociedad real y virtual, y su creciente amenaza a los principales pilares y la seguridad, se presentó un conjunto de propuestas para la penalización del terrorismo informático y su futura inclusión en la Ley de Delitos Informáticos del Perú, propuestas que fueron estudiadas y avaladas por los expertos anteriormente mencionados, y que, en palabras suyas, son medidas cuya ejecución no solo sería efectiva sino también deseable de aplicar en muchos países, de acuerdo con la realidad que se vive en tiempos actuales, especialmente en el Perú.

5.1 Mejores penas sin beneficios penitenciarios

Primer debate durante la sustentación de la tesis, pues este punto se basa en una de las teorías jurídicas de más controversia en los últimos años, pero que está regresando con fuerza debido a la inseguridad y peligrosidad que no solo se viven en el ambiente de la informática, sino también en el ambiente de la seguridad ciudadana, teoría aplicada todavía en muchos países y con resultados realmente positivos: "La Teoría del Derecho Penal del Enemigo".

9 Según un estudio realizado y publicado en el diario *Publimetro*, en el Perú se genera una pérdida de 98 millones de nuevos soles al año, producida solamente a través de la modalidad informática, dinero que no es alcanzado ni en una décima parte por los delitos de robo a bancos a mano armada.

Debemos recordar que lo que se busca es la seguridad de la nación y la protección de todos aquellos que viven en ella; por lo tanto, "ante los diferentes hechos internacionales y la peligrosidad que significaría un terrorista en las calles o en la web, ¿es factible darle beneficios penitenciarios?". Primando los principios constitucionales de "defensa y seguridad de la nación", y aplicando la Teoría del Derecho Penal del Enemigo, el terrorista, y también el ciberterrorista, "debe ser juzgado como un criminal, sin beneficios que podrían seguir perjudicando a la sociedad". Recomiendo estudiar esta propuesta, pues debemos recordar que la sanción no va unida al grado de peligrosidad del delincuente, sino a la prioridad del Estado de velar por la seguridad de la nación.

5.2 Muerte civil

Ante la duda de aplicar la primera propuesta, se generó la alternativa de "muerte civil", que debe aplicarse una vez se dicte la sentencia y cuya aplicación debe ser inmediata. Esta sanción impedirá que la persona pueda adquirir derechos y obligaciones, quedando totalmente lejos de la protección del Estado. Nuevamente, para esta medida, priman los principios constitucionales de "defensa y seguridad de la nación", principios por los que siempre ha velado la normativa legal tanto nacional como internacional. Finalmente, para una mejor efectividad de esta propuesta, debe mantenerse con conocimiento a la población sobre el estado "civilmente muerto" del delincuente.

5.3 Prohibición del uso de los medios informáticos al delincuente

Más que una alternativa legal, esta propuesta consta de una "estrategia de seguridad" que busca la constante pacificación en donde se aplique la denominada propuesta. Esta se basa en el comportamiento constante que guarda un delincuente informático y la predicción de su accionar.

Cristian Amicelli, especialista en seguridad informática de MKit Argentina©, con referencia al delincuente informático y al *ethical hacking*, resalta que "aquel que una vez atacó un sistema informático, tenga por seguro que lo volverá a hacer" (2013). Esto no solo resalta sus años de experiencia sino aquello que la prohibición busca demostrar: "La necesidad de constante exposición del delincuente informático, su factor de debilidad".

Y es que lo que busca esta propuesta es que el mismo delincuente "reincida en la conducta típica", de tal manera que su ingreso al centro penitenciario sea irrefutable. No se busca lo contrario, como querrían

algunas normas, como evitar la conducta punible, sino que esta se cometa para tener sustento de seguir resguardando la seguridad de la población; de igual modo, se buscará la sanción de aquel que, a sabiendas o no de que esta persona es un delincuente informático, le brinde los componentes necesarios para nuevamente ejecutar la conducta delictiva. Si bien hubo debate en este punto, debemos recordar que la ignorancia en la norma no exime de responsabilidad.

6. Recomendaciones

Luego de reafirmada la hipótesis es necesario brindar las siguientes recomendaciones que fueron vertidas en la tesis y buscan no solo ayudar a combatir el ciberterrorismo, sino también la ciberdelincuencia:

a) Debemos trabajar en la "modificación total" de la Ley de Delitos Informáticos del Perú, para que esta no solo incluya al delito de terrorismo informático, también para que se encuentre más acorde con la realidad nacional y mundial, y deje de ser un conjunto de vacíos legales que brindan ventaja al hampa.

b) Buscar la adhesión de Perú a los países miembros del Convenio de Budapest, con la finalidad de un mejor sustento jurídico. La resolución del primer punto puede ser un excelente sustento para pasar a formar parte del convenio de lucha contra el cibercrimen más importante del mundo.

c) Educar a la población peruana, con especial enfoque en estudiantes escolares y universitarios, sobre los hechos que se dieron en el Perú a causa del terrorismo, buscando no repetir los errores del pasado y evitando así el avance terrorista.

d) Instituir el curso de Derecho Informático como cátedra obligatoria en todas las universidades del país, pues necesitamos "abogados capacitados en la materia, para enfrentar las nuevas modalidades del crimen organizado".

e) Capacitar a jueces y fiscales en la temática del cibercrimen, ciberdelito y demás conceptos del derecho informático y la seguridad informática, con el fin de poder enfrentar y juzgar correctamente a los nuevos criminales informáticos.

f) Generar planes de seguridad ciudadana que nos permitan educar y proteger a la población nacional, para así enfrentar y evitar

el resurgimiento del terrorismo, y hacer frente al ya conocido e instaurado terrorismo informático.

g) Finalmente, de la mano con la División de Delitos de Alta Tecnología de la Dirincri, y siguiendo el ejemplo de la Marina de los Estados Unidos y del Mando Conjunto de Ciberdefensa formado en España, dar inicio a la formación de un grupo especializado en combatir no solo a los ciberterroristas y demás cibercriminales, sino que esté también capacitado para generar un sistema de defensa listo para la *ciberguerra*, un campo de batalla ya vigente en Internet desde hace más de una década.

7. Punto final

El Perú es un país que económicamente está creciendo y cuyo nivel comercial ha mejorado en los últimos años; sin embargo, los enfoques en seguridad ciudadana y cibernética han quedado en el olvido, y empezamos a vivir los estragos de un país sumergido en la delincuencia que poco a poco gana más espacio en el territorio. En planes de ciberseguridad y TICS no estamos a la par de países como Chile, Venezuela, Colombia o Costa Rica; mucho menos de países como Francia, Italia y Estados Unidos, solo por nombrar algunos países que sí vienen trabajando en planes para evitar la cibercriminalidad y prosperar en la seguridad de su nación en todo aspecto. Como se señala en la tesis,

> que el presente trabajo sirva como ejemplo para muchos países, pues si el delito ha optado por evolucionar al medio digital, es momento de que el Derecho haga lo mismo, pero con proyección, para estar a un paso delante de ellos –la delincuencia– y hacer un cambio en esta cadena evolutiva. No podemos seguir pensando que venceremos al cibercrimen con códigos que datan de una época adversa.

Referencias

Amicelli, C. (16 de octubre de 2013). "Ángeles vs demonios: *hackers* vs abogados". XVII Congreso Iberoamericano de Derecho e Informática. Santa Cruz de la Sierra, Bolivia.

Elsalvador. (24 de enero de 2003). Ciberterrorismo. Piden combatir nueva amenaza. *Elsalvador.com*. recuperado de: http://www.elsalvador.com/noticias/2003/1/24/nacional/nacio8.html

Graña, R. (Conductor), & Ini, F (Director). (24/01/2007). *Ciberterrorismo, ¿mito o realidad?* [Reportaje]. Informe Central [programa televisivo], recuperado de: http://www.youtube.com/watch?v=h4a_QlwbRjE

Iarnoticias. (12 de marzo de 2008). El 'ciberterrorismo' se convierte en una 'amenaza global' para la OTAN. *Iarnoticias.com*. recuperado de: http://www.iarnoticias.com/2008/secciones/europa/0006_ciberterrorismo_otan_06mar08.html

Office of The Director of National Intelligence. (2012). Global Trends 2030: Alternative Worlds. A publication of the National Intelligence Council. [en línea]. Recuperado de: http://info.publicintelligence.net/GlobalTrends2030.pdf

Organización de las Naciones Unidas. (2010). "Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluso en el delito cibernético". 12° Congreso de las Naciones Unidas sobre la Prevención del Delito y Justicia Penal. Respuesta al Delito Cibernético. Salvador, Brasil.

Santiváñez, D. (2014). *Perú: #NoAlSoftwarePirata.* [en línea]. Davidsantivanez.com. recuperado de: http://davidsantivanez.wordpress.com/2014/06/26/peru-noalsoftwarepirata/

Santiváñez, J. (2013). *Seguridad ciudadana. Estrategias para combatir la inseguridad ciudadana*. Lima: AFA Editores Importadores.

Segall, L. (30 de septiembre de 2014). Las tácticas de reclutamiento de ISIS: Redes sociales y videojuegos. *CNN en español*. Recuperado de: http://cnnespanol.cnn.com/2014/09/30/las-tacticas-de-reclutamiento-de-isis-redes-sociales-y-videojuegos/