

Delitos informáticos: ¿nuevas formas de criminalidad?

Autor: Mg. Edson Zelada Herrera¹

Publicado: 17/05/2021*

Introducción

En los últimos tiempos se han presentado algunos problemas en el derecho penal en torno a las condiciones de legitimidad de intervención para casos, principalmente, de fraudes, suplantación de identidad y manipulación de datos realizados a través de la internet².

En tal sentido, ensayaremos una breve opinión respecto a si debe ser necesaria la intervención del derecho penal en este ámbito, y de ser el caso, cuál debe ser el tratamiento para la obtención de su eficacia práctica.

Para ello resulta útil revisar brevemente las posiciones desarrolladas en doctrina al respecto y cuál es la situación legislativa actual en el Perú a través de la denominada Ley de los delitos informáticos³.

El derecho penal como instrumento legítimo de intervención del Estado

El punto de partida para analizar cualquier fenómeno delictivo es tener en cuenta lo siguiente: el derecho penal es parte del ordenamiento jurídico de carácter público, y al contener sanciones de carácter especialmente graves para la libertad del ser humano, requieren las mismas exigencias de legitimación para su intervención a través de la pena⁴.

La necesidad de intervención estatal en los actos cometidos a través de la internet se dio a raíz de la evolución de la sociedad misma, a partir de la denominada “*era o revolución cibernética*” aproximadamente en los años 1950, y que ha producido cambios en la transmisión de datos personales e intercambio de información personal por medio de tecnologías de la comunicación⁵.

En la doctrina, se han visto marcadas dos posiciones al respecto: la *primera*, que propugna una intervención estatal a través del derecho penal la cual se legitima en virtud a la necesidad de protección penal de la información que circula en internet; y la *segunda*, por el contrario, apuesta por un “derecho penal mínimo” y apuesta por una despenalización de estos actos en virtud a la concepción restrictiva del bien jurídico (vinculado al individuo como elemento ontológico)⁶.

Situación legislativa actual del Perú: Ley 30096 sobre delitos informáticos

En el Perú los delitos informáticos están previstos en la Ley 30096 (en adelante la Ley), la cual busca prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos cometidas mediante la utilización de tecnologías de la información o de la comunicación⁷.

Dentro de esta Ley, se protegen bienes jurídicos como **datos y sistemas informáticos**, para casos de acceso sin autorización a datos o sistemas vulnerando

medidas de seguridad; **indemnidad y libertad sexual**, si es que el agente realiza proposiciones a menores de edad por medios tecnológicos con fines sexuales; **intimididad**

y **secreto de las comunicaciones**, para sancionar a aquel que intercepta datos informáticos o utiliza indebidamente una base de datos; **patrimonio**, para casos de fraudes informáticos, y **fe pública**, si es que se comprobase una suplantación de identidad.

Si bien se ha tratado de dar soluciones a los casos que aparecen en el ámbito de la llamada ciberdelincuencia, lo cierto es que aún existen graves problemas en el fundamento para la persecución penal y la aplicación práctica de la sanción para estos delitos.

Principales problemas en torno a los delitos informáticos

Un problema que se presenta en las relaciones y actividades desarrolladas en internet es el anonimato o difícil identificación de los actores, hecho por el cual se facilitan muchas veces la comisión de hechos delictivos como se dan en casos de *hackeo*, *menoscabo a la imagen y proposiciones de índole sexual a menores de edad*. Con ello, resulta difícil la persecución de estos actos debido a la imposibilidad de identificación de los autores. Piénsese, por ejemplo, en el caso de que el sujeto A utilice datos falsos para crear una cuenta de red social y de ese modo engañe a su víctima para obtener una ventaja patrimonial (estafa) o un engaño para abusar sexualmente de un menor. Más compleja se vuelve la situación si una organización criminal dedicada al tráfico de datos, desfalca una cuenta bancaria nacional desde otro lugar distinto en otro continente.

La complejidad en la comisión de delitos informáticos ha puesto en tela de juicio incluso la legitimación de los procesos penales para estos casos. Condición básica para la imposición de una sanción (al cabo de un proceso penal) es la declaratoria del juicio de culpabilidad personal y la acreditación fehaciente de la misma a través del mecanismo probatorio. Y ello no resulta tan sencillo en casos en los que, por ejemplo, un *hacker* utiliza a otras personas, para que estas a su vez capten a otras más, que realizan las operaciones bancarias como transferencias, depósitos y retiros. En la estructura de estas organizaciones, se requiere delimitar los ámbitos de responsabilidad, para determinar quién responde por qué, es decir, quien o quienes ostentan la condición de autor, co autor, autor mediato, y cómplice, sea este primario o secundario. Lo último guarda especial relevancia de cara a la determinación judicial de la pena⁸.

Otro gran obstáculo en la lucha contra la ciberdelincuencia es el hecho de que las sanciones, tal como están previstas en la Ley, resultan ser insuficientes para el efecto intimidatorio en el potencial delincuente. La mayoría de ellas prevén penas que no superan los cuatro años (indispensables para que puedan cumplirse de manera efectiva). Con ello no se quiere decir que la solución se encuentre únicamente en la modificación de la Ley por sanciones más drásticas. Por el contrario, se debe revisar cada una de las formas contempladas en el citado texto normativo, y adecuarlas según la gravedad que revista en el bien jurídico lesionado, y contemplar formas agravadas que legitimen la sanción, como se da por ejemplo en el caso de los fraudes informáticos, en la cual la Ley no prevé aún formas agravadas para integrantes de organizaciones o bandas criminales. Con ello se legitimaría la correcta intervención estatal mediante la pena para que cada quien responda exactamente por lo que ha contribuido al delito cometido y no como se prevé hasta ahora, donde no hay claridad respecto a la sanción de los autores y partícipes.

Finalmente, otro eslabón en la cadena de adversidades es la falta de prevención por parte de los Estados. Si bien en el Perú se ha creado recientemente la Unidad Fiscal Especializada en Ciberdelincuencia, aún falta realizar las directivas, lineamientos, instructivos, guías u otros, en el ámbito de su competencia, que orienten las investigaciones en estos casos. Asimismo, falta desarrollar las políticas institucionales orientados a facilitar la obtención de la prueba digital, determinante en los procesos penales para cumplir con el debido proceso y no generar impunidad en los casos que se presentan en la práctica judicial.

Conclusiones

- Los delitos cibernéticos son nuevas formas de criminalidad que se vienen desarrollando en los últimos años a la par de las actividades en la red de internet. El fundamento de la intervención estatal en este ámbito se debe a la afectación de los diversos bienes jurídicos que merecen protección (intimidad, indemnidad sexual, patrimonio, entre otros) y se desarrollan en este contexto.
- La Ley que prevé estas formas criminales merece especial atención en torno a las conductas previstas, los bienes jurídicos que protege, y las sanciones aplicables a los autores (y partícipes). Asimismo, merece revisar determinados actos delictivos que requieren de una adecuación para delimitar ámbitos de responsabilidad y sancionar formas que aún no han sido reguladas.
- En el presente trabajo se han detallado solo algunos problemas que se presentan en el análisis de los casos de cibercriminalidad; no obstante, es una tarea pendiente el poder dar solución a estos conflictos y adversidades en torno a su aplicación, a fin de efectivizar la intervención punitiva por parte del Estado. Ello implica, sin duda alguna, la relación interdisciplinaria con otras ramas de la ciencia tales como la informática, la criminología y sociología, entre otras.
- La lucha eficaz contra la cibercriminalidad requiere mayores esfuerzos respecto de la capacitación para entender las formas complejas de aparición, y posterior persecución. Ello supone una respuesta penal adecuada acorde a la manifestación internacional de estas formas criminales⁹.

Bibliografía

- (1) Magister en Derecho Penal por la Universidad Philipps de Marburgo (Alemania). Profesor de Derecho en la Universidad Nacional Federico Villarreal. Abogado consultor del área penal en ZH Consultores.
 - (2) Marinucci, G. & Dolcini, E. (2001). Derecho penal mínimo y nuevas formas de criminalidad. *Revista Peruana de Doctrina y Jurisprudencia penales*, 2, 119 y ss.
 - (3) Poder Legislativo. (22, octubre, 2013). Ley de delitos informáticos. [Ley N. 30096]
 - (4) Freund, G., *Strafrecht Allgemeiner T.* (2008). 2 Edición. capítulo 1 margen 1
 - (5) Casación N. 367-2011-Lambayeque del 15 de julio de 2013.
 - (6) Mazuelos Coello. (2001). Delitos informáticos: una aproximación a la regulación del código penal peruano. *Revista Peruana de Doctrina y Jurisprudencia penales*, N. 2, pp. 253 y ss.
 - (7) Marinucci, G. & Dolcini, E. (2001). Derecho penal mínimo y nuevas formas de criminalidad. *Revista Peruana de Doctrina y Jurisprudencia penales*, N. 2, pp. 128 y ss.
 - (8) Cesano, J. (2008). Criminalidad económica e internacionalización del derecho penal. *Derecho Penal contemporáneo, Revista Internacional*, 24, pp. 57 y ss.
-