ENSAYO CRÍTICO DE LA GESTIÓN DOGMÁTICA DEL BIEN JURÍDICO TUTELADO EN LOS DELITOS INFORMÁTICOS EN EL PERÚ

Carlos Pajuelo Beltrán*

"… la tecnología es sin duda una aplicación
y una consecuencia pero desde
luego no la sustancia primaria.
La tecnología te lo da todo enseguida,
mientras que la ciencia avanza despacio".

Umberto Eco

RESUMEN:

Los nuevos delitos tecnológicos avanzan día a día y con ellos, quienes estudian riesgos que ponen en riesgo a las infraestructuras gubernamentales buscan la colaboración mutua de los gobiernos para la lucha y prevención del crimen tecnológico.

ABSTRACT:

New technological crimes progressing day by day, and with them, those who studied risks threatening Government infrastructures are looking for mutual collaboration of Governments to the fight and technological crime prevention.

PALABRAS CLAVES:

Criminalización; Bien Jurídico, Materia Informática; Delito Informático; Hackeo; Crakeo; Cibercrimen; Sistema Informático.

* Agente Aduanas SUNAT PERÚ.

KEY WORDS:

Criminalisation; Legal Right; Computing matter; Computer crime; Hack; Crack; Cybercrime; Computer system.

INTRODUCCIÓN

A propósito de una invitación por parte del gremio de trabajadores judiciales para poder brindar algunos alcances respecto de los llamados Delitos Informáticos en un foro muy interesante, preparamos unos apuntes que fueron desarrollando la temática sobre el bien jurídico tutelado en el llamado cibercrimen, en especial de su carácter esencial.

Como alguien curioso del tema lo primero que llamó mi atención fue la delimitación del evento criminal en materia de crímenes cometidos teniendo como instrumento a la tecnología.

Ciertamente al dar un vistazo a la legislación peruana y comparada nos dimos con la "sorpresa" de que el legislador había preparado una esquematización errónea para integrar a los llamados delitos informáticos en el cuerpo legal penal o debiera decirse corporatividad legal penal. Se vulneraba una vez más los cánones elementales mínimos para que el proceso de criminalización culmine con una norma limpia en atención a la técnica legislativa adecuada.

Carnelutti [1]dice que "…Las leyes, pues, están hechas, si no precisamente solo, por lo menos también por hombres que no han aprendido a hacerlas" refiriéndose que la calidad de juristas decae por la democratización de su elección y no su adecuada selección. En algunos casos de países vecinos, por ejemplo, el caso de Colombia para el tratamiento del intrusismo y crackeo, se adopta la solución "intermedia" con una técnica legislativa distinta y formula un título especial dentro de su código penal para tipificar la protección penal de la protección datos (data base) y de los sistemas informáticos.[2]

---

[1] Francesco Carnelutti. Cómo Nace El Derecho. Editorial Temis S.A. 2000.

[2] Ley 1273 que modifica el Código Penal colombiano.

Así también, en el caso de Chile simplemente se produce una Ley especial – Ley 19223 – que no introduce nada a la estructura de su código penal y opta por lo que se conoce como una ley penal especial. Los Estados Unidos lo tienen más claro y basan su política criminal en la protección a la seguridad de la información[3], una suerte de posición ecléctica si se quiere. En el caso peruano tenemos menudo problema, veamos.

La dogmática penal ciertamente plantea que para que un acto hecho por el hombre sea considerado delito debe de haber activado todos los pasos o fases del proceso de criminalización. Claus Roxin[4] en este sentido enuncia que no se debe perder a la solución social de conflictos como el eje de la función político-criminal de la antijuridicidad, para lo cual el legislador debe ceñirse a un número limitado de principios ordenadores.

Pues bien, al referirnos preferentemente a la criminalización primaria y secundaria tenemos que señalar la denominada alarma social en materia de uso de la tecnología prácticamente sigue la suerte de todos los demás delitos cuyo objeto de tutela jurídica es de carácter supra-individual, esto es, no acusa una gravedad más o menos ostensible. Pero, cuándo se advierte el peligro, o debiéramos decir cuándo se produce el riesgo de la afectación es cuando a niveles empresariales de alto nivel se percibe un evidente atentado a probablemente legítimos intereses económicos.

En fin, cuando se atenta contra intereses básicamente de personas jurídicas se activa la alerta propia de la teoría del control social. Entonces viene la necesidad de precisar el primer nivel de composición de todo delito, que no es otra cosa que identificar claramente el bien jurídico materia de tutela penal en materia informática.

La discusión estriba en saber si el bien objeto de tutela es la información propiamente dicha, llegando en todo caso a existir un breve

---

[3] Se tutela la seguridad personal, social y principalmente estadual en el manejo de la información vía telemática (La seguridad en la red es un concepto que debe ser materia de un estudio más amplio per se).

[4] Claus Roxin. Política Criminal y Sistema del Derecho Penal. Editorial Hammurabi SRL. 2002. Pág. 20.

avocamiento en la doctrina respecto si esta información tendría recién el rango de protección una vez que es transmitida, esto sancionaría el tráfico de la información y quedaría ligado a un nuevo sub elemento: los efectos de dicha transmisión.

Definitivamente la discusión al respecto puede seguir y seguir pero no es la intención del presente ensayo el expugnar dicha controversia sino el dirigir la atención a la técnica legislativa utilizada para la subsunción de la afectación en materia informática primero desde el punto de vista autoral y luego – ciertamente de manera inexplicable- en el ámbito de la defensa penal del patrimonio.

El dispositivo que integra los delitos informáticos a legislación penal es la ley 27309 que tiene su basamento en la protección jurídica desde el punto de "patrimonial" de la información. Aceptando aquello diremos que los delitos informáticos no pueden estar limitados a la univocidad de un bien objeto de tutela sino que este tipo de perpetración ingresa, en todo caso al plano de aquellas figuras delictivas a las que la dogmática penal otorga el carácter de pluriofensiva en cuanto al bien jurídico de tutela penal, esto es, que la lesividad produce la afectación a varios bienes jurídicos. Sin embargo la técnica legislativa elegida para el tratamiento en el código sustantivo en el caso peruano inicia una suerte de degradación de la figura penal resultante dado que en otros segmentos de la norma ya se encuentran tipificadas las diversas figuras de ciber crimen.

Por lo demás, el mismo ingreso de la figura del delito informático en la forma en que el código penal peruano viene en absorber no es la más feliz debido a que en todo caso se debió asumir la forma de una ley penal especial como en el caso de la legislación chilena[5] que optó por la ley especial y se quitó de encima la tarea de descontextualizar la tipificación de las perpetraciones contra los sistemas de información expugnando otras figuras del código penal.

---

[5] Chile. Ley 19223 *RELATIVA A DELITOS INFORMATICOS*. "Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

Existe otra posición similar a la peruana como es el caso de Colombia que genera todo un nuevo Título –el VII- en su Código Penal sobre la base de un nuevo bien jurídico tutelado que no es otra que la "protección de la información y los datos".[6] Por lo menos se observa que se trata de evitar la mezcla o confusión con otras figuras penales como nos pasa en el caso peruano.

Para empezar la norma que admite los delitos informáticos desglosa el artículo 207 del Código Penal en tres figuras adicionales. La primera ingresa en el artículo 207 A, que trata sobre el hackeo de la información. La segunda tiene el espacio mediante el denominado artículo 207 B que tipifica las prácticas de daños a sistemas de información y base de datos más conocido como crackeo. Y, por último el artículo 207 C que trata sobre las "circunstancias agravantes" de este tipo de figura consistiendo estas en el acceso y manipulación de información de relevancia en el ámbito de la seguridad nacional.

Lo primero que debemos observar es que se ingresan estas figuras dentro del Título V del código sustantivo que trata sobre los Delitos Contra el Patrimonio. Como es natural, respecto de la naturaleza patrimonial de la información ya la discusión estaba planteada de mucho tiempo atrás por cuanto dicha acepción de patrimonial tal vez sería más apropiada para los casos de información contenida en un soporte mecánico pero de ninguna manera en el caso de información contenida en un soporte magnético.

El problema de no tener claro por lo menos un modelo "racional" puede ser lesivo dado que el juzgador no tiene mucho rango de acción para evitar la falta de aproximación a la solución del caso concreto. Díez Ripollés por ejemplo invoca adoptar un modelo racional mínimo de legislación en el plano prescriptivo para no caer en error, además de un parámetro de control mínimo de la norma.[7]

---

[6] La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

[7] José Luis Díez Ripollés. "La Racionalidad Legislativa Penal: Contenidos e instrumentos de control." Revista Peruana de Ciencias Penales. Nro. 17. IDEMSA. 2005.

Es el caso del tratamiento internacional del tema tenemos que el Convenio de Budapest[8] del año 2001 la entonces Comunidad europea tuvo la intención de homologar los términos relativos a la tutela jurisdiccional penal a nivel de todos los países suscribientes y en el artículo 2 dio una pauta interesante: " Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. En realidad los europeos en este foro intentaron con vano éxito marcar la pauta para la prosecución o represión policial de las actividades y no se hizo un análisis de la base jurídica de las figuras penales pretendidas de combatir, así, lo que podría ser un meridiano avance constó en el acuerdo de que los Estados suscribientes podrán exigir como requisito tipificante tres ingredientes: que la infracción sea cometida con vulneración de medidas de seguridad y que se perpetre con la intención dolo de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático"[9].

Evidentemente la orientación europea trata de proscribir toda conducta eminentemente dolosa de ingreso a una base de datos y sancionarla pero de modo tal que aun se requiera el elemento preexistente de vulneración de un sistema de seguridad para que la tipicidad funcione.

Sin embargo la orientación de este ensayo va dirigido no al aspecto de tipicidad o culpabilidad de la conducta que se pretende acotar como negativa de manera sofisticada sino que nos interesa la afectación antijurídica que creemos mediatizada al no identificarse un claro bien u objeto de tutela penal, lo que ocasiona en la práctica esos diversos tratamientos en la legislación de cada país.

Ese tratamiento corre básicamente bajo dos vertientes: la primera que tiene que ver con la convivencia de los delitos informáticos con las

---

[8] -Convenio sobre Ciber criminalidad Budapest. 23. Nov. 2001. Considerado como el primer instrumento supranacional sobre la materia.

[9] La principal traba que encontró el Convenio de Budapest y que no pudo superar el evento de Berna al años siguiente fue el problema de la soberanía o competencia para la adecuada represión de estas actividades, pero ello no es leiv motiv del presente trabajo.

perpetraciones de carácter patrimonial. Y por otro lado la que simplemente se limita a perseguir a todo aquel que invada y afecte los sistemas informáticos protegidos por derechos de propiedad intelectual[10] y seguridad, aplicando sanciones más que severas.

En el caso peruano tenemos la mala fortuna de haber elegido la primera vía insertando las figuras de cibercrimen dentro de un marco relativo a los delitos contra el patrimonio. Insertar dentro de los delitos contra el patrimonio a las perpetraciones vía ordenador colisiona con la naturaleza misma del patrimonio que es la susceptibilidad de ser transmitido, trasladado, desplazado de un lugar en el espacio a otro lugar en el espacio.

En cambio si comparamos la naturaleza del contenido de la información contenida en un soporte magnético y las reducimos a una figura básica del delito contra el patrimonio denominada "hurto simple", encontraremos que en el caso de la información soportada magnéticamente no se puede producir el despojo o apoderamiento dado que simple y llanamente no es posible distinguir la copia de un original, llegando a afirmarse que la copia efectuada de un original puede perder calidad pero no se ha de producir el tan despreciado acto del "despojo".

El artículo 207 del Código sustantivo que fue desglosado para dar pase a las figuras de los delitos informáticos prescribe lo siguiente: "El que produce o vende alimentos, preservantes, aditivos y mezclas para consumo animal, falsificados, corrompidos o dañados, cuyo consumo genere peligro para la vida, la salud o la integridad física de los animales, será reprimido con pena privativa de libertad no mayor de un año y con treinta a cien días-multa".

La pregunta viene de natural. ¿Qué cosa tiene que ver la venta de productos ilícitos de alimentos de consumo animal con los delitos computacionales? Pues nada. Desprendiéndose que la técnica legislativa empleada en el Perú en esta materia no es del todo feliz. Y podemos sustentar ello en otros aspectos, por ejemplo, si observamos el caso de que tampoco se puede invocar la pluriofensividad del bien jurídico

[10] Emitiéndose una ley penal especial como en el caso de EEUU por ejemplo.

tutelado en materia penal dado que cada una de las figuras contenidas ya tiene una contraparte en otro acápite del código penal con sanciones incluso más altas que las que prescribe el desglosado artículo 207 A, B y C.

Así en el caso del hacker o piratería informática no hay mayor problema porque se configura el intrusismo respecto de bases de datos, sin embargo al detenernos en lo referido a que se sanciona también la copia de información en tránsito nos podemos percatar –como ya bastante lo advirtió la doctrina-[11] de la imposibilidad de equiparar el desplazamiento de la información como desplazamiento patrimonial porque no existe la cosa material necesaria para que se configure delito contra el patrimonio.

Luego nos encontramos con otra forma de delito contra el patrimonio que es el delito de daños y que se encuentra contenida en el artículo 205 que a la letra dice "… el que daña, destruye o inutiliza un bien, mueble o inmueble, total o parcialmente ajeno, será reprimido con pena privativa de libertad no mayor de dos años y con treinta a sesenta días-multa."

Nuevamente nos encontramos en la imposibilidad de equiparar la información soportada en medios magnéticos como bienes (muebles o inmuebles) total o parcialmente ajenos, de modo tal que el artículo 207 B que está orientada a sancionar los daños ocasionados en los sistemas informáticos[12] se muestra como una figura impropia penalmente.

Pues bien, para casi para finiquitar esta apreciación legal tenemos que la figuras cibercriminales como son el hackeo (intrusismo) y el crackeo (ocasionar daños al sistema informático), aparentemente más agravadas vendría a ser la contenida en el artículo 207 C que se encuentran referidas a siguientes circunstancias:

---

[11] Moisés Tambini Vásquez en su compendio sobre Informática Jurídica coincide. Universidad Alas Peruanas. Año 2007.

[12] Artículo 207-B.- Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras

- Que se efectúe dentro del ejercicio de un cargo; y,
- Que ponga en peligro la seguridad nacional.

Vemos que la primera no explica si debe tratarse de un ejercicio de cargo público o privado. En todo caso se debió el legislador ser más taxativo pero se debe entender que se trata de perpetrar en ejercicio de un cargo dentro de una entidad pública o privada. Lo que sí es relevante es el segundo acápite referido a que se considera circunstancia agravante que la actividad de hackeo o crackeo se realice poniendo en riesgo la seguridad nacional y por ejemplo en el plano del bien jurídico materia de tutela tenemos que claramente viene a ser la seguridad nacional que ya se encuentra protegida en el título XV del código sustantivo que en su Capítulo I relativo a los Atentados contra la seguridad nacional y traición a la patria (Artículo 325 al 334) se llega a establecer inclusive una pena no menor de quince años por acto de sometimiento de la patria.

Es decir que la pena es más grave que la prescrita por el artículo 207 C que plantea pena privativa de libertad no mayor a los siete años. Y ello se repite en las otras figuras, cabiendo entonces preguntarse si la normativa vigente debió – creemos que si- seguir por lo menos la égida de la ley penal especial sin alterar el código penal vigente o hacer como en el caso colombiano que procedieron a integrar un nuevo capítulo, título a esquema de clasificación de delitos sin comprometer la rígida lógica jurídica que demuestra por simple eurística y hermenéutica elemental que se produce una colisión de normas, lo que no hace otra cosa que comprometer al juez a elegir una u otra dentro de un esquema de codex propio de nuestra cultura jurídica sistémica romano germánica cada vez más en declive.

Por último, lo que debe diferenciarse claramente y no lo hace –como acabamos de probar- la técnica legislativa elegida en no solo en nuestro país sino en otros como España cuyo código penal sanciona el apoderamiento de la mensajería de correo electrónico con una pena de prisión no mayor a cuatro años, o también países dentro de la región como Brasil que para sostener su posición en contra de la perpetración de ilícitos a través del ordenador colige su legislación (Código Penal) protegiendo como un bien jurídico de naturaleza autoral el software, lo cual se encuentra en discusión (antes ya señalada y de amplio debate) en la doctrina por cuanto la naturaleza de producción intelectual del

software tiene su esencia en el derecho de propiedad industrial o patentes.

Pero es interesante el caso de Alemania[13] que plantea en una ley especial la proscripción de delitos informáticos ingresándolos al ámbito de tutela jurídica de los bienes económicos de naturaleza económica,[14]lo que si deviene en más razonable a la lógica de protección de cualquier base de datos siempre que tengan un componente de valor económico insoslayable. La pregunta sobre la necesidad de catalogar la información de acuerdo a su "importancia" en todo caso, es tarea por venir.

Una muestra de la limitación del Ius puniendi[15] estatal pertinente se da en los otros casos vinculados al cibercrimen como son los ilícitos de fraude o "estafa informática" como el caso de Fishing, Scamming (pesca a través de la clonación de páginas web el primero y utilización de argucias tecnológicas para obtener claves de seguridad y beneficiarse ilícitamente el segundo.) son delitos computacionales por cuanto se utiliza el ordenador y las Tics[16] par su perpetración.

Todos ellos ya tienen su complemento legislativo en el Título V, Capítulo V del Código penal peruano sobre Delitos Contra el Patrimonio en las figuras de estafas y otras defraudaciones de modo tal que aquí si no se vió la necesidad de agregar mayor texto el corpus juris penal, a diferencia del tratamiento del hackeo , crackeo y sus eventuales agravantes por causa de riesgo de la seguridad nacional.

Autor: Carlos Alberto Pajuelo Beltrán
Catedrático de Criminología e Informática Jurídica Facultad de Derecho de la Universidad Privada de Tacna.

---

[13] Ver el trabajo de Egil Ramírez Bejarano y Ana Rosa Aguilera Rodríguez. en el link: http://www.eumed.net/rev/cccss/04/rbar2.pdf

[14] Segunda Ley Contra la Criminalidad Económica.

[15] Hernán Hormazábal Malareé. Bien Jurídico y Estado Social y Democrático de Derecho. Edit. IDEMSA. 2005. Pág. 24-25.

[16] Tecnologías de la Información y las Comunicaciones.

Bibliografía Principal:

- Hernán Hormazábal Malareé. Bien Jurídico y Estado Social y Democrático de Derecho. Edit. IDEMSA. 2005. Pág. 24-25.

- Moisés Tambini Vásquez en su compendio sobre Informática Jurídica. Universidad Alas Peruanas. Año 2007.

- José Luis Díez Ripollés. "La Racionalidad Legislativa Penal: Contenidos e instrumentos de control." Revista Peruana de Ciencias Penales. Nro. 17. IDEMSA. 2005.

- Claus Roxin. Política Criminal y Sistema del Derecho Penal. Editorial Hammurabi SRL. 2002.

- Umberto Eco. "A Paso de Cangrejo". Primera Edición, 2007. Editorial Nomos S.A.

- Francesco Carnelutti. Cómo Nace El Derecho. Editorial Temis S.A. 2000.

- Convenio sobre Ciber criminalidad Budapest. 23. Nov. 2001. Considerado como el primer instrumento supranacional sobre la materia.

- Convenio de Berna.

- La convención sobre la Propiedad Intelectual de Estocolmo.

- La Convención para la Protección y Producción de Phonogramas de 1971.

- Segunda Ley contra la Criminalidad Económica de 1986 en Alemania.

- 10. Boletín de las Naciones Unidas sobre los delitos informáticos de 2002