BREVE ANALISIS Y ALGUNAS OBSERVACIONES AL DELITO INFORMATICO

Raúl Herrera Rosello[24]

RESUMEN

El objetivo de este trabajo es el de analizar la otra cara de la moneda, las conductas delictivas que puede generar el gran avance tecnológico, sobre todo en el campo de la informática. Si bien aun no podemos saber la envergadura de lo que se esté o pueda hacerse, es probable que su incidencia se acentúe con la expansión del uso de computadoras y redes telemáticas. Un problema actual están resultando nuestros tipos penales tradicionales los cuales son inadecuados para las nuevas formas delictivas. El desarrollo tan amplio ofrece un aspecto negativo. Abre la puerta a conductas antisociales y delictivas que se manifiestan en una multiplicidad de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales[25].

En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen de manera más eficiente, las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general. El acceso masivo a Internet, los avances tecnológicos, las cámaras digitales y los videos

[24] Estudiante de la Facultad de Derecho y Ciencia Política de la Universidad Privada Antonio Guillermo Urrelo de Cajamarca, Perú.
[25] Blossiers Hüme, Juan José, Criminología & Victimología, Editorial Disartgraf, Lima, 2005.

grabadoras son cada vez más accesibles para los cibernautas de clases media y alta. Los costos a conexiones de banda ancha propician aún más el cyberdelito.

INTRODUCCION

Los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella. En ese entendido es necesario implementar medidas preventivas, ya sean de carácter administrativo o penal que deben ser tomadas en cuenta para evitar que la comisión de este tipo de delitos alcance en el Perú los niveles de peligrosidad que se han dado en otros países.

El incuestionable perfeccionamiento actual y moderno ha traído ventajas substanciales para la humanidad, pero es penoso a su vez que vengan acompañados de hechos delictivos no anhelados, siendo imperioso e ineludible estudiar e indagar su accionar delictivo.

La definición de Delito Informático que presenta la Organización para la Cooperación Económica y el Desarrollo, señala que será cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o transmisión de datos. Estos pueden ser clasificados en las siguientes categorías (MARCHENA GOMEZ, Juan. *Prevención de la Delincuencia Tecnológica*, Editorial Lima, Lima, 1992)

a) **The Fraud for manipulation of a computer against a system of processing of information - El Fraude por manipulación de un ordenador contra un sistema de procesamiento de datos,** conocido

también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos. Podemos incluir en este concepto el cambio de datos ó informaciones para obtener un beneficio económico. Tal delito podría afectar datos que representen activos (depósitos monetarios, créditos, etc.) u objetos materiales (manejo de inventario). El uso de los cajeros automáticos, puntos de venta y otras máquinas electrónicas puede acrecentar su perpetración (introducción de datos falsos en la computadora), modificación de los resultados,[26] ó del resultante del cambio en los programas de computación, tal como las fórmulas de "Caballo de Troya" (ingreso de instrucciones para que el programa realice funciones no autorizadas, ejemplo, el acreditar la cuenta bancaria ó un salario en la cuenta designada por el delincuente) además están los programas virus (instrucciones que se infiltran automáticamente en otros programas y archivos). Dado que en algunos países la figura del fraude requiere que una persona sea engañada, ella puede no ser aplicable cuando es la computadora la que ha sido objeto del engaño.

b) **The IT Espionage and Theft of Software - El Espionaje informático y Robo de Software**. Estos delitos se refieren principalmente a la obtención (por parte de competidores) del resultado de direcciones de clientes, investigaciones, etc. Son realizados con el ingreso de

[26] Mir Puig, Santiago, Derecho Penal. Parte General, Editorial PPU, Barcelona, 1996

programas copiadores o por otros métodos (un terminal informático genera una radiación magnética esta puede ser captada y registrada sin mayor complicación hasta cerca de un kilómetro del lugar de la instalación).

c) **The IT Sabotage - el Sabotaje Informático**. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema (ejemplo: un programa temporizado que destruye el programa principal o una rutinador cáncer que distorsiona el funcionamiento de aquel mediante instrucciones que se auto reproducen.

d) **The Theft of Services -El Robo de Servicios**. Conocido también como hurto de tiempo y se da cuando los empleados utilizan sin autorización horas de máquina del empleador, para la realización de trabajos particulares.

Mediante los sistemas de acceso remoto a sistemas de procesamiento de datos podemos tener la obtención ilegal de información, destrucción de ésta u otras acciones delictuales. Los Estados Unidos tipifica penalmente el acceso no autorizado a sistemas informáticos operados por el gobierno y en particular a los asociados a la defensa nacional, las relaciones externas y la energía atómica, así como a los de instituciones financieras. La ley Sueca castigó el mero acceso a un sistema de procesamiento de datos.

Los pedófilos del ciberespacio utilizan ese medio para saciar sus anómalos apetitos y perversiones sexuales (pornografía infantil), la transmisión de imágenes de ultraje y abuso de menores en una demanda sinnúmero que los adquieren. En la variedad que ofrecen los medios del internet, aflorando una variedad de psicopatologías sexuales.

e) **Traditional offenses in the business represented by computer and Access not authorized to Systems of Processing of Information - Ofensas tradicionales en los negocios asistidos por computador y Acceso no autorizado a Sistemas de Procesamiento de Datos.-** "cometerá delito informático la persona que maliciosamente uso ó entre a una base de datos, sistema de computadores ó red de computadoras ó a cualquier parte de la misma con el propósito de diseñar, ejecutar ó alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes ó información. Asimismo, comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización, intercepta, interfiere, recibe, usa, altera, daña ó destruye una computadora, un sistema o red de computadoras, un soporte lógico ó programa de la computadora o los datos contenidos en la misma, en la base, sistema ó red". Código chileno.

La gran variedad de los delitos informáticos nos prevé evitar la distorsión y dispersidad de normas, por tanto sería conveniente postular un nuevo Título en el Libro Segundo del Código Penal, que trate la tipificación coherente y sistemática, de todas las conductas criminales que esta actividad involucra y no sólo los de carácter patrimonial.

SUJETO ACTIVO

Son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, ó bien en el uso de sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que facilitan la comisión de este tipo de delitos.

SUJETO PASIVO

Sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos, las victimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera, que usan sistemas automatizados de información generalmente conectados a otros.

LA NORMATIVIDAD DEL DELITO INFORMATICO EN NUESTRA LEGISLACION

Mediante Ley 27309, (De fecha 17 de julio del 2000) se modificó el Título V, del Libro Segundo del C. P., insertando un nuevo capítulo (Capítulo X), denominado "Delitos Informáticos", que, sólo constituyen un sector parcial de este género delictivo, orientado al ámbito patrimonial**.** Su fuente: El proyecto de "Ley de Informática" del Ministerio de Justicia de Chile (año 1986), que prescribe que: "cometerá delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier

parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información. También comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras, un soporte lógico o programa de la computadora o los datos contenidos en la misma, en la base, sistema o red".

EI Libro Segundo, Título V del C. P., contiene a través de la Ley Nº 27309-Capitulo X: Ley de Delitos Informáticos siguiente clasificación típica:

Interferencia, Acceso o copia indebida a base de datos, sistema o red de computadoras-Art. 207-A: "El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar u para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas" "Si el agente actúo con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas[27]. Tal delito es conocido también por la doctrina internacional como "Hacking lesivo" o "Hacking".

[27] Código Penal Peruano, Edit. Jurista Editores, Lima, 2008, Pág. 188. Pág. 189.

El bien jurídico protegido es el patrimonio. Sin embargo, de la descripción del tipo penal se puede denotar que el bien jurídico protegido en este delito no es el patrimonio, sino más bien, preliminarmente, la intimidad. Ello a consecuencia que en el tipo no se exige que el sujeto tenga la finalidad de obtener un beneficio económico, este requisito es constitutivo de la modalidad agravada, más no de la conducta delictiva descrita en el tipo básico, ya que el legislador considera el mero ingreso no autorizado como afectación a la intimidad. Por tanto, en el artículo 207-A, lo que se protege es la seguridad informática, ya que la conducta descrita se refiere a la utilización o ingreso indebido a una base de datos, sistema o red de computadoras, lo cual está en relación a la afectación de la seguridad informática y no el patrimonio o la intimidad, ya que se lesiona el acceso o su utilización indebido.

En tal sentido, el objeto material de la conducta realizada es la base de datos, sistema o redes informáticas. Con relación a la conducta típica, ésta comprende el hecho de utilizar o ingresar indebidamente a una base de datos, sistema o red de ordenadores. El vocablo "indebido" se refiere a lo injusto, ilícito y falto de equidad. El carácter indebido adjetiviza las conductas de ingresar o utilizar una base de datos, sistema o red de computadoras, podemos señalar que una de las características del carácter indebido de la conducta será la falta de autorización para el ingreso o utilización de la red o sistemas informáticos. Luís Alberto Bramont-Arias[28] realiza una descripción de los verbos típicos que están

[28] Bramont-Arias Torres, Luis Alberto, El Delito Informático en el Código Penal Peruano. Edit. Biblioteca de Derecho Contemporáneo, Volumen VI, Pontificia Universidad Católica del Perú, Lima, 2000, Pág. 72

comprendidos en el art. 207-A. Así, el verbo ingresar se refiere a entrar a una base de datos, sistema o red de computadoras. El verbo utilizar, hace referencia al uso de la base de datos, sistema o red de computadoras. Aclarando: Este no se refiere al sujeto activo que ingresa indebidamente, sino cuando el sujeto activo se encuentra ya dentro de la base de datos o red y comienza a utilizarla sin autorización. En dichos casos, se requiere que no se tenga la autorización debida, ya que el tipo penal señala "el que utiliza ó ingrese indebidamente"[29]. Se trata de un delito de mera actividad porque afirmamos que se trata de un tipo penal de lesión y no de puesta en peligro.

Por lo tanto, se trata de un delito doloso, el agente actúe con conciencia y voluntad de ingresar o utilizar el elemento informático indebidamente. Y éste es el sustento central de la conducta prohibida. No contar con autorización, el consentimiento del titular del sistema, base de datos o red de computadoras. El segundo párrafo del artículo 207°-A, contempla la modalidad agravada en la medida que sanciona el ingreso o utilización indebida de una base de datos o sistema informático con el fin de obtener un beneficio económico.

El sujeto activo puede ser cualquier persona mientras que el sujeto pasivo puede ser una persona natural y en el supuesto del último párrafo del artículo 207°-A, una persona natural y una persona jurídica. El tipo de delito exige el dolo del sujeto activo (subjetivo), ya que se requiere en el sujeto conciencia y voluntad de utilizar ingresar indebidamente a

[29] Reyna Alfaro, Luis Miguel, Los Delitos Informáticos, Aspectos Criminológicos, Dogmáticos y de Política Criminal, Editorial Jurista, Lima, 2002.

una base de datos o sistema informático además la concurrencia de una finalidad económica en la realización de la conducta. Por último, siendo un tipo de resultado material, es posible la configuración de la tentativa, con las dificultades ya expresadas para la consumación y prueba del ilícito, por la especialidad del delito en análisis. Asimismo, dada su característica típica, la instigación y la complicidad es perfectamente posible. El que financia, el que induce, el que presta los equipos, el que aporta los datos o claves necesarias, etc.

Alteración, daño o destrucción de base de datos (Sabotaje Informático): Art. 207-B "El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadora o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa".

Conocido también con el nombre de daño informático el artículo 207-B, comprendido en los delitos contra el patrimonio, por lo que la conducta es la de ingresar o utilizar un sistema para dañarlo o alterarlo. El bien jurídico protegido es el patrimonio, representado por el valor económico que encierra un sistema o programa de computadoras. Para mejor configuración típica, deberá sancionarse la lesión efectiva al patrimonio, hallando una mayor armonía con los principios de proporcionalidad y lesividad.

El delito de sabotaje informático comprendería las conductas de utilizar, ingresar o interferir (a diferencia del artículo 207° A. Es decir, la persona que no permite la utilización o comunicación adecuada dentro del programa o sistema informático) indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el ánimo de alterarlos, dañarlos o destruirlos. El aspecto subjetivo tenemos al dolo sumado al ánimo de dañar, destruir o alterar la base de datos o sistema informático constituye un elemento subjetivo de intención trascendente, cuya realización material no es exigida por el tipo penal. En este delito existirá la dificultad acerca de los elementos de prueba, es decir el animus del delincuente informático, el determinar la intención del sujeto activo, estaremos ante un delito de mero intrusismo informático (pena no mayor de dos años) o en el caso del delito de daño informático (pena no mayor de cinco años). A mi pensar el legislador ha debido determinar la alteración, daño o destrucción de sistemas informáticos como consumación del delito.

Luís Miguel Reyna Alfaro[30] nos manifiesta: "en el presente supuesto el legislador ha debido incluir la inhabilitación como pena principal". Esta posibilidad queda abierta para que en una sentencia (según lo dispuesto por el artículo 39 del Código Penal), el Juez Penal fije la inhabilitación como pena accesoria.

[30] Reyna Alfaro, Luis Miguel, Los Delitos Informáticos, Aspectos Criminológicos, Dogmáticos y de Política Criminal, Edit. Jurista, Lima, 2002, Pág. 278

Circunstancias Cualificantes Agravantes Art. 207-C. Nuestro Código Penal describe dos agravantes; la primera con relación al cargo que posee el sujeto activo, la segunda, en razón a la seguridad nacional.

a) El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.

b) El agente pone en peligro la seguridad nacional. De igual manera señala como agravante al agente que se aprovecha de la información que obtiene por la función que desempeña, que se relaciona con la confianza depositada en la persona del autor y en el manejo de determinada información, ej. acceso a claves, passwords, etc. Se sanciona su abuso o aprovechamiento. Estamos convencidos que aquí se incurriría en una confusión, creándose un concurso de delitos respecto del delito de abuso de información privilegiada tipificado en el artículo 251-A, de nuestro catálogo punitivo. Del aspecto subjetivo, comprenderá el dolo previsto para los artículos 207-A o 207-B y, adicionalmente, el ánimo del agente respecto del prevalecimiento de la función que desempeña.

A mi entender es atípico que el legislador decida ubicar la sistemática de los delitos informáticos dentro de los delitos contra el patrimonio, sin tener en cuenta el incluir la protección de la intimidad en alguna de sus modalidades. Esta debió ser agrupada en un solo capítulo el empleo de los medios informáticos sin importar la afectación de distintos bienes jurídicos ya sea **individuales** y **colectivos.** Al respecto, Javier Momethiano manifiesta: es un delito

multiofensivo, incluyéndose en el ámbito del Derecho Penal Económico, pues la conducta del agente constituye una avanzada forma de ataque a bienes jurídicos cuya salvaguarda ya lo había reconocido el Derecho Penal.

ALGUNAS OBSERVACIONES A NUESTRA LEGISLACIÓN

La citada ley, adolece de aspectos fundamentales; la delimitación del bien jurídico protegido. De la hermenéutica (Arte de explicar, traducir o interpretar, es el conocimiento y arte de la interpretación, sobre todo de textos, para determinar el significado exacto de las palabras mediante las cuales se ha expresado un pensamiento) de la Ley Nº 27309, sobre Delitos Informáticos, y a esto se suma la gran cantidad de inexactitudes que ésta contiene, sobre aspectos: conceptuales, gramaticales y relativos a los principios generales del Derecho Penal. De esta clase de ilícitos penales, la competencia de los Estados en la persecución de delitos se atiende al lugar de su comisión. A esta se la denomina Principio de Territorialidad, (sin dificultad cuando el delito sea cometido en territorio nacional). De otro lado, cuando la comisión del delito sea en una nación extranjera, será complicado distinguir si la acción y la afectación a la seguridad informática se originaron en el mismo lugar o no a consecuencia del amplio debate entre la Teoría de la Actividad, si el delito es cometido en donde se ha realizado la acción y la Teoría del Resultado el delito es cometido en donde se ha producido el efecto. La teoría que es seguida por nuestra legislación tal y como lo prevé el artículo 5 del

Código Penal Peruano[31]Se apoyan en la Teoría de la Ubicuidad, es decir, se puede considerar cometido el hecho tanto en el lugar donde se ha llevado a cabo la acción como en aquel en el que se ha producido el resultado.

La característica resaltante, son la del compromiso de los Estados en facilitar una investigación y persecución de los ilícitos penales vinculados con sistemas y datos informáticos, e innovar el Derecho Penal y ajustarlo a las exigencias jurídico-sociológicas. Resulta limitado encontrar policías especializados en informática para determinar en un Parte Policial o en un Atestado Policial, la comisión de un delito informático, seguidamente en la instrucción de un proceso penal, a fin de determinar de manera científica, si ha existido un perjuicio. El Estado debe agotar los medios menos lesivos que el Derecho Penal otorga, antes de acudir a éste. Sólo a través de una regulación previa a la penal que determine qué es lo debido y lo indebido en la red todo con el fin de preservar los intereses sociales, fomentar la prevención, trabajando multisectorialmente, sobre el rol de la sociedad y del Estado, procurando la protección de ésta.

[31] Peña Labrin, Daniel Ernesto, La Firma Digital, En Revista "El Diplomado", Editada por la Escuela Universitaria de Post Grado de la Facultad de Derecho y Ciencia Política de la Universidad Nacional Federico Villarreal, Lima,2005,Pág.145

CONCLUSIONES

- Esta nueva e impredecible modalidad de crimen no está circunscrita a los sectores menos pudientes de la sociedad, y se ha probado de actuaciones de los "delincuentes de cuello blanco" en las áreas económicas y financieras, por lo que su incursión en los ilícitos informáticos no debería sorprendernos. A la vez son conductas criminógenas de cuello blanco, en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlos.
- Estos avances y su utilización comprenden amplias posibilidades que es necesario delimitar a fin de combatir ciertos excesos que se vienen apreciando. Por lo que ante esta situación, es natural la aparición de renovadas disposiciones penales en salvaguarda de los bienes jurídicos que urgen de protección. los obligados a legislar, tiene la palabra para establecer propuestas que permitan su control y consecuente sanción. Son muchos los casos y pocas las denuncias, y todo ello debido a una falta de regulación adecuada por parte del derecho.
- Este maravilloso mundo virtual, es una contundente realidad, que tiene que ser aprovechada por las sociedades. Pero en la perniciosa criminalidad informática, ejercitada por individuos y grupos sociales que manejan programas de esta índole se aprovechan de omisiones legales y atipicidades lo cual les facilita mantenerse en el limbo de la impunidad, relajando el aporte de la informática a la humanidad. Además ofrecen facilidades para su comisión a los menores de edad.
- Es uno de los derechos constitucionales básicos que gozan los ciudadanos del acceso al conocimiento de la información. Sabemos que el Estado se esfuerza para que esta información llegue a quien la solicite,

esto aún resulta insuficiente, pues cotidianamente somos espectadores y a veces protagonistas disconformes, de cómo se administran estos servicios por lo que su manejo oficial no es satisfactorio para la colectividad, lo que deja mucho que desear, por el sentimiento generalizado que exige.

- Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico. Estos adelantos informáticos agilizan la comunicación y el conocimiento, pero también ha permitido que emerjan conductas antisociales y delictivas que atentan contra los méritos del adelanto científico, pensado y fabricado para dotar a la humanidad de lo necesario para su eficaz desarrollo.
- Al Internet se le define como información, tecnología y una red física de telecomunicación, para que cualquier persona se integre a este mundo virtual, necesitando para ello una computadora conectada al ciberespacio y sirve para trabajos legales o para el desenvolvimiento cultural en sentido positivo, pues también se encuentra por desgracia, proxenetismo, de infanto prostitución, meretricio masculino y femenino, pornografía, promiscuidad, juegos compulsivos, dudoso turismo, propaganda de tóxicos no permitidos que alientan la drogadicción, etc. Todas conductas antisociales o delictivas que se dejan pasar ante la carencia de una regulación jurídica. Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Presentan grandes dificultades de comprobación, esto por su mismo carácter técnico. Por el momento siguen siendo ilícitos impunes por la falta de denuncias.

REFERENCIAS

Blossiers Hüme, Juan José. 2005. "*Criminología & Victimología"*, Editorial Disartgraf, Lima.

Marchena Gómez, Juan. 1992. "*Prevención de la Delincuencia Tecnológica"*, Editorial Lima, Lima.

Mir Puig, Santiago. 1996. "*Derecho Penal"*. Parte General, Editorial PPU, Barcelona.

Código Penal Peruano. 2007. Edit. Jurista Editores, Lima, Pág. 188.

Bramont-Arias Torres, Luis Alberto. 2000. "*El Delito Informático en el Código Penal Peruano"*. Edit. Biblioteca de Derecho Contemporáneo, Volumen VI, Pontificia Universidad Católica del Perú. Lima. Pág. 72.

Reyna Alfaro, Luis Miguel, 2002. "*Los Delitos Informáticos, Aspectos Criminológicos, Dogmáticos y de Política Criminal"*, Editorial Jurista. Lima.

Código Penal Peruano. 2007. Pág. 189.

Reyna Alfaro, Luis Miguel. 2002. "*Los Delitos Informáticos, Aspectos Criminológicos, Dogmáticos y de Política Criminal"*, Edit. Jurista. Lima. Pág. 278.

Peña Labrin, Daniel Ernesto. 2005. "*La Firma Digital",* En Revista "El Diplomado", Editada por la Escuela Universitaria de Post Grado de la Facultad de Derecho y Ciencia Política de la Universidad Nacional Federico Villarreal, Lima. Pág.145.