UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y SISTEMAS

LA DESPROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS, EXPUESTOS A CÓDIGO MALICIOSO Y SU INCIDENCIA EN LA VULNERACIÓN AL DERECHO A LA INTIMIDAD

TESIS

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN CIENCIAS CON MENCIÓN EN INGENIERÍA DE SISTEMAS

ELABORADO POR

JORGE LUIS ABANTO GARNIQUE

ASESOR

Mg. ALFREDO RAMOS MUÑOZ

LIMA-PERÚ

2012

A mis queridos padres que
contribuyeron y abrigaron el deseo
de verme en el camino de la superación.

ÍNDICE

CAPÍTULO II

MARCO TEÓRICO Y CONCEPTUAL

RESUMEN

Nuestra investigación, gira en torno a uno de los derechos constitucionales, más relevantes como es el derecho a la intimidad, que está integrado por dos aspectos: el primero correspondería al derecho que tiene todo ser humano a disponer de momentos de soledad, recogimiento y quietud que le permitan replegarse sobre sí mismo, meditar, orar, abrirse a la contemplación tanto exterior como interior; el segundo aspecto se traduciría en el derecho de mantener fuera del conocimiento ajeno hechos o actos que pertenecen a lo privado de una persona.

Al analizar los elementos que integran el concepto del derecho a la vida privada, encontramos que no solo se trata del control de la información de hechos reservados de nuestra vida, sino también de los derechos a la tranquilidad, a la paz, a la soledad, a que ninguna persona se inmiscuya o fisgonee, respecto a los actos de la vida privada.

En este contexto, es conveniente destacar, la presencia en estos últimos años de un accionar ilícito a través, en el mundo informático, donde los cibernautas se ven expuestos a un conjunto de amenazas informáticas, que pueden atentar contra su información, en este caso datos de alta relevancia y trascendencia como son los que pertenecen a la vida privada.

Si bien es cierto hay una legislación sancionatoria, por haberse vulnerado el bien jurídico protegido denominado Intimidad de las Personas, puesto que se utilizan elementos informáticos para vulnerar y acceder a la información contenida en los sistemas informáticos de la víctima, violando de esta forma la intimidad de la misma, pero no es suficiente, en la actualidad hay una

realidad que no se puede ignorar que es la desprotección de los datos personales de los cibernautas peruanos, expuestos al código malicioso y la vulneración al derecho a la intimidad.

ABSTRACT

Our investigation, tour concerning one of the constitutional, more relevant laws since it is the right to the intimacy, which is integrated by two aspects: the first one would correspond to the right that every human being has to have moments of loneliness, concentration and quietude that allow him to be folded on yes same, to ponder, to pray, to be opened for the contemplation so much exterior as interior; the second aspect would be translated in the right to support out of the foreign knowledge facts or acts that belong to deprived of a person.

On having analyzed the elements that integrate the concept of the right to the private life, we think that not only it is a question of the control of the information of facts reserved of our life, but also of the rights for the tranquility, for the peace, for the loneliness, to which no person interferes or pries, respect to the acts of the private life.

In this context, it is suitable to stand out, the presence in the latter years of one to gesticulate illicitly to slant, in the IT world, where the cybernauts meet exposed to a set of IT threats, which can commit an outrage against his information, in this case information of high relevancy and transcendency since they are those who belong to the private life.

Though it is true there is a legislation punitive, for there having been damaged the juridical protected good named Intimacy of the Persons, since IT elements are in use for damaging and acceding to the information contained in the IT systems of the victim, violating of this form the intimacy of

the same one, but it is not sufficient, at present there is a reality that cannot ignore that it is the vulnerability of the personal information of the Peruvian cybernauts, exposed to the malicious code and the violation to the right to the intimacy.

PALABRAS CLAVES

Derechos constitucionales, Derecho a la vida privada, Datos personales, Cibernautas peruanos, Código Malicioso, Delitos Informáticos.

INTRODUCCIÓN

La mayor parte de los derechos a la integridad son absolutos, en el sentido de que no pueden anularse. La libertad de acción, en cambio, puede en alguna medida estar limitada, para proteger los derechos de los demás. Por ejemplo, la libertad de expresión puede restringirse para impedir los discursos que inciten al odio, otro donde por ejercer el derecho a la libertad de expresión, el periodismo invade la privacidad de las personas, de su ámbito familiar, sin tener ningún tipo de limite.

Las normas reconocen derechos, y en esos casos, estos derechos parecerían ser contradictorios o incompatibles. En el caso del aborto, el derecho a la vida del niño y el derecho a la privacidad y libertad de la madre.

En el consumo de drogas, el derecho a la libertad y privacidad del drogadicto y el derecho a la salud pública y seguridad de la población. En la pornografía, el derecho a la libertad de expresión y privacidad, frente al derecho a la moral pública, a la defensa de la familia, a la sana educación de los niños y jóvenes. En los noticieros, el derecho a la libertad de expresión frente al derecho al honor y la intimidad.

Nuestra constitución señala en el artículo 2, que toda persona tiene derecho: (...) 7. Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviadas en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y

proporcional, son perjuicio de las responsabilidades de ley. *De allí la relevancia que* todos los seres humanos tenemos una vida "privada" conformada por aquella parte de nuestra vida que no está consagrada a una actividad pública y que por lo mismo no está destinada a trascender e impactar a la sociedad de manera directa y en donde en principio los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia, ni les afecta.

Lamentablemente en estos últimos años el derecho a la intimidad, ha perdido su vigencia, solidez y respeto por nuestra sociedad, somos testigos de las constantes violaciones a la intimidad de las personas, creando un clima de impunidad, que no impide que se siga vulnerando tan preciado derecho.

Así mismo con el avance de la tecnología y la informática, esta se vuelto indispensable en nuestro vida, es parte de nosotros, y por lo tanto se utiliza en todos los ámbitos. El impacto de la Internet en el mudo entero ha sido realmente arrollador, de una u otra forma todos hablan de Internet, recurren a ella y/o realizan negocios en línea. Siendo este último un importante punto de partida para el estruendoso desarrollo de un nuevo mercado. Desde el momento en que empezamos a navegar en Internet, cada clic del ratón va dejando una serie de pistas que hacen que todos nuestros movimientos queden reflejados. La actual revolución tecnológica y la "autopista de la información" han facilitado muchos medios que ponen en peligro el derecho a la intimidad. De allí la importancia de nuestra investigación.

El capitulo I, que trata del PLANTEAMIENTO DEL PROBLEMA, nos introduce a nuestra problemática como la presencia constante de vulneraciones al derecho a la intimidad, por la desprotección de los datos personales de los cibernautas peruanos, expuestos a código malicioso. En el capitulo II, presentamos el MARCO TEÓRICO, donde resaltamos primero los antecedentes del problema, para conocer después las bases teóricas de nuestra investigación. El capitulo III, sobre el cuerpo de tesis, donde desarrollaremos nuestra investigación, donde se vera los resultados y el

análisis de las encuestas realizadas. Y por último presentaremos las conclusiones y recomendaciones.

CAPITULO I

PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1. DIAGNÓSTICO Y ENUNCIADO DEL PROBLEMA.

El derecho a la vida privada está reconocido por el Código Civil de 1984, fundamentalmente en el artículo 14, pero ha sido tratado solo parcialmente, sin haberse considerado todos los elementos conceptuales que lo integran y que la doctrina los desarrolla ampliamente. En efecto, al analizar los elementos que integran el concepto del derecho a la vida privada, encontramos que no solo se trata del control de la información de hechos reservados de nuestra vida, sino también de los derechos a la tranquilidad, a la paz, a la soledad, a que ninguna persona se inmiscuya o fisgonee, respecto a los actos de la vida privada. Pero además de estos aspectos negativos relacionado con acciones de terceros, existe un contenido positivo y que constituye la garantía de la libertad de las personas, aspecto denominado autonomía, entendido como la posibilidad de tomar por sí mismo las decisiones más importantes de su existencia.

El artículo 14 acoge solo uno de los elementos, el control de la información, estableciendo que" la intimidad de la vida personal y familiar no puede ser puesta de manifiesto sin el asentimiento de la persona o si ésta ha muerto, sin el de su cónyuge, descendientes,

ascendientes o hermanos, excluyentemente y en este orden". La redacción es limitativa, no comprendiendo el aspecto de la reserva a que tiene derecho la persona y que le permite la paz y la tranquilidad para su desarrollo psíquico equilibrado, así como tampoco se vislumbra el desarrollo positivo que garantice la libertad de la persona y, mucho menos, el problema latente que implica la informática en relación a los datos de la vida privada que pueden ser compilados y organizados.

Una interpretación estricta del artículo en comentario nos circunscribiría, única y exclusivamente, a controlar la posible divulgación de un hecho de la vida privada. Pero, *¿si una persona o el Estado fisgonean, vigila, observa, inmiscuyéndose en la vida privada del cibernauta, y divulga los hechos, estaría atentando contra el derecho a la vida privada?* Es necesario recurrir a una interpretación extensiva y comprender dentro de sus alcances este aspecto de la tranquilidad que forma parte del derecho a la vida privada.

Evidentemente, el legislador ha puesto el acento en el aspecto que hasta hace dos décadas era el más peligroso, es decir, el conflicto con la información, en lo que se refiere al aspecto de brindarla y, específicamente, en relación con los medios de comunicación masiva.

La vida privada no puede ser puesta de manifiesto, no puede ser objeto de información, de divulgación, sin que existan razones y es que el derecho a la vida privada no tiene un carácter absoluto.

Como señalamos al inicio, en estos últimos años el derecho a la intimidad, ha perdido su vigencia, solidez y respeto por nuestra sociedad, somos testigos de las constantes violaciones a la intimidad de las personas, creando un clima de impunidad, que no impide que se siga vulnerando tan preciado derecho.

La intimidad se encuentra protegido en diversas fuentes de nuestro ordenamiento jurídico y que al igual que los demás valores fundamentales, no es un derecho absoluto. Así diversos autores manifiestan que la protección de la intimidad deriva del derecho al

honor (que incluye tanto la mayor o menor estima que los terceros tengan de una persona, como la mejor o peor imagen que pueda tener ella de sí misma). Así visto, las intromisiones que deberían ser castigadas serían aquellas que sólo causen perjuicio a esta estima e imagen. Postura que ha sido criticada, "por considerar que no sólo le niega autonomía a la situación jurídica que protege la intimidad, que es una proyección primordial del ser humano, sino que dejaría desprotegido a éste de todas aquellas intromisiones que sin ser difamantes o injuriosas atentan contra la intimidad del ser humano."

Al igual que el resto de valores fundamentales, la privacidad no es un derecho absoluto e irrestricto.

En este contexto, el Internet tiene un conjunto de características impresionantes. Es instantáneo, inmediato, mundial, descentralizado, interactivo, capaz de extender ilimitadamente sus contenidos y su alcance, flexible y adaptable en grado notable. Es igualitario, en el sentido de que cualquiera, con el equipo necesario y modestos conocimientos técnicos, puede ser una presencia activa en el ciberespacio, anunciar su mensaje al mundo y pedir ser oído. Permite a las personas permanecer en el anonimato, desempeñar un papel, fantasear y también entrar en contacto con otros y compartir. Según los gustos del usuario, se presta igualmente a una participación activa o a una absorción pasiva en « un mundo narcisista y aislado, con efectos casi narcóticos ». Puede emplearse para romper el aislamiento de personas y grupos o, al contrario, para profundizarlo.

La configuración tecnológica que implica Internet tiene una importante relación con sus aspectos éticos: la gente ha tendido a usarlo según como se había proyectado, y a proyectarlo para adaptar este tipo de uso. De hecho, este « nuevo » sistema se remonta a la década de 1960, los años de la guerra fría; fue concebido para frustrar un ataque nuclear, creando una red descentralizada de ordenadores que almacenaban datos vitales. La descentralización fue la clave del

esquema, puesto que de este modo —ese fue el razonamiento—, la pérdida de uno o incluso muchos ordenadores no causaría la pérdida de los datos.

La explosión de la tecnología de la información ha incrementado la capacidad de comunicación de algunas personas y grupos favorecidos durante mucho tiempo. Internet puede servir a la gente en su ejercicio responsable de la libertad y la democracia, ampliar la gama de opciones realizables en diversas esferas de la vida, ensanchar los horizontes educativos y culturales, superar las divisiones y promover el desarrollo humano de múltiples modos. « El libre aluvión de imágenes y palabras a escala mundial no sólo está transformando las relaciones entre los pueblos a nivel político y económico, sino también la misma comprensión del mundo. Este fenómeno ofrece múltiples potencialidades, en otro tiempo impensables ». Cuando se basa en valores compartidos arraigados en la naturaleza de la persona, el diálogo intercultural facilitado por Internet y demás medios de comunicación social puede ser « un instrumento privilegiado para construir la civilización del amor ».

Con el avance vertiginoso de la tecnología e informática que implica la posibilidad de obtener información así como de difundirla también se advierte el peligro de ciertos aspectos existenciales o de la personalidad humana generados por el avance de la tecnología de la información como es la intimidad personal; dado que cuando los actos del ser humano, sus convicciones, opiniones, creencias son captados, almacenados y ordenados mediante las computadoras u ordenadores, la libertad de éste disminuye al ser capturado como un elemento más de la sociedad de la información; haciéndolo carecer de individualidad e identidad personal; y es que la actual revolución tecnológica y la "autopista de la información" han facilitado muchos medios que ponen en peligro esta gama de derechos ligados al desarrollo en sociedad de la persona. De allí la necesidad de contar con un derecho que regule la libertad de información como factor indispensable para el desarrollo del individuo y la sociedad y que manifieste sus límites para defender los

márgenes de la intimidad necesarios para el normal desarrollo de la personalidad humana.

A medida que más personas empiecen a usar la red y comience el auge del comercio electrónico, nuestras navegaciones por la red dejaran rastros cada vez más visibles, porque hay que aceptar que la tecnología avanza a una velocidad vertiginosa y por tanto, las cookies podrían ser desplazadas por sistemas más sutiles y eficaces de capturar información.

La tecnología que acecha nuestra intimidad podría ofrecernos soluciones mediante la criptografía, también podría ofrecernos programas que permitan nuestro anonimato o nuevos protocolos de comunicación que nos permitan dirigir a quiénes entregamos información y dosificarla verdaderamente. Pero, esta alternativa que a primera vista parece la más adecuada y fácil ofrece problemas. El primero es que seguramente los que comercian con la información serán los primeros interesados en vender ese software a precios poco accesibles lo cual degenerará en unos pocos afortunados que puedan pagar por su privacidad. Si lo ofreciesen gratuitamente podrían pedir igualmente nuestros nombres para la licencia de uso (lo cual ocurre en cualquier utilitario al cual hagamos un download).

Otra alternativa que nos ofrece la informática es la que Pérez Luño nos advierte respecto a los "Ficheros Robinson". De acuerdo con Pérez Luño, el mismo nombre ya indica un juicio de valor. Quiere sugerirnos la idea que el ciudadano normal acepta sin ningún problema que su vida privada sea contaminada

" (...) por los intereses consumistas de los mercaderes de la publicidad. El ciudadano insólito será aquél que se obstine en salvaguardar su derecho fundamental a la intimidad y se autoconfina en un aislamiento parangonable al sufrido por Robinson en su isla solitaria. Podría objetarse a este torpe mensaje ideológico subliminal que precisamente

son las sociedades tecnológicas del presente las que han dado origen al fenómeno de las "muchedumbres solitarias" de seres gregarios, espectadores inertes y manipulados por y desde mil formas de propaganda. Todavía es más importante aducir que en un Estado de Derecho ningún ciudadano debe verse obligado a inscribirse en un archivo adicional de datos para que sean respetados sus derechos y libertades. Parecería grotesco que, en una sociedad democrática, el respeto de la dignidad, de la libertad personal o de conciencia, o el secreto de las comunicaciones quedara limitado a aquellos ciudadanos que expresamente lo solicitaren".

No podría confiarse en que las propias empresas renuncien a invadir la privacidad e intimidad de las personas, menos aún que la tecnología se inhiba de crear nuevos mecanismos de captura de información, toda ayuda que ofrezca la tecnología es bienvenida sin duda alguna, pero se necesita la intervención del derecho a fin de garantizar los derechos fundamentales de cada ciudadano.

Debido a ésta situación es por lo que se ha generado el surgimiento de un nuevo derecho a la libertad informática que implica tanto el derecho del individuo a negarse a brindar información sobre si mismo y el derecho a pretender información concernida a su persona o personalidad; en suma controlar la identidad personal informática a través del consentimiento para preservar, acceder, o rectificar datos informativos referidos a la vida privada de las persona, es decir el derecho a la "autodeterminación informativa", que (como derivado que es de los derechos de privacidad y a la libertad personal), participa de su naturaleza de derecho fundamental.

Uno de los elementos que vulneran la intimidad personal los llamados "cookies", en un principio, son ficheros no perjudiciales ya que sirven para evitar la sobrecarga de los servidores en diversas funciones de uso cotidiano, como pudiera ser la consulta de un correo Web o utilizar los servicios de un buscador. Sin embargo, existen algunos sites que

desarrollan otro tipo de "cookies", que están diseñadas para obtener información del usuario sin que éste sea consciente de ello y por supuesto, sin su consentimiento.

Todos los navegadores permiten deshabilitar las "cookies", pero con ello, muchas de las actividades que normalmente realizamos, tales como utilizar un correo Web, se ven mermadas, con lo cual muchos cibernautas optan por no dar importancia a los posibles datos que las "cookies maliciosas" extraen de su ordenador.

Los "cookies" permiten la obtención de información de datos del usuario para el administrador de un servidor y para los departamentos de marketing de las empresas que tienen una página web en Internet, al obtener información de esta manera, pueden vulnerar el derecho a la intimidad y afectar la información sensible que es intrínseco únicamente a la propia persona que navega en el ciberespacio, se podría decir que si no existe consentimiento por parte de los cibernautas, toda captura de información por intermedio de las cookies seria contrario al ordenamiento jurídico y por lo tanto ilegal, puesto que los datos identifican a un determinado cibernauta que no brindó su consentimiento por estar registrado en bancos de datos que no autorizó.

Nuestra doctrina nacional aún es rudimentaria, pues ésta solo se ha limitado a entender a la intimidad como un derecho a no revelar a los demás determinados aspectos de sus relaciones con otras personas, haciendo uso de la autodeterminación informativa; y en donde la información objeto de mayor reserva ha sido considerada por la doctrina nacional como datos sensibles.

Respecto al consentimiento que debe brindar el cibernauta en la red informática, se debe establecer que el consentimiento expreso y escrito motivo por el cual los sitios Web que registren usuarios deberán tener la posibilidad de que el usuario otorgue su consentimiento inequívoco

en forma previa a realizar su registró, aceptando las condiciones de la misma. Los sitios que no realizan registro pero que captan datos deberán dejar claro cuales son las condiciones de uso del sitio a través de algún vínculo, para que el cibernauta esté informado de los datos que recabarán.

ENUNCIADO DEL PROBLEMA

LA DESPROTECCION DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS, EXPUESTOS A CÒDIGO MALICIOSO Y LA VULNERACIÓN AL DERECHO A LA INTIMIDAD.

1.2. DEFINICIÓN DEL PROBLEMA.

¿EN QUE MEDIDA LA DESPROTECCION DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS, EXPUESTOS A CÒDIGO MALICIOSO, INCIDE EN LA VULNERACIÓN AL DERECHO A LA INTIMIDAD?

1.3. FORMULACION DE LOS OBJETIVOS DE LA INVESTIGACIÓN.

1.3.1. OBJETIVOS GENERAL.

DETERMINAR EN QUE MEDIDA LA DESPROTECCION DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS, EXPUESTOS A CÓDIGO MALICIOSO, INCIDE EN LA VULNERACIÓN AL DERECHO A LA INTIMIDAD.

1.3.2. OBJETIVOS ESPECIFICOS.

OBJETIVOS ESPECIFICOS 1.

Evaluar de qué manera, la vulnerabilidad de los sistemas de información de la administración pública, aumenta los riesgos que afectan la infraestructura tecnológica y la integridad, confidencialidad y disponibilidad de la información de las entidades gubernamentales.

OBJETIVOS ESPECIFICOS 2.

Estudiar a qué se debe que los entes encargados de sancionar a quienes hacen uso ilegal y delictivo de las herramientas informáticas, no tengan cómo judicializar a las nuevos modalidades en contra de los cibernautas.

OBJETIVOS ESPECIFICOS 3.

Precisar los procedimientos y políticas de seguridad de la información; que utiliza el estado y, en consecuencia, determinar cuales son las acciones penales que pueden adelantar contra las personas que incurran en las conductas que vulneren el derecho a la intimidad.

1.4. HIPÓTESIS DE LA INVESTIGACIÓN.

1.4.1. HIPÓTESIS.

1.4.1.1. HIPÓTESIS GENERAL.

SI SE VIENE DANDO UNA DESPROTECCION DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS, EXPUESTOS A CÒDIGO MALICIOSO ENTONCES NO SE

EVITARA LA VULNERACIÓN DE LA INTIMIDAD DE LAS PERSONAS.

1.4.1.2. HIPÓTESIS ESPECÍFICAS.

Hipótesis 1

La vulnerabilidad de los sistemas de información de la administración publica, por la falta de una legislación eficaz, aumenta los riesgos que afectan la infraestructura tecnológica y la integridad, confiabilidad y disponibilidad de la información de las entidades gubernamentales.

Hipótesis 2

Mientras los entes encargados de sancionar a quienes hacen uso ilegal y delictivo de las herramientas informáticas, no tengan cómo judicializar a las nuevos modalidades en contra de los cibernautas, se seguirá vulnerando el derecho a la intimidad.

Hipótesis 3

A una aplicación efectiva de procedimientos y políticas de seguridad de la información; que utiliza el estado, se podrá determinar las acciones penales contra las personas que incurran en las conductas que vulneren el derecho a la intimidad.

1.4.2. IDENTIFICACIÓN Y OPERACIONALIZACIÓN DE VARIABLES.

VI: DESPROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS.

INDICADORES

Inseguridad.

Datos vulnerables.

Cibernautas afectados.

VD: VULNERACIÓN DE LA INTIMIDAD DE LAS PERSONAS.

INDICADORES

Derechos fundamentales.

Intimidad de las personas.

Afectación a la intimidad.

VI: CÓDIGO MALICIOSO.

INDICADORES

Vulnerabilidad

Sistemas de información

Procedimientos de seguridad.

1.5. MATRIZ DE CONSISTENCIA

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES
Problema principal	**Objetivo principal**	**Hipótesis principal**	**Operacionalización de variables**	
¿En qué medida la desprotección de los datos personales de los cibernautas peruanos, expuestos a código malicioso, incide en la vulneración al derecho a la intimidad?	Determinar en qué medida la desprotección de los datos personales de los cibernautas peruanos, expuestos a código malicioso, incide en la vulneración al derecho a la intimidad.	Si se viene dando una desprotección de los datos personales de los cibernautas peruanos, expuestos a código malicioso, entonces no se evitará la vulneración al derecho a la intimidad.	VI. Desprotección de los datos personales de los cibernautas peruanos. VD: Vulneración al derecho a la intimidad. VI: Código malicioso.	Inseguridad. Datos vulnerables. Cibernautas afectados. Derechos fundamentales. Intimidad de las personas. Afectación a la intimidad. Vulnerabilidad Sistemas de información Procedimientos de seguridad.
Problemas secundarios	**Objetivos secundarios**	**Hipótesis secundarias**	**Operacionalización de variables**	
P.S. 1. ¿De qué manera, la vulnerabilidad de los sistemas de información de la administración pública, aumenta los riesgos que afectan la infraestructura tecnológica y la integridad, confiabilidad y disponibilidad de la información de las entidades gubernamentales? P.S. 2. ¿ A que se debe que los entes encargados de sancionar a quienes hacen uso ilegal y delictivo de las herramientas informáticas, no tengan cómo	O. E. 1. Evaluar de que manera, la vulnerabilidad de los sistemas de información de la administración pública, aumenta los riesgos que afectan la infraestructura tecnológica y la integridad, confiabilidad y disponibilidad de la información de las entidades gubernamentales. O. E. 2. Estudiar a que se debe que los entes encargados de sancionar a quienes hacen uso ilegal y delictivo de las herramientas informáticas,	H. 1La vulnerabilidad de los sistemas de información de la administración pública, por la falta de una legislación eficaz, aumenta los riesgos que afectan la infraestructura tecnológica y la integridad, confiabilidad y disponibilidad de la información de las entidades gubernamentales. H. 2 Mientras los entes encargados de sancionar a quienes hacen uso ilegal y delictivo de las herramientas informáticas, no tengan cómo judicializar a las	VI. Vulnerabilidades de los sistemas de información de la administración pública. VD: Infraestructura tecnológica y la integridad, confiabilidad y disponibilidad de la información de las entidades gubernamentales. VI. Entes encargados de sancionar VD. Judicializar a las nuevos modalidades en	Vulnerabilidades "Cero Day" Actualización de Sistemas Operativos Botnets Poder judicial. Ministerio Público. Proceso penal. Delitos tipificados.

judicializar a las nuevos modalidades en contra de los cibernautas?	no tengan cómo judicializar a las nuevos modalidades en contra de los cibernautas.	nuevos modalidades en contra de los cibernautas, se seguirá vulnerando el derecho a la intimidad.	contra de los cibernautas.	
P.S. 3. ¿A Cuales son los procedimientos y políticas de seguridad de la información; que utiliza el estado y, en consecuencia, determinar cuales son las acciones penales que pueden adelantar contra las personas que incurran en las conductas que vulneren el derecho a la intimidad?	O. E. 3. Precisar cuales son los procedimientos y políticas de seguridad de la información; que utiliza el estado y, en consecuencia, determinar cuales son las acciones penales que pueden adelantar contra las personas que incurran en las conductas que vulneren el derecho a la intimidad	H. 3 A una aplicación efectiva de procedimientos y políticas de seguridad de la información; que utiliza el estado y, se podrá determinar las acciones penales contra las personas que incurran en las conductas que vulneren el derecho a la intimidad.	VD: Aplicación efectiva de procedimientos y políticas de seguridad de la información VI: Acciones penales contra las personas que incurran en las conductas que vulneren el derecho a la intimidad	Seguridad Informática. Protección de Identidad Política gubernamental Sistema penal. Sanción penal.

1.6. JUSTIFICACIÓN Y DELIMITACIÓN DE LA INVESTIGACIÓN.

1.5.1. IMPORTANCIA.

Así como la tecnología y su desarrollo han incidido en prácticamente todas las actividades del ser humano a lo largo de su historia, en la actualidad, la dependencia tecnológica ha venido concentrándose cada vez más en el fenómeno de la tecnología informática, la información y la comunicación. Con efecto retardado, se descubrió luego que ese desarrollo venía acompañado de distintos y también novedosos riesgos.

La legislación peruana debe implementar normas que garanticen un niveladecuado de protección respecto a los datos personales de los cibernautas, en tal sentido esta investigación será insumo a nuevas investigaciones que busquen minimizar el riesgo del compromiso de los datos de los cibernautas en sus tres entornos de relación: personal-social-familiar, laboral y gubernamental.

1.5.2. JUSTIFICACIÓN

El presente proyecto de investigación, tiene carácter descriptivo y evaluativo, pues busca describir y caracterizar factores y procedimientos; por otro lado se aplicarán análisis de documentos y encuestas en una población de aproximada de 120 profesionales; lo que permitirá conocer de cerca la realidad problemática desde diferentes enfoques, que finalmente contribuyan a identificar que la desprotección de datos de las personas, se está convirtiendo en el eslabón más débil asociado a la seguridad de la información, donde para este enfoque inicialmente se vulnera el derecho a la intimidad,

sin embargo las consecuencias posteriores existen, las cuales podrían ser materia de otra investigación.

1.5.3. DELIMITACION

DELIMITACIÓN ESPACIAL.

Esta investigación se realizara en la ciudad de Lima en razón de que fue en esta capital en la que se concentró el mayor porcentaje de casos y por la naturaleza del procedimiento.

DELIMITACIÓN TEMPORAL:

Son los problemas que se ven en la actualidad, por ello nos llevará al estudio de casos de los años 2009, 2010 y 2011, principalmente.

DELIMITACIÓN SOCIAL:

El cibernauta peruano que aborda esta investigación se circunscribe a la capital del Perú, considerando el grupo académico en general, así como profesional público y privado.

CAPITULO II
MARCO TEÓRICO

2.1. TRABAJOS PREVIOS.

Claudia Isabel Campos Motta, (2010) de la Universidad Tecnológica del Perú en la tesis titulada *vulneración del derecho a la intimidad, por la carencia de lineamientos, en la responsabilidad penal y obtención de medios probatorios en el proceso penal*, concluye que en la medida de que los derechos fundamentales no son absolutos sino relativos, según la Corte Interamericana de Derechos Humanos y el Tribunal Constitucional, la policía puede limitarlos o restringirlos en su ejercicio, modo o tiempo, pero de manera razonable y proporcional, cuando realice detenciones, tareas de control de identidad, vídeo-vigilancia, pesquisas –de lugares, cosas o personas–, retenciones, intervenciones corporales o allanamientos de moradas, entre otras intervenciones. Para ello, la policía debe: i) obtener los medios probatorios de conformidad con la finalidad legítima de su tarea de investigación, ii) establecer la necesidad de obtener las pruebas de la forma señalada, en la medida de que no existan otras posibilidades que sean eficaces y legítimas, y iii) asegurar la mínima afectación de los derechos fundamentales aludidos.

Jorge Ojeda Pérez (2010) de la Universidad Tecnológica del Perú en la Universidad Santo Tomás de Aquino, USTA. en la tesis titulada *Delitos informáticos y entorno jurídico vigente en Colombia, donde concluye* normatividad sobre el cibercrimen, que ha venido vulnerando distintos campos de las relaciones y comunicaciones personales, empresariales e institucionales. El ciberdelito, como tendencia que incide no sólo en el campo tecnológico sino también en el económico, político y social, debe ser conocido, evaluado y enfrentado, por lo cual el análisis de la norma, su aporte y alcance puede dar otros elementos de juicio para entender la realidad de nuestras organizaciones y visualizar sus políticas y estrategias, a la luz de la misma norma y de los estándares mundiales sobre seguridad informática.

2.2. MARCO TEÓRICO.

2.2.1. LA DESPROTECCION DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS

2.2.1.1. Internet

Entendemos por Internet, una interconexión de redes informáticas que le permite a las computadoras conectadas comunicarse directamente entre sí. Esta palabra suele referirse a una interconexión en particular, abierta al público la cual es capaz de conectar tanto a organismos oficiales como educativos y empresariales; la definición de Internet admite que se la conoce vulgarmente con el nombre de "autopista de la información" debido a que es una "ruta" en donde podemos encontrar casi todo lo que buscamos en diferentes formatos[1].

[1]DEFINICIÓN DE INTERNET: una red global. Recuperado el 28 de Abril del 2012 en http://www.abcpedia.com/diccionario/definicion-internet.html

Internet posee un funcionamiento que puede resultar bastante complejo para aquellos que no estén familiarizados con la informática; ésta es un conjunto de redes locales que están conectadas entre sí a través de una computadora especial por cada red. Dichas interconexiones se llevan a cabo utilizando varias vías de comunicación, entre ellas podemos mencionar a las líneas de teléfono, los enlaces por radio y la fibra óptica; los diferentes tipos de servicios proporcionados emplean diferentes formatos. A uno de ellos se lo conoce como decimal con puntos; otros se encargan de distinguir a la computadora por destinos estableciendo el .es (para España), .com.ar (para Argentina) o el .com.mx (para Mexico).Una vez que la información es direccional, sale de la red de origen a través de la puerta y es encaminada hacia la red local que contiene la máquina de destino[2].

La definición de Internet también habla de los "protocolos"; el que utiliza este espacio virtual es el IP, el mismos es el soporte básico que se utiliza para controlar los ordenadores conectados a la web. También existe el Protocolo de Control de Transmisión (TCP) el cual comprueba si la información ha llegado a la computadora de destino, si esto no ocurrió, la vuelve a enviar.

Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta fue un desarrollo posterior (1990) y utiliza Internet como medio de transmisión[3].

---

[2]Ibidem.
[3]**CASTELLS, M.:** La galaxia Internet – Reflexiones sobre Internet, empresa y sociedad. Barcelona (Plaza &Janés), 2001. p.12

Existen, por tanto, muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia -telefonía (VoIP), televisión (IPTV)-, los boletines electrónicos (NNTP), el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea[4].

El género de la palabra Internet es ambiguo, según el Diccionario de la lengua española de la Real Academia Española[5].

2.2.1.2. La expansión de la Internet

Internet surgió de un proyecto desarrollado en Estados Unidos para apoyar a sus fuerzas militares. Luego de su creación fue utilizado por el gobierno, universidades y otros centros académicos[6].

Internet ha supuesto una revolución sin precedentes en el mundo de la informática y de las comunicaciones. Los inventos del telégrafo, teléfono, radio y ordenador sentaron las bases para esta integración de capacidades nunca antes vivida. Internet es a la vez una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus ordenadores independientemente de su localización geográfica[7].

Desde que la Internet comenzó a expandirse, gran parte de los estudios acerca de ella destacan el porcentaje de usuarios que tiene en cada país y el rezago que significa la gran cantidad de gente

---

[4]Ibidem.
[5]Ibidem.
[6]**FACHA AROCHE**Sthepany*La Historia del Internet* Recuperado el 3 de Abril del 2012 en http://www.maestrosdelweb.com/editorial/internethis/
[7]Ibidem.

marginada del acceso a ella. La brecha digital ha sido reconocida como el reto principal para que la Internet llegue a ser expresión auténtica de la globalización y de las peculiaridades nacionales y regionales que persisten y asumen nuevas formas de expresión. Desde luego, instalar computadoras y conectarlas a la Internet no es suficiente para que la gente se acerque a ellas y las aproveche. Es necesaria una sostenida labor de educación y persuasión para que quienes hasta ahora han estado al margen de la Red puedan y decidan apropiarse de ella. Hoy en día se han reconocido manifestaciones más complejas de la brecha digital que ya no es solamente la disparidad entre quienes tienen y quienes no cuentan con acceso a la Internet"[8]

Nuestras sociedades están cambiando debido a la introducción del Internet, redes sociales cambian la forma de interactuar con personas y sobre cómo conocer a nuevas personas. Sitios como plentyoffish.com han cambiado la percepción acerca de citas en países norteamericanos y europeas, y probablemente habrán sitios en habla hispana que cambiarán la forma en que interactuamos con las personas[9].

La cuestión no es sí es importante o no, es que tan importante puede llegar a ser y hasta donde permitirá el ser humano que reemplace las relaciones humanas físicas por las cibernéticas. Creo que estamos muy abiertos a un cambio. La privacidad juega un papel muy importante en la disponibilidad que tienen las personas a utilizar el Internet. Ya no es necesario sentir vergüenza en realizar una pregunta o tratar de conocer a una persona no implica sentirnos tímidos al respecto[10].

---

[8]**CASTELLS, M.** Ob Cit. p. 9
[9]**ROMERO** Daniel *Importancia del Internet en nuestra sociedad*Recuperado el 2 de Abril del 2012 en http://www.area123.com/2009/01/importancia-del-internet-en-nuestra-sociedad/
[10]Ibidem.

Sobre Internet y sociedad, es pertinente pronunciarnos, Internet tiene un impacto profundo en el mundo laboral, el ocio y el conocimiento a nivel mundial. Gracias a la web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea. Un ejemplo de esto es el desarrollo y la distribución de colaboración del software de Free/Libre/Open-Source (FLOSS) por ejemplo GNU, Linux, Mozilla y OpenOffice.org[11].

Comparado a las enciclopedias y a las bibliotecas tradicionales, la web ha permitido una descentralización repentina y extrema de la información y de los datos. Algunas compañías e individuos han adoptado el uso de los weblogs, que se utilizan en gran parte como diarios actualizables. Algunas organizaciones comerciales animan a su personal para incorporar sus áreas de especialización en sus sitios, con la esperanza de que impresionen a los visitantes con conocimiento experto e información libre[12].

Internet ha llegado a gran parte de los hogares y de las empresas de los países ricos. En este aspecto se ha abierto una brecha digital con los países pobres, en los cuales la penetración de Internet y las nuevas tecnologías es muy limitada para las personas; no obstante, en el transcurso del tiempo se ha venido extendiendo el acceso a Internet en casi todas las regiones del mundo, de modo que es relativamente sencillo encontrar por lo menos 2 computadoras conectadas en regiones remotas[13].

Desde una perspectiva cultural del conocimiento, Internet ha sido una ventaja y una responsabilidad. Para la gente que está interesada en otras culturas, la red de redes proporciona una cantidad significativa

---

[11]**METZNER-SZIGETH**, A.: "El movimiento y la matriz" – Internet y transformación socio-cultural. En: Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación (CTS+I), No. 7, 2006. p.38

[12]Ibidem.

[13]Ibidem.

de información y de una interactividad que sería inasequible de otra manera. Internet entró como una herramienta de globalización, poniendo fin al aislamiento de culturas. Debido a su rápida masificación e incorporación en la vida del ser humano, el espacio virtual es actualizado constantemente de información, fidedigna o irrelevante[14].

2.2.1.3. Informática e información.

Actualmente, la riqueza es constituida por la sistematización de la información[15], la cual empieza a tener valor económico y tener grandes consecuencias sobre las comunicaciones, el trabajo y la vida diaria en general. Uno de los aspectos más relevantes de esta etapa es la aparición de la Internet, la cual permite acceder a través de una computadora a sitios remotos que en vida tal vez nunca podríamos visitar; asimismo permite relacionarse con personas cuya lejanía espacial es remplazada por una cercanía virtual. De esta manera, es posible comunicarse con varias personas distantes a la vez y acceder a información remota mediante newsgroup, sin limitaciones. Al respecto Bill Gates comenta: "Cualquier persona puede enviar ya un mensaje a otra, mediante la Internet, tanto para asuntos de negocios como de educación o formación o simplemente por diversión. Los estudiantes de todo el mundo se pueden enviar mensajes. Los presidiarios pueden entablar animadas conversaciones con amigos con los que nunca se podrán reunir.[16]"

Sin embargo, Internet tiene sus riesgos, no siempre sabemos si la persona con quien nos comunicamos es verdaderamente quien dice ser. y mucho menos podemos estar seguros que nuestra relación con la Red sea totalmente inocente, en realidad, podríamos dar más

[14]**METZNER-SZIGETH**, Ob Cit. p. 39
[15]**TOFFLER**,Alvin "La tercera Ola". Madrid: Plaza & Janes. 1994. P.20.
[16]**GATES III**, William H. Camino al futuro. New York: Penguin Books. P. 92

información personal de la que quisiéramos ofrecer. Es algo que caracteriza a estos tiempos modernos, en que los satélites son capaces de fotografiar el interior de nuestras casas, minúsculas cámaras pueden ser introducidas en nuestros cuerpos, o que de un momento a otro una amable señorita, muy al tanto de varios detalles personales, a quien no conocemos nos llame para vendernos un seguro de vida mediante la modalidad del Marketing Directo[17].

"En etapas anteriores el respeto a la vida privada podía realizarse mediante el uso de los sentidos tales como la vista y el oído. Se permanecía así dentro de los límites de las relaciones naturales. Los muros de una casa, la soledad de un lugar desierto, incluso el tono expresivo oral de un susurro, eran suficientes para asegurar la protección de la intimidad y para excluir el conocimiento y la difusión de las acciones y de las palabras de un individuo o de varias personas unidas entre sí por el vínculo de la confidencia. Hoy es posible observar y escuchar a distancia, sin límites de tiempo, de espacio o de modo; se pueden realizar fotografías en la noche, establecer comunicación simultánea de imagen y sonido con distintos lugares gracias a los circuitos televisivos, dejar involuntariamente el testimonio registrado de la propia imagen o de las conversaciones mantenidas e, incluso, se pueden confesar los propios pensamientos sin el uso de la tortura física y casi inadvertidamente"[18].

Estas nuevas situaciones que están convirtiéndose en parte de la cotidianidad del S. XXI merecen una reflexión jurídica y en este capítulo nos dedicaremos a explicar los elementos principales del problema que abordamos; es decir, la proliferación de bases de

---

[17] En "CAMINO AL FUTURO" de Bill Gates aparece un notable dibujo de Peter Steiner que muestra a dos perros, uno de los cuales tecleando sobre la computadora comenta a su compañero: "En internet nadie sabe que eres un perro". Recuperado el 4 de Mayo en http://www.monografias.com/trabajos57/cookies-privacidad-internet/cookies-privacidad-internet2.shtml

[18] **PEREZ LUÑO,** Antonio Enrique. Dilemas actuales de la protección de la intimidad. EN: Ius et Praxis. Universidad de Lima. N° 21-22. 1993. P.19

datos, la aparición de la internet y los cookies, aspecto que motiva este trabajo el cual es sólo uno de los nuevos riesgos que enfrenta el hombre moderno. En el próximo capítulo intentaremos delimitar una noción de intimidad que sirva como herramienta a nuestro trabajo; por ahora, nos dedicaremos a plantear la realidad del fenómeno, a fin de dejar establecido el problema, antes de describir el estado de la cuestión en la doctrina jurídica[19].

Sobre el banco de datos, Pérez Luño advierte que: "Desde los años setenta es notorio que bancos de datos del sector público norteamericano, pertenecientes al Pentágono, la CIA o el FBI, procesan informes sobre actitudes individuales y comportamiento político que afectan a millones de ciudadanos. Datos que recabados en función de la defensa nacional o de la seguridad pública han servido, en determinadas ocasiones, para prácticas de control político y discriminación ideológica. La comunidad académica de USA sufrió una conmoción al saber que, durante la etapa de contestación estudiantil, diversas universidades que contaban con bibliotecas informatizadas proporcionaron a la policía relaciones exhaustivas de las lecturas de aquellos profesores y/o alumnos sospechosos de ser contestatarios o disidentes. Desde hace años las agencias de información comercial y de crédito norteamericano almacenan datos personales que conciernen a cientos de millones de individuos, que tras su adecuada programación, pueden transmitirse a clientes en más de 10,000 aspectos diferentes (por edad, profesión, sexo, ingresos, automóvil o vivienda poseídos, pertenencia a sindicatos, partidos o sociedades mercantiles, culturales o recreativas"[20].

Nadie duda que las computadoras y los bancos de datos son esenciales para el hombre contemporáneo, lo que se quiere evitar es anular su intimidad y convertirla inescrupulosamente en objeto de

[19]Ibidem.
[20]**PEREZ LUÑO,** Ob. Cit. P.49.

explotación económica o vehículo de control político. El uso de los bancos de datos es una veta económica a la cual es difícil renunciar y lógicamente tiene que encontrar defensores:

"La autopista de la información podrá seleccionar los consumidores de acuerdo con matices más precisos y enviar una publicidad diferente para cada uno. (...) Se pueden recopilar y distribuir datos sobre las preferencias de cada uno sin violar la privacidad de nadie, porque la red interactiva podrá utilizar información sobre los consumidores para encaminar la publicidad sin revelar qué hogares específicos son los que la reciben. Una cadena de restaurantes podría saber solamente que recibieron el anuncio una determinada cantidad de familias con ingresos medios y niños pequeños (...)Uno de los modos que tendrán los anunciantes de captar nuestra atención será ofrecernos una pequeña cantidad de dinero, unos céntimos por ejemplo, cuando miremos un anuncio (...) los anunciantes procurarán enviar mensajes pagados solamente a aquellas personas que reúnan determinadas características demográficas"[21].

Al respecto, podría argumentarse que aún no hay seguridad total en la reserva de los bancos de datos y que no se realicen cruces entre ellos, y el simple hecho que los anunciantes estén dispuestos a pagar para ser escuchados involucra la aceptación de la titularidad del derecho a la intimidad y ese pago es una compensación encubierta.

Con el tiempo, las personas preferirían el dinero recibido a cambio de parcelas cada vez mayores de su intimidad.

[21]**GATES**, William H. Camino al futuro. New York: Penguin Books. P. 169-171.

2.2.1.4. Cookies.

A las cookies podríamos definir como: "fichas de información automatizada, las cuales se envían desde un servidor Web al ordenador del usuario, con el objetivo de identificar en el futuro las visitas al mismo sitio. Las cookies son una potente herramienta para almacenar o recuperar información empleada por los servidores Web debido al protocolo de transferencia de ficheros (http). Los riesgos ya los conocemos: recopilación de gustos, preferencias, hábitos, nombre y contraseña y además que algún experto podría manipular estos archivos[22]".

En este sentido las cookies vendrían a ser, huellas electrónicas que posibilitan a la página Web y redes publicitarias el control de nuestros movimientos. Un ejemplo del peligro potencial de las cookies se puede remitir a los datos siguientes:

"En mayo de 1998, Al Gore encargó al FTC (Federal TradeComission) un estudio acerca de la privacidad en Internet. Los desesperantes resultados aparecieron en junio: de 1400 websites comerciales visitados, un 85% recogían y almacenaban datos personales de los visitantes. Sólo un 14% daban alguna indicación acerca de la privacidad de la información recogida y sólo un 2% ofrecía una política en favor de la privacidad de los usuarios con sentido"[23].

El objetivo de usar los cookies es permitir a los sitios y redes publicitarias el control de nuestros movimientos en la red, lo cual incluye cosas tan elementales como la simple búsqueda de palabras en un motor de búsqueda (como Altavista, Yahoo, Excite, etc.),

---

[22] SEGURIDAD INFORMATICA, los cookies y el dleito informático Recuperado el 25 de Abril del 2012 en http://seguridaddigitalizada.blogspot.com/

[23] Ibidem.

lectura de artículos o páginas web. Una vez que el navegante de internet visite alguno de los sitios de los 2,500 clientes de Doubleclick, estará listo para el abordaje de anuncios "personalizados", precisamente del mismo tipo que Bill Gates comentaba en "Camino al futuro" y que mencionamos anteriormente.

En noviembre de 1999 esta empresa compró AbacusDirect, la cual era un banco de datos con nombres, domicilios e información acerca de los hábitos de compra no electrónica de 90 millones de hogares. En enero del 2000 empezaron a compilar perfiles que vinculaban a nombres y domicilios de personas reales con sus compras electrónicas y convencionales. Esta política recibió severa resistencia por los defensores de la intimidad de Estados Unidos y asociaciones de consumidores[24].

No es el único ejemplo del potencial peligro de las cookies.

"(...) en mayo de 1998, Al Gore encargó al FTC (Federal TradeComission) un estudio acerca de la privacidad en Internet. Los desesperantes resultados aparecieron en junio: de 1400 websites comerciales visitados, un 85% recogían y almacenaban datos personales de los visitantes. Sólo un 14% daban alguna indicación acerca de la privacidad de la información recogida y sólo un 2% ofrecía una política a favor de los usuarios con sentido"[25].

Esta constatación nos muestra que en Estados Unidos se ha visto la captura de información como una nueva "goldenrush", una nueva búsqueda de oro. Las empresas para inhibirse de empezar a transar con esta "mercancía" deberán recibir alguna compensación si

---

[24]**ROSEN**, Jeffrey. La intimidad amenazada. Artículo del New York Times reproducido EN: Expreso. 12 de mayo del 2000. P. 27

[25]**CASACUBERTA**, David. La privacidad en los nuevos medios electrónicos. Aspectos técnicos y sociales. Redi Nº 11. Revista electrónica de derecho informático.

seguimos las leyes del mercado. Si no recurren a comprarnos nuestros datos como sugiere Bill Gates, podría ocurrir que la misma privacidad sea un producto en venta, ofreciendo software costoso para inhabilitar las cookies o mecanismos similares que la reemplazarán. Si fuese así, sólo las personas que tienen mayor poder adquisitivo estarán a salvo y los demás que realizan conexiones baratas no lo estarían y la información sobre ellos circularía en todo el mundo[26].

2.2.2.5. Privacidad y cookies de terceros

Las cookies tienen implicaciones importantes en la privacidad y el anonimato de los usuarios de la web. Aunque las cookies sólo se envían al servidor que las definió o a otro en el mismo dominio, una página web puede contener imágenes y otros componentes almacenados en servidores de otros dominios. Las cookies que se crean durante las peticiones de estos componentes se llaman cookies de terceros[27].

Las compañías publicitarias utilizan cookies de terceros para realizar un seguimiento de los usuarios a través de múltiples sitios. En concreto, una compañía publicitaria puede seguir a un usuario a través de todas las páginas donde ha colocado imágenes publicitarias o web bugs. El conocimiento de las páginas visitadas por un usuario permite a estas compañías dirigir su publicidad según las supuestas preferencias del usuario.

La posibilidad de crear un perfil de los usuarios se ha considerado como una potencial amenaza a la privacidad, incluso cuando el seguimiento se limita a un solo dominio, pero especialmente cuando

---

[26] Ibidem.

[27] COOKIE (INFORMÁTICA) Recuperado El 2 de Mayo Del 2012 en http://es.wikipedia.org/wiki/Cookie_(inform%C3%A1tica)

es a través de múltiples dominios mediante el uso de cookies de terceros. Por esa razón, algunos países tienen legislación sobre cookies[28].

El gobierno de los Estados Unidos definió estrictas reglas para la creación de cookies en el año 2000, después de que se conociese que la Oficina de Control de Drogas Nacional de la Casa Blanca utilizaba cookies para seguir a los usuarios que tras visitar su campaña anti-drogas, visitaban sitios relacionados con la fabricación o el uso de drogas. En 2002, el activista por la privacidad Daniel Brandt averiguó que la CIA había estado definiendo cookies persistentes en ordenadores durante diez años. Cuando les informó de que estaban violando la política, la CIA confirmó que esas cookies no habían sido creadas intencionadamente, y dejó de utilizarlas[29]. El 25 de diciembre de 2005, Brandt descubrió que la Agencia de Seguridad Nacional había estado creando dos cookies persistentes en los ordenadores de sus visitantes debido a una actualización de software. Tras ser informada, la agencia deshabilitó inmediatamente las cookies[30].

La directiva de la Unión Europea de 2002 sobre privacidad en las telecomunicaciones contiene reglas sobre el uso de cookies. En concreto, en el artículo 5, párrafo 3 establece que el almacenamiento de datos (como cookies) en el ordenador de un usuario sólo puede hacerse si: 1) el usuario recibe información sobre cómo se utilizan esos datos; y 2) el usuario tiene la posibilidad de rechazar esa operación. Sin embargo, este artículo también establece que almacenar datos que son necesarios por motivos técnicos está

---

[28] Ibidem.

[29]CBS News. CIA Caught Sneaking Cookies. March 20 2002. En COOKIE (INFORMÁTICA) Recuperado El 2 de Mayo Del 2012 en http://es.wikipedia.org/wiki/Cookie_(inform%C3%A1tica)

[30]The Associated Press. Spy Agency Removes Illegal Tracking Files. December 29 2005.En COOKIE (INFORMÁTICA) Recuperado El 2 de Mayo Del 2012 en http://es.wikipedia.org/wiki/Cookie_(inform%C3%A1tica)

permitido como excepción. Se esperaba que esta directiva hubiese comenzado su aplicación desde octubre de 2003, pero un informe de diciembre de 2004 dice (página 38) que no ha sido aplicado en la práctica, y que algunos países miembros (Eslovaquia, Letonia, Grecia, Bélgica y Luxemburgo) ni siquiera la han transpuesto a su legislación. El mismo informe sugiere un profundo análisis de la situación en los estados miembros[31].

Los Cookies de terceros constituyen una preocupación sobre la privacidad y seguridad de los usuarios. Si bien los Cookies son enviados únicamente al servidor que los define o que está en el mismo dominio de Internet, una página Web podría contener imágenes u otros componentes almacenados en servidores de otros dominios. Los Cookies definidos durante la recuperación de estos componentes se denominan Cookies de terceros[32].

HTTP, el protocolo que proporciona los fundamentos para la Web, no puede realizar el seguimiento de las acciones de los usuarios en sesiones en línea sucesivas. Como comodidad para los usuarios, se ideó una extensión para permitir el mantenimiento de un estado, una memoria de eventos anteriores, a través de múltiples solicitudes y respuestas HTTP. Los Cookies, definidos en RFC 2109 en 1997, son valores simbólicos dentro de las solicitudes y respuestas HTTP que permiten que los sitios Web "recuerden" al usuario en cada visita. Si los Cookies se definen por sesión, permanecen en la memoria volátil y caducan cuando el usuario cierra el explorador, o en una fecha de vencimiento configurada previamente, como por ejemplo un mes. Estos Cookies persistentes permanecen en la computadora del usuario; residen en un archivo "Cookies" en el disco duro. Los Cookies persistentes constituyen un atractivo objetivo para los hackers. Al "olfatear" o leer los Cookies de su computadora, los

[31]Ibidem.
[32]COOKIE Recuperado El 2 de Mayo Del 2012http://es.internetsecurityzone.com/Glossary/Cookie

criminales pueden obtener datos personales suficientes para robarle la identidad o inferir información para otros tipos de fraude[33].

El seguimiento de Cookies controla las actividades de los usuarios en diferentes sitios Web. El seguimiento dentro de un sitio se realiza generalmente con el objetivo de generar estadísticas de uso. El seguimiento en diferentes sitios generalmente es utilizado por empresas de publicidad para generar perfiles de usuario anónimo, que luego se utilizan para dirigir la publicidad según el perfil del usuario[34].

La mayoría de los exploradores admite Cookies y permite que los usuarios definan reglas para el uso de Cookies. Además de elegir si se aceptarán Cookies o no, los usuarios pueden elegir aceptar o rechazar determinados Cookies provenientes de dominios específicos; desautorizar Cookies de terceros; aceptar únicamente Cookies no persistentes, y permitir que un servidor defina Cookies para otro dominio. Asimismo, los exploradores pueden permitir que los usuarios vean y eliminen Cookies individuales[35].

2.2.2.6 Las Cookies: ¿amenaza a la privacidad de información en la Internet?

Como muchas cosas emprendidas por el hombre, las cookies no nacieron para capturar información sino que tenían como objetivo favorecer al usuario, como archivos de texto fueron pensados para que el usuario de una página no tuviera que repetir datos como claves de acceso, números de tarjeta de crédito, etc. cada vez que accediese a ella. Pero ahora se han convertido en archivos que a

[33]Ibidem.
[34]Ibidem.
[35]Ibidem.

priori pueden rastrear información en el disco duro de los usuarios[36], a favor de empresas como Doubleclick, NetGravity o IntelliWeb, que siguen al usuario con fines comerciales y crear un perfil del mismo para ingresarlo en su banco de datos.

Este instrumento de captura de información puede infringir las normas sobre intimidad, y afectar información sensible que atañe únicamente a una persona. Podría decirse que puede desactivarse la cookie y si no se hace es un consentimiento, pero la desactivación incluye instrucciones que no siempre se conocen. En todo caso, si no hay consentimiento toda captura de información no sería legal desde que los datos sirven para identificar a una persona en concreto que no prestó su consentimiento.

"Un caso parecido sería la personalización de los navegadores o de los sistemas operativos con los nombres y apellidos de los usuarios, (por ejemplo Windows 95) las cookies pueden recopilar estos nombres y añadirlos al fichero cookie para recabar cierta información del usuario lo que produciría una clara transgresión del derecho a la intimidad, ya que se han obtenido una serie de datos personales sin el consentimiento del afectado. Pero a esto se podría rebatir diciendo que el usuario acepta la cookie y por tanto da su consentimiento. Sin embargo, esto no es así ya que [hay que configurar] personalmente el Navegador para [que avise de la recepción de cookies y] el consentimiento prestado para la admisión de una cookie ni mucho menos supone una renuncia a los derechos salvaguardados en la [ley][37]."

A partir de lo expuesto, desde el momento en que los datos que aporta la cookies son identificables o identificados con una

---

[36] **GARDNER**, ELIZABETH. El anonimato en la Red. EN: Internet World en español. 1999. Año 5 N° 11. P. 33.
[37] **RAMOS SUAREZ**. ¿Es legal el uso de cookies? EN: REDI N° 8. Agosto 1998.

determinada persona que no prestó su consentimiento para un tratamiento automatizado, son considerados como datos obtenidos ilegalmente. Si el Proyecto al cual nos referimos anteriormente es aprobado, se debe permitir al Comisionado conocer estos casos e imponer la sanción correspondiente.

2.2.2.7. Tecnología digital e Internet

En la sociedad previa a la tecnología digital e Internet el precio a pagar por acceder a la información derivaba de dos factores diferentes: al valor que la información poseía en sí misma había que añadir inevitablemente los costes de producción, replicación y distribución, pues era inevitable que esta información estuviera sujeta a algún tipo de soporte material. Si tomamos el ejemplo de un libro, éste debe estar fabricado en papel y fabricar ese papel cuesta dinero. Además, aunque desde la invención de la imprenta los costes de producción se habían reducido y ya no había que emplear a dedicados y cuidadosos escribanos para reproducir los libros, todavía hacía falta comprar la imprenta, el papel y la tinta, ensamblar el libro y permitir que toda la cadena, desde el autor hasta el librero, obtuviera un beneficio que les permitiera continuar con su actividad[38].

La información digital, en ausencia de formatos físicos, es barata de producir y distribuir, y a pesar de ello resulta no sólo codiciada, sino que además es el activo de mayor valor en la sociedad digital.

La sociedad digital se caracteriza por un hecho singular: el coste de producción del primer ejemplar de cualquier tipo de información (recordemos que información puede ser cualquier cosa, como ya hemos mencionado más arriba) es en la práctica el coste total de producción de todos los ejemplares que se quieran producir. El coste

[38] **ALCANTARA** José F. *La sociedad de control: Privacidad, propiedad intelectual y el futuro de la libertad.* Barcelona. 2008. p. 27

de la copia es marginal y en ello reside una diferencia básica e importante con respecto a los sistemas de producción no digitales. El coste de producción y distribución de la segunda copia de cualquier información (incluidas películas, libros y álbumes musicales) será cero siempre que consideremos un formato electrónico para nuestra copia[39].

2.2.1.8. La estructura técnica de la red. Protocolos y controles.

Aunque formalmente existen una gran cantidad de redes, dado que actualmente hay una infraestructura única que da cobijo a una gran red que acoge en su seno un sinfín de pequeñas redes temáticas, hemos preferido hablar de la red en singular, de Internet, aunque esa red sea en sí misma una red de redes.

Si tenemos que hablar de la red y de sus características estructurales, hemos de comenzar mencionando que la red fue diseñada por científicos y, en tanto que criatura de la ciencia, se rige por sus principios. La red está diseñada para ser funcional, y de este interés por dotarla de funcionalidad derivan dos de sus principales características: la red es abierta y la red es libre. Esto queda perfectamente expresado en la siguiente característica: todas las conexiones de la red se realizan empleando protocolos, que constituyen una sólida base de software libre, los protocolos TCP/IP.

Habituado como estoy desde hace años a utilizar computadoras y la red, en mi vida diaria hace ya mucho que dejé de pensar en qué quieren decir cuando nos dicen que estamos usando un *protocolo.*

[39] **ALCANTARA** Ob Cit. p. 31

2.2.1.9. Normatividad y buenas prácticas nacionales e internacionales relacionadas a la TI y la seguridad de la información

ISO 27001: Gestión de la Seguridad de la Información

Estándar internacional, de amplio uso en las organizaciones públicas y privadas en nuestro país, que tiene por objetivo asegurar que los activos de información de una organización se encuentran protegidos en términos de confidencialidad, integridad y disponibilidad.

ISO 20000: Gestión Servicios de TI

Estándar internacional, de reciente publicación, es la evolución de ITIL, la biblioteca más completa de buenas prácticas para la gestión de los servicios, que enfocados en TI, está fuertemente enfocado en la Entrega del Servicio (ServiceDelivery) y el Soporte al Servicio (ServiceSupport).

COBIT: Objetivos de Control para la Información y Tecnologías Relacionadas

Conjunto de Buenas Prácticas, promovidas por el ITGI (Instituto de Gobierno de TI) una iniciativa de ISACA, la Asociación Internacional de Auditores de Tecnología de Información, que tiene como principal objetivos proporcionar un marco de referencia para el Gobierno de la Tecnología dentro de una organización, asegurando que la inversión que se realiza en tecnología esté alineada con los objetivos del negocio.

NTP 17799: 2007 Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.

Esta Norma Técnica Peruana, es una adopción de la ISO/IEC 17799:2005, hoy renombrada por ISO como ISO/IEC 27002:2005ISla homologación peruana de la ISO 27002

NTP 12207: 2004 Ciclo de Vida del Desarrollo de Sistemas.

Esta Norma Técnica Peruana, es la homologación peruana de la ISO 12207

2.2.1.10. Las contraseñas o claves de acceso son la primera línea de defensa (y a veces la última) de muchos datos de carácter confidencial que se pueden obtener a través de Internet.

¿Tiene usted cuenta de correo electrónico? ¿Y una conexión Wifi doméstica? ¿Es usuario de redes sociales como Facebook o Twitter? ¿Utiliza Microsoft Messenger, Hotmail, Gmail u otro sistema de correo basado en web? Si es así tiene **varias contraseñas de acceso** que permiten acceder a **información confidencial** que no todo el mundo debería conocer. ¿Son seguras sus contraseñas?

Cualquier interesado en acceder a un sistema protegido únicamente por una contraseña tan solo tiene que tener el **tiempo** suficiente para probar una y otra vez claves al azar hasta conseguir encontrar la

correcta: esto es lo que se llama un ataque de **fuerza bruta** por motivos obvios[40].

Si conoce cuales son las **contraseñas más habituales** utilizadas por la gente o si dispone de una lista de palabras comunes en el idioma de su víctima puede utilizar un **ataque de diccionario**, consistente en probar variaciones de esas palabras (mayúsculas, minúsculas, seguidas o precedidas de números o símbolos, con la primera letra mayúscula y el resto en minúsculas, etc...[41])

Por último, si conoce los suficientes **datos personales** de su víctima (fecha de nacimiento, lugar de residencia, nombre de sus seres queridos, aficiones, etc.) puede intentar usar la **ingeniería social** para que el propio usuario le indique su contraseña.

La mejor forma de conseguir que sus passwords de acceso sean seguros es muy fácil: tienen que ser **aleatorios** (para evitar ataques de diccionario), **largos** (para dificultar los ataques de fuerza bruta) y contener una gran variedad de tipos de **caracteres distintos** (para dificultar ambos tipos de ataques). Si además asume el hecho de que nunca nadie le solicitará su clave por teléfono o e-mail, y de que siempre debe asegurarse de estar en la web o programa en el que la usa antes de introducirla, su contraseña estará protegida adecuadamente.

La contraseña ideal debería tener al menos ocho caracteres de longitud y contener letras mayúsculas y minúsculas, símbolos y números. Utilice contraseñas distintas para aplicaciones o sitios diferentes y nunca la envíe por e-mail o la diga por teléfono.

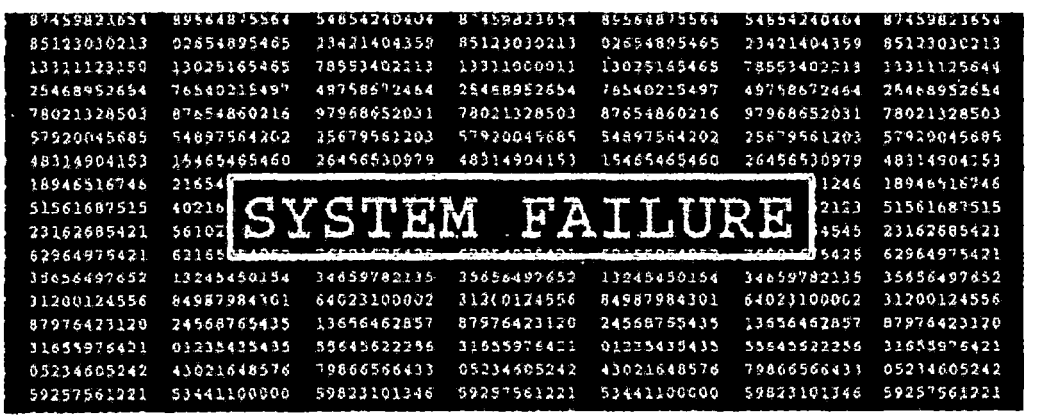
El problema de este tipo de claves es que son **difíciles de recordar**, por lo que una buena técnica para hacerlo consiste en crearlas a

[40]**TICS CONSULTING** - www.ticsconsulting.es. Recuperado el 12 de Febrero del 2012.
[41]Ibidem.

partir de una frase fácil de memorizar con unas reglas que nos permitan convertirla en una contraseña.

Un ejemplo de lo anterior sería este: la contraseña **MdCe"E1ldLMdcnnqa..."** se ha generado a partir de la frase **Miguel de Cervantes escribió "En un lugar de La Mancha de cuyo nombre no quiero acordarme..."**. Esta contraseña es suficientemente larga, contiene letras mayúsculas y minúsculas, números (el 1 sustituyendo la palabra "un") y caracteres especiales (las comillas y los puntos finales) y es fácil de memorizar. No obstante el mero hecho de haberla publicado en este blog hace que su seguridad no sea tan alta.

Tal y como se mencionó en los párrafos anteriores, una contraseña segura debería tener una longitud mínima de ocho caracteres y contener letras mayúsculas y minúsculas, símbolos y números. De esta forma el esfuerzo necesario para averiguar la contraseña aumenta, y se dificulta en gran manera el trabajo de quien intente averiguarla mediante fuerza bruta[42].



Además de estas características generales de la contraseña, hay que tener en cuenta una serie de factores que ayudarán a **mejorar la seguridad** de la misma y que deben ser tenidos en cuenta a la hora

[42]TICS CONSULTING Ob Cit.

de generar, almacenar o usar claves de acceso en cualquier entorno[43]:

- Es importante **no utilizar la misma contraseña para aplicaciones distintas** ya que en caso de un fallo de seguridad en una de ellas que permita a un atacante obtener la contraseña, tendría acceso a otras aplicaciones más protegidas.
- Es necesario **cambiar con frecuencia la contraseña** para dificultar el trabajo de cualquiera interesado en averiguarla mediante un método de fuerza bruta. El tiempo de vida de una contraseña dependerá de la importancia del sistema que protege y deberá cambiarse con más frecuencia (cada treinta días) en los sistemas más importantes y con menos frecuencia (seis meses) en los menos importantes.
- Es conveniente **anotar la contraseña en un papel** para evitar olvidarla, y asegurarse de que ese papel no está cerca del ordenador. Puede servir una página de un libro de nuestra biblioteca, un pequeño trozo de papel guardado tras un cuadro, etc.
- Configurar el navegador o el programa de correo para que **no almacene las contraseñas** o, en caso de que deba hacerse por facilidad de uso, utilice **software de protección de claves** para garantizar su privacidad.
- Evitar el uso de **información personal** como la fecha de nacimiento, el nombre de la mascota, número del documento de identidad, etc. y también de palabras comunes en cualquier idioma. Las claves basadas en datos personales del usuario son las primeras que se suelen probar en un ataque y la información personal ya no es tan personal como debería debido al auge de las redes sociales.
- Si está usando un ordenador que no es el suyo (en un cibercafé, en casa de un amigo, etc.) no puede garantizar su integridad, por lo que debería **evitar introducir contraseñas en ordenadores que no**

[43]TICS CONSULTING Ob Cit.

sean de confianza. Hay programas y dispositivos físicos denominados keyloggers que son capaces de almacenar todo lo que teclea un usuario en un ordenador y son totalmente indetectables si se instalan correctamente.

Una opción es emplear una herramienta de **generación de contraseñas seguras** que le permitirá generar en su navegador contraseñas fuertes para todos los servicios que la precisen. Las contraseñas generadas por este programa no se almacenan en el navegador y pueden usarse con seguridad. La fortaleza de las contraseñas puede ser muy débil, débil, media, fuerte o muy fuerte[44].

Ingeniería social: cuando no es necesario averiguar la contraseña

A pesar de las medidas de seguridad que se tomen a la hora de generar, usar y almacenar las contraseñas, hay que estar siempre atento a una modalidad de ataque que cada día tiene mayor éxito. Nos referimos a la **ingeniería social**.

En cualquier sistema de seguridad, el eslabón más débil de la cadena siempre es el usuario del mismo.

El principio que sustenta la ingeniería social es el que en cualquier sistema **"los usuarios son el eslabón débil"** de la cadena. En la práctica, un ingeniero social usará el teléfono, o la red Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa relacionada con nosotros, un compañero de trabajo, un técnico del departamento de informática o un cliente que requiere acceso a datos confidenciales.

Los consejos respecto a la longitud, complejidad y tiempo de vida de las contraseñas que se mencionaron en párrafos anteriores no

[44]TICS CONSULTING Ob Cit.

ofrecen protección contra el que es, sin lugar a dudas, el sistema de ataque más poderoso y que ofrece un mejor resultado: **la ingeniería social.**

Un ordenador puede tener instalado un excelente **cortafuegos**, un sistema **antivirus** de última generación e incluso un mecanismo de **cifrado de datos** de alto nivel, pero si no se protege uno de los elementos claves del sistema la seguridad no está garantizada. Ese elemento es el usuario, y la **ingeniería social** es la práctica de obtener información confidencial a través de los usuarios legítimos de un sistema.

Como lo dijimos anteriormente si el factor humano es el **eslabón más débil** en un sistema de seguridad, entonces mediante la **manipulación y el engaño** es relativamente sencillo obtener la información confidencial necesaria para hacer que todas las medidas de seguridad sean inútiles.

Kevin Mitnick que se define a si mismo como un **hacker sin malas intenciones** y es uno de los ingenieros sociales más famosos de los últimos tiempos, dice que la ingeniería social se basa en estos cuatro principios[45]:

- Todos queremos **ayudar**.

[45]**TICS CONSULTING** Ob Cit.

- El primer movimiento es siempre de **confianza** hacia el otro.
- No nos gusta **decir no**.
- A todos nos gusta que nos **alaben**.

Una vez planteados esos principios en los que se basa la ingeniería social, es necesario ver con detalle en qué consisten esas técnicas de manipulación. Con unos cuantos **ejemplos reales** de este tipo de ataques es fácil identificar sus características principales:

- ¿Si una web le ofreciera acceder al **historial de conversaciones** de todos tus contactos de MSN de forma sencilla, introduciría tus datos de acceso a Microsoft Messenger?
- ¿Si su banco le indicara que tiene que **confirmar un ingreso en su cuenta** de una cantidad de dinero, seguiría sus instrucciones para hacerlo?
- ¿Si recibiera una llamada telefónica de su compañía telefónica para **confirmar sus datos bancarios** y evitar la baja de su línea se los proporcionaría?
- ¿Si le solicitaran pagar una pequeña cantidad de dinero para realizar los trámites para **cobrar un premio** de lotería de un país extranjero, lo haría?

Todos los ejemplos anteriores son reales y seguro que en alguna ocasión ha recibido un mensaje de correo electrónico o una llamada parecida a los que se indican en ellos. En todos los casos se sigue una misma pauta: la **posibilidad de alcanzar algo deseable** (acceso a datos confidenciales, conseguir dinero, evitar la desconexión del teléfono, etc.) mediante un **mecanismo sencillo** (acceder a una web, indicar un número de cuenta, etc.) y originado por lo general en una **fuente de confianza** (nuestro banco o compañía telefónica[46])

[46]**TICS CONSULTING** Ob Cit.

¿Cómo evitar ser víctima de la ingeniería social?

La mejor herramienta para protegerse de los ataques de ingeniería social es el **sentido común**. Con un pequeño esfuerzo de análisis de los ejemplos anteriores puede encontrar rápidamente preguntas sin respuesta: ¿Es posible que un servicio usado por millones de usuarios como MSN tenga una vulnerabilidad que permita acceder al historial de conversaciones? ¿Es creíble que una entidad bancaria necesite confirmación para recibir dinero en una cuenta? ¿De verdad cree que una compañía telefónica puede perder sus datos bancarios? ¿Es posible ser el ganador de un premio de lotería sin haber jugado?

A continuación, algunas recomendaciones que pueden ayudar a identificar las estrategias usadas en la ingeniería social y por tanto a evitar ser víctima de este tipo de ataques:

- Nunca revele por teléfono o e-mail **datos confidenciales** (como claves de acceso, números de tarjetas de crédito, cuentas bancarias, etc.).
- Nunca haga click en un **enlace a una página web** que le llegue a través de un e-mail en el que le piden datos personales.
- Desconfíe de cualquier mensaje de e-mail en el que se le ofrece la **posibilidad de ganar dinero** con facilidad.
- Si es usuario de banca electrónica o de cualquier otro servicio que implique introducir en una web **datos de acceso**, asegúrese de que la dirección de la web es correcta.
- No confíe en las direcciones de los **remitentes de e-mail** o en los **identificadores del número llamante** en el teléfono: pueden falsearse con suma facilidad.
- Instale en su ordenador un buen **software de seguridad** que incluya si es posible funcionalidad antivirus, antiphising, antispyware y antimalware para minimizar los riesgos.

- **Utilice el sentido común** y pregúntese siempre que reciba un mensaje o llamada sospechosa si alguien puede obtener algún beneficio de forma ilícita con la información que le solicitan.

2.2.1.11. Legislación internacional.

Podemos mencionar múltiples ejemplos de legislación nacional que se ocupa del tema, sin embargo previamente mencionaremos algunos casos de legislación supranacional[47]:

- Organización para la Cooperación y Desarrollo Económico (OCDE), la cual es una organización internacional intergubernamental que reúne a los países más industrializados de economía de mercado. En 1978, formó un Grupo de Expertos que elaboró un conjunto de Directrices, referentes a la intimidad personal y a las transmisiones internacionales de datos, que fueron adoptadas por el Consejo de Ministros de la OCDE, en forma de recomendación a los Estados miembros, el 23 de septiembre de 1980.
Estas Directrices recomiendan a los Estados cuatro principios básicos:

a) los Estados deben tener en cuenta las implicaciones del procesamiento interno y reexportación de datos personales a otros Estados (parágrafo 15). Pone de relieve la necesidad de un respeto mutuo entre los Estados en el área de la protección de datos personales y la vida privada.

b) cada Estado debe tomar las medidas razonables y apropiadas para que las transmisiones internacionales sean ininterrumpidas y seguras, incluso cuando se realizan a través del territorio de un Estado miembro.

---

[47]**DE URIOSTE**, Mercedes. Protección de Datos Personales. REDI N° 23. Junio del 2000

c) Los Estados deben evitar, en general, restringir las transferencias internacionales de datos personales, excepto cuando: 1) los Estados receptores "no observen" el contenido de las Directrices; 2) cuando la reexportación de datos personales eluda las disposiciones internas del Estado transmisor; ó 3) cuando ciertas categorías de datos personales –por ejemplo: datos sensibles- reciban una protección especial en la legislación interna y tal protección no sea equivalente en otros Estados;

d) Los Estados deben evitar adoptar disposiciones normativas, políticas y prácticas legales cuando: 1) la única finalidad sea proteger la intimidad y las libertades individuales, si para ello se obstaculiza la transmisión internacional de datos; 2) el contenido de las disposiciones exceda de la normativa ya existente sobre el tema. Con esta cláusula, las Directrices intentan buscar un equilibrio entre la protección de la intimidad y la libre circulación internacional de información.

- Directiva 95/46/CE de la Comunidad Europea sobre la protección de los individuos en relación al procesamiento de datos personales y sobre la libre circulación de esos datos, del 24 de octubre de 1995.
A fin de remover los obstáculos al libre movimiento de datos sin dejar de garantizar la protección del derecho a la privacidad, se aprobó esta Directiva que armoniza las normas nacionales en la materia. De este modo, el derecho a la intimidad de los ciudadanos goza de una protección equivalente en toda la Comunidad. Contiene el desarrollo internacional más importante en materia de protección de datos de la última década. En tal sentido:

a) establece los principios para la protección de la privacidad a nivel europeo que deben ser incorporados a la legislación de todos los Estados miembros. Por lo tanto, representa el más moderno

consenso internacional sobre el contenido deseable del derecho a la protección de datos y constituye un modelo valioso para otros países y,

b) prohíbe la transferencia de datos personales desde la Comunidad a cualquier Estado no miembro que no tenga leyes de protección de datos "adecuadas", lo cual impone un grado de presión internacional para que aumente el nivel de protección en los demás países, particularmente en el sector privado.

En Internet, muchos usuarios hacen circular archivos, expedientes o correo confidencial mediante "attachment" (adjunto) u otra manera, pero esa no es la única información involucrada, el sólo conocimiento del destinatario puede convertirse en una información valiosa.

Como ya se ha indicado, para los cazadores de información es una presa demasiado suculenta para ignorarla, aunque en nuestro trabajo nos concentramos en el sector privado, hay que aceptar que en el sector público los daños pueden ser mayores por la gran variedad de bancos de datos que existen en cada entidad pública.

Según Hance[48], la legislación europea y la de América del Norte hace una distinción entre "ser monitoreado" por una autoridad pública o por un usuario privado. En la mayoría de estos países, se considera a la privacía como un valor que merece protección, aunque los medios legales para hacerlo varían de un país a otro, en algunos casos la ley es la que protege y en otros casos la jurisprudencia lo hace. Lo importante es que la protección contra el monitoreo público y privado existe por igual, siendo estrictamente regulado el procesamiento de datos personales (tanto en el sector privado y público europeo y en el sector público de Estados Unidos y Canadá) o está sujeto a la

[48]**HANCE**, Olivier. Leyes y Negocios en Internet. México: Mc Graw Hill. P. 127-133.

autorregulación (con referencia al sector privado de estados Unidos y Canadá).

La autorregulación empresarial ha sido blanco de varias críticas, porque al contrario de la confianza que tiene Hance en esta opción, existen expertos que la ven con desconfianza por varias razones, una de ellas es que no pasa de ser una colección de tópicos de buena voluntad. No hay precisiones ni se indica que el usuario pueda consultar la base de datos para ver que información ha sido capturada sobre él, saber que pasa con sus datos si una empresa es absorbida por otra (o comprada, recordemos el caso de DoubleClick), conocer si hay cookies, donde se almacenan y qué tipo de perfiles se generan de cada usuario. Como ya hemos dicho, la autorregulación depende de la buena voluntad de las empresas, pero bien sabemos que las empresas no tienen como fin la buena voluntad sino el lucro (lo cual es natural, para eso existen; sostener lo contrario sería ilógico) y por tanto, en cualquier momento podría cambiarse la mencionada buena voluntad, que no tiene que ser unánime en todo el sector empresarial, y podemos encontrar empresas sin buena voluntad con mucha facilidad, en tal caso el usuario no podría protestar porque no tendría a quien dirigirse. Puede ser que la empresa en verdad crea en la buena fe, pero puede ser comprada por otra, ser absorbida, sufrir un cambio de directorio o cambiar su giro a la venta de datos personales[49].

La legislación estadounidense no regula la creación de archivos computarizados de datos personales en el sector privado, lo cual no está contemplado en el ElectronicsCommunicationsPrivacyAct de 1986 el cual se dirige al sector público, y lo mismo ocurre con el PrivacyAct de Canadá (1985).

[49]CASACUBERTA, David. La privacidad en los nuevos medios electrónicos. Aspectos técnicos y sociales. EN: REDI-Revista Electrónica de Derecho Informático. N° 11. Recuperado el 2 de mayo del 2012 en http://www.alfa-redi.org/rdi.shtml

En Europa se ha recogido la experiencia norteamericana y extendido sus efectos al sector privado. Por ejemplo, en Alemania la Ley Federal de Protección de Datos del 27 de enero 1977, Bundesdatenschutzgesetz, que se caracterizó por regular la protección de datos en el sector público sino también disciplina la utilización informática de datos personales por parte de las empresas privadas, además crea un comisario federal para supervisar esta cuestión y crea un responsable del cumplimiento de esta ley en cada departamento administrativo o empresa privada que elaboren automáticamente este tipo de información[50].

Pero este no es el único aspecto interesante de esta ley, también encontramos un decálogo de las actuaciones que es necesario efectuar para impedir el acceso indebido a los bancos de datos por parte de terceros:

I. Impedir a las personas no autorizadas el acceso a los aparatos con los que se elaboran datos personales.

II. Impedir que quienes llevan a cabo la elaboración de datos personales transporten sin autorización los soportes que los recojan.

III. Impedir la inserción no autorizada de datos personales en la memoria, al igual que el conocimiento, modificación o cancelación de los memorizados.

IV. Impedir la utilización por parte de personas no autorizadas de sistemas de tratamiento de datos, los cuales, de los cuales, en los cuales o a través de los cuales se transmitan informaciones personales por medio de dispositivos autónomos.

---

[50] MURILLO DE LA CUEVA, Pablo Lucas. El Derecho a la autodeterminación informativa. La protección de los datos personales frente al uso de la informática. Madrid:Tecnos. 1990. P.131-132.

V. Asegurar que las personas autorizadas para utilizar un sistema de elaboración de datos mediante dispositivos autónomos únicamente puedan acceder a aquellos datos personales contemplados en la autorización.

VI. Asegurar que se pueda controlar y verificar posteriormente a qué centros se pueden transmitir datos personales mediante dispositivos autónomos.

VII. Asegurar que se pueda controlar y verificar posteriormente qué datos personales han sido introducidos en un sistema de elaboración de datos, cuando y por quién.

VIII. Asegurar que los datos personales, elaborados a requerimiento de terceros, sólo se traten de acuerdo con las instrucciones del requirente.

IX. Asegurar que en la transmisión de información personal, así como en el transporte de los correspondientes soportes, aquella no puede ser leída, modificada o cancelada.
X. Orientar la organización empresarial interna y externa de manera adecuada a las particulares exigencias de la protección de datos.

Ante realidades del mundo moderno como las adquisiciones de DoubleClick y otras empresas, nos parece interesante llamar la atención sobre el sexto postulado. Hay una restricción a la transmisión de los contenidos del banco de datos y es un aspecto de especial importancia en nuestro trabajo teniendo en cuenta que si mediante los Cookies obtenemos información y lo complementamos con bancos de datos de empresas adquiridas, fusionadas, absorbidas o que se dedican a este negocio, el poder que se puede obtener es fabuloso y demasiado tentador como para pensar en

autorregulaciones empresariales, en tal sentido, a riesgo de adelantar nuestra opinión, nos parece bien que haya regulación en el sector privado referida a los bancos de datos.

En Francia, la Ley Nº 78-17 del 6 de enero relativa a la informática, ficheros y libertades; exige como requisito previo al comienzo de las actividades de un banco de datos, su autorización previa por ley o acto reglamentario si se trata de un organismo público o de una entidad particular que presta un servicio público. En cambio, para las agencias privadas basta una comunicación previa.

Portugal fue el primer país en constitucionalizar la protección de datos (artículo 35 de la Constitución de 1976). De esta forma se contemplaron el derecho de acceso, la prohibición de informatizar datos sensibles personalizados y el rechazo rotundo al número personal de identificación (recordemos el ejemplo mencionado sobre la II guerra mundial).
En Inglaterra destacan el YoungerReport de 1972 y el Data ProtectionAct del 12 de julio de 1984 en cuyos 8 principios se pretendió condensar su significado[51]:

I. Los datos personales han de recogerse y procesarse con lealtad y legalmente.

II. Los propósitos para los que se recogen datos personales deben ser legales y han de especificarse.

III. El uso y revelación de datos personales deben ser compatibles con los propósitos para los que se conservan los datos.

[51]MURILLO DE LA CUEVA, Pablo Lucas. El Derecho a la autodeterminación informativa. La protección de los datos personales frente al uso de la informática. Madrid:Tecnos. 1990. P. 135-139.

IV. La calidad y extensión de los datos personales deben ser adecuadas, pertinentes y proporcionadas a los propósitos para los que se conservan.

V. Los datos personales han de ser precisos y deben actualizarse cuando sea necesario.

VI. No se pueden conservar los datos personales más tiempo que el estrictamente necesario para la consecución del propósito perseguido.

VII. Toda persona tiene derecho: a) a intervalos razonables y sin retrasos ni gastos injustificados, a.i) a ser informado por quien los maneja de si conserva datos personales suyos, a.ii) a acceder a tales datos; y b) cuando sea preciso, a rectificar o cancelar dichos datos.

VIII. Es preciso adoptar medidas de seguridad adecuadas para proteger los datos personales contra el acceso no autorizado, su alteración, revelación o destrucción o su pérdida accidental.

En España es importante destacar a la LORTAD, La ley Orgánica 5/1992 de 29 de Octubre de regulación del tratamiento automatizado de los datos de carácter personal, (42) la cual se sujeta al artículo 18.4 de la Constitución Española, dirigido a la limitación del uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos, y el ejercicio legítimo de sus derechos. Limita el uso de la informática por considerar que la existencia de bancos de datos de carácter personal son un riesgo para el derecho a la intimidad, por esta razón se intenta prevenir violaciones a la intimidad, derivadas del tratamiento de la información. En palabras de MOLINA MATEOS: "La LORTAD, no es una ley de seguridad de la información, ni tampoco una norma destinada a limitar el uso y abuso

de la informática de forma general, sino que está referida específicamente a la regulación del tratamiento de datos personales." Sin embargo, cabe indicar que esta norma sobre la cual la doctrina española se ha ocupado ampliamente ha sido remplazada por la Disposición Derogatoria Única de la nueva Ley de Protección de datos de carácter personal de España del 13 de diciembre de 1999.(43) Esta nueva Ley Orgánica tiene como ámbito el sector público y privado y tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. Entre los varios aspectos de los que se ocupa, están las seguridades ofrecidas a las personas sobre el recojo de información con pleno conocimiento de sus fines, de los alcances de su consentimiento en otorgar información, etc.; también regula la Agencia de Protección de Datos en lo que a su naturaleza jurídica y funciones concierne, así como las sanciones que es capaz de imponer.

2.2.2. VULNERACIÓN AL DERECHO A LA INTIMIDAD

2.2.2.1. Derechos fundamentales.

Los derechos fundamentales son definidos como el Conjunto de derechos subjetivos y garantías reconocidos en la Constitución como propios de las personas y que tienen como finalidad prioritaria garantizar la dignidad de la persona, la libertad, la igualdad, la participación política y social, el pluralismo o cualquier otro aspecto fundamental que afecte al desarrollo integral de la persona en una comunidad de hombres libres. Tales derechos no sólo vinculan a los poderes públicos que deben respetarlos y garantizar su ejercicio estando su quebrantamiento protegido jurisdiccionalmente, sino que

también constituyen el fundamento sustantivo del orden político y jurídico de la comunidad.

El constitucionalista español PÉREZ LUÑO, indica que los derechos fundamentales, como objetivo de autonomía moral, sirven para "designar los derechos humanos positivizados en el ámbito interno, en tanto que la fórmula derechos humanos es la más usual en el plano de las declaraciones y convenciones internacionales[52]" Los derechos fundamentales son derechos humanos positivizados en un ordenamiento jurídico concreto. Es decir, son los derechos humanos concretados espacial y temporalmente en un Estado concreto.
La terminología de los derechos humanos se utiliza en el ámbito internacional porque lo que están expresando es la voluntad planetaria de las declaraciones internacionales, la declaración universal de los derechos humanos frente al derecho fundamental.
Destacar que los derechos humanos son propios de la condición humana y por tanto son universales, de la persona en cuanto tales, son también derechos naturales, también son derechos preestatales y superiores al poder político que debe respetar los derechos humanos. Se decía también que eran derechos ligados a la dignidad de la persona humana dentro del Estado y de la sociedad. Lo que interesa destacar es que si los derechos fundamentales son derechos humanos, tienen éstos también las características que hemos reconocido a los derechos humanos. Por tanto, a los derechos fundamentales no las creas el poder político, ni la Constitución, los derechos fundamentales se imponen al Estado, la Constitución se limita a reconocer los derechos fundamentales, la Constitución propugna los derechos fundamentales, pero no los crea.

Si los derechos fundamentales son derechos humanos, los antecedentes legislativos de los derechos humanos los encontramos

[52]**PÉREZ LUÑO,** Antonio. *Derechos Humanos. Estado de Derecho y Constitución.* 4ta. ed.: Tecnos, Madrid,1991, p 31

en las tres grandes declaraciones de derechos de los tres primeros estados liberales:

- Declaración de derechos británica (Bill of rights de 1689).
- Declaración de independencia de Estados Unidos, y ladeclaración de derechos del buen pueblo de Virginia, ambas de 1776.
- Declaración de derechos del hombre y del ciudadano de 1789.

Terminología y contenido esencial. Según BrageCamazano[53], que para determinar si una determinada limitación a un derecho fundamental concreto es legítima conforme a la Constitución, deben examinarse los siguientes aspectos:

A) En primer lugar, hay que saber si un determinado supuesto de hecho encaja en el ámbito normativo de protección del derecho fundamental (sí es "vida" o "domicilio" o "intimidad", por ejemplo): Si no encaja el examen se detiene, pues no hay ninguna verdadera cuestión de derecho fundamental a resolver; si encaja, el examen continúa;

B) Luego, hay que averiguar si ha habido una interferencia en ese ámbito normativo de protección (también llamado "tipo" del derecho fundamental, por analogía con los tipos penales): si la ha habido el examen continúa, pero si no la ha habido se detiene, pues no hay ninguna verdadera cuestión de derecho fundamental a resolver; si, por el contrario, se concluye que sí ha habido esa intervención en el derecho fundamental, se pasa a la siguiente fase;

[53]**BRAGE CAMAZANO** Joaquín*Aproximación a una Teoría General de los Derechos Fundamentales En El Convenio Europeo De Derechos Humanos*. -Madrid: Centro de Estudios Políticos y Constitucionales - CEPC, 2005. p. 111

C) En esta tercera fase, dice BrageCamazano que hay que determinar si es legítima la intervención en los derechos fundamentales, para lo cual han de darse los siguientes requisitos constitucionales, que a su vez hay que analizar escalonadamente: a) reserva de ley; b) generalidad de la ley; c) no retroactividad; d) exclusividad jurisdiccional penal o reserva jurisdiccional general; e) Principio de proporcionalidad: 1) Fin constitucionalmente legítimo; 2.- Adecuación o idoneidad; 3.- Necesidad; 4.- Proporcionalidad en sentido estricto; 5.- Contenido esencial, en su caso[54].

Teoría de los derechos fundamentales.

De Vega señala que "Las diversas teorías de los derechos fundamentales constituyen aportes adecuados para el desarrollo de los derechos de libertad en sus realidades, como también resultan insuficientes para resolver por si solas los problemas contemporáneos de la falta de realización de los derechos fundamentales en todas las regiones con culturas diferentes. Por eso, hay que recordar que junto a las teorías de los derechos fundamentales, se encuentran diversas concepciones jurídicas culturales de Estado, sociedad, economía y naturaleza, que deben poner en relación de interdependencia a los derechos fundamentales con las variables culturales de cada Estado constitucional, para afrontar integralmente la teoría y la praxis de los derechos fundamentales. En ese entendido, la realidad constitucional latinoamericana esta caracterizada básicamente por la necesidad de desarrollar o de ajustar la dogmática de los derechos fundamentales a las demandas y desafíos contemporáneos; proceso en el cual, el perfeccionamiento de la jurisdicción de la libertad sobre la base de la mirada atenta a la realidad y también a la dogmática europea, ayudará a la recuperación del sentido de la teoría y de la práctica de los derechos fundamentales para el fortalecimiento del Estado democrático

[54]Ibidem.

constitucional. De lo contrario, los derechos fundamentales quedarán reducidos a un ejercicio semántico de los mismos y sometidos a los poderes fácticos de turno, experiencia propia de los Estados neoliberales en América Latina"[55].

El contenido esencial de los derechos fundamentales

Todo derecho fundamental tiene un contenido jurídicamente determinado, el cual es inmodificable, en caso sea necesario llevar a cabo una regulación infraconstitucional para posibilitar su goce y ejercicio en la vida comunitaria.

Claudia Villaseñor Goyzueta señala que "comprende la "sustancia" del derecho; sin el cual deja de ser tal. Esta nota sustancial de la norma hace que esta tenga en relación a las restantes una peculiaridad privativa y especifica. En ese orden de ideas, el contenido esencial se convierte en la parte indispensable e indisponible que permite al titular del derecho a gozar de los atributos, facultades o beneficios que esta declara. Su afectación conlleva a la transformación del derecho contenido en un precepto en otra categoría jurídica distinta; amén de generar la imposibilidad o dificultad extrema para hacer efectivo el goce de un derecho"[56].

Claudia Villaseñor Goyzueta plantea que el establecimiento del contenido esencial de un derecho debe ser observado en un doble plano, a saber[57]:

---

[55]**DE VEGA** Pedro, *Neoliberalismo y Estado*, en *Pensamiento Constitucional*, Año IV, Nº 4, Pontificia Universidad Católica del Perú – Maestría en Derecho Constitucional, Fondo Editorial, Lima, 1997, pp. 31 y ss.

[56]**VILLASEÑOR GOYZUETA** Claudia Contenido esencial de los derechos fundamentales y jurisprudencia del Tribunal Constitucional Español. Madrid: Universidad Complutense, 2003

[57]Ibidem.

a) Plano negativo

Señala un límite a la regulación legislativa de los derechos fundamentales.

b) Plano positivo

Señala el valor asignado al contenido de los derechos fundamentales, por ende, este deviene en imprescindible e insustituible.

En efecto, en todo derecho fundamental existen dos zonas: una esfera medular que constituye a su contenido esencial –y en cuyo ámbito toda intervención del legislador se encuentra vedada y en una esfera adjetiva o no esencial en la cual es admisible la actuación regulatoria del legislador. Cabe señalar que esto último opera a condición que se lleve a cabo conforme a los principios de razonabilidad, racionalidad y proporcionalidad.

2.2.2. Derecho a la intimidad.

La necesidad de intimidad es inherente a la persona humana ya que para que el hombre se desarrolle y geste su propia personalidad e identidad es menester que goce de un área que comprenda diversos aspectos de su vida individual y familiar que esté libre de la intromisión de extraños. Así pues, debemos entender que todos los seres humanos tenemos una vida "privada" conformada por aquella parte de nuestra vida que no está consagrada a una actividad pública y que por lo mismo no está destinada a trascender e impactar a la sociedad de manera directa y en donde en principio los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia, ni les afectan[58].

Ciertamente el concepto de vida privada es muy difícil de definir con

[58]**CUAUHTÉMOC** M. De DienheimBarrigueteEl *Derecho a la Intimidad, al Honor y a la Propia Imagen*. México UNAM. 2006. p. 2.

precisión pues tiene connotaciones diversas dependiendo de la sociedad de que se trate, sus circunstancias particulares y la época o el periodo correspondiente.

Sin embargo, dentro de esta esfera de vida privada podemos considerar a las relaciones personales y familiares, afectivas y de filiación, las creencias y preferencias religiosas, convicciones personales, inclinaciones políticas, condiciones personales de salud, identidad y personalidad psicológica, inclinaciones sexuales, comunicaciones personales privadas por cualquier medio, incluso algunos llegan a incluir la situación financiera personal y familiar.

La necesidad de intimidad podemos decir que es inherente a la persona humana y que el respeto a su vida privada manteniendo alejadas injerencias no deseables e indiscreciones abusivas, permitirá que la personalidad del hombre se desarrolle libremente. De esta forma la protección a la vida privada se constituye en un criterio de carácter democrático de toda sociedad.

Sin duda alguna, el respeto a la vida privada y a la intimidad tanto personal como familiar se constituye en un valor fundamental del ser humano, razón por la cual el derecho ha considerado importante tutelarlo y dictar medidas para evitar su violación así como para intentar subsanar los daños ocasionados.

De esta manera surge el llamado derecho a la privacidad, a la vida privada o simplemente derecho a la intimidad, como un derecho humano fundamental por virtud del cual se tiene la facultad de excluir o negar a las demás personas del conocimiento de ciertos aspectos de la vida de cada persona que solo a ésta le incumben.

García-Villegas Sánchez-Cordero señala que "dentro de los diversos límites a la libertad de expresión, cuya existencia se advierte de la

lectura de cualquiera de los artículos antes referidos, se encuentra el también derecho fundamental a la honra y a la intimidad"[59].

"En relación con los derechos citados en último término, los tribunales han tendido a resolver la colisión con el derecho a la libertad de expresión, tomando como base el criterio de jerarquía de derechos constitucionales"[60].

Para acreditar la aseveración que antecede, se señalarán sólo dos asuntos, el primero, resuelto en Chile, en el llamado *caso Martorell*, en donde se privilegió el derecho al honor de un funcionario público, sobre la libertad en la expresión de críticas en relación con actuaciones de su vida privada que al salir a la luz pública en un libro la dejaban desvelada y desprotegida. En este asunto "un periodista, Francisco Martorell, publicó un libro llamado *Impunidad Diplomática* en el que se aludía a la conducta indecorosa de ciertos personajes públicos chilenos. Algunos de los aludidos presentaron un recurso de protección. El fallo que acoge el recurso de protección presentado en contra de Francisco Martorell y en el que se prohíbe la circulación del libro en Chile, determina que el derecho al honor y el *derecho a la vida privada tienen mayor jerarquía que la libertad de expresión*[61]."

No obstante, el rango jerárquico superior de la vida privada sobre la libertad de expresión, en relación con aquélla -la vida privada- de los servidores públicos, se ha estimado que está más acotada que la de los particulares, incluso, no pocos estudiosos de los derechos fundamentales, se han formulado preguntas cómo "¿Qué pasa, por ejemplo, si se trata de un político muy conservador que dentro de su campaña para ganar al electorado se jacta de sus grandes atributos

---

[59]**GARCÍA-VILLEGAS** Sánchez-Cordero Paula María La libertad de expresión y algunos de sus límites, articulo en http://www.scjn.gob.mx/NR/rdonlyres/D18C6F32-BF5E-4D34-B398-DB1EC4F72DA3/0/PAULAMAGARCIAVILLEGASSANCHEZCORDERO.pdf, P.9, CONSULTADO EL X/XI/2011

[60]Ibidem.

[61]ObCit, P.10

morales y promete que cuando llegue al parlamento votará por una serie de leyes que contribuirán a fomentar los valores cristianos de nuestra sociedad, pero que no es más que un impostor que por detrás lleva una vida totalmente licenciosa?. ¿No se justificaría aquí desenmascarar a este impostor que, en el fondo, está engañando a quienes votan por él[62]?"

"El derecho a la intimidad es una situación jurídica en la que se tutela el espacio individual y familiar de privacidad de la persona, conformados por experiencias pasadas, situaciones actuales, características físicas y psíquicas no ostensibles y, en general, todos aquellos datos que el individuo desea que no sean conocidos por los demás, porque de serlo, sin su consentimiento, le ocasionaría incomodidad y fastidio".[63]

2.2.2.3. Contenido del derecho a la intimidad.

Este derecho que tiende a proteger la vida privada del ser humano, es un derecho complejo que comprende y se vincula a su vez con varios derechos específicos que tienden a evitar intromisiones extrañas o injerencias externas en estas áreas reservadas del ser humano como son:

· El derecho a la inviolabilidad del domicilio,
· El derecho a la inviolabilidad de correspondencia,
· El derecho a la inviolabilidad de las comunicaciones privadas,
· El derecho a la propia imagen,
· El derecho al honor,
· El derecho a la privacidad informática,

---

[62]ObCit, P.10
[63]**ESPINOZA ESPINOZA**, *Juan*. Derecho de las personas. *Editorial Rodhas*, Lima 1999, Pág. 358. En esta cita, el derecho a la intimidad individualiza a la persona en la reacción que ocasionara la información llegue al público de los comportamiento del individuo, sin que este consienta la propagación de dichos datos.

· El derecho a no participar en la vida colectiva y a aislarse voluntariamente,
· El derecho a no ser molestado[64].

Igualmente este derecho se relaciona con muchos otros derechos como son: el derecho a la no exteriorización del pensamiento e ideas como parte de la libertad de expresión, la libertad de religión y creencias, la libertad de procreación y de preferencia sexual, la libertad de pensamiento y de preferencia política, así como muchos otros derechos de índole familiar.

Por supuesto, también es importante mencionar la relación del derecho a la privacidad con los derechos de libertad de expresión, de imprenta y de información ya que como veremos la vida privada constituye un límite al ejercicio de estas libertades.

Sobre su posición frente a la libertad de información la sentencia del tribunal constitucional, EXP. N.° 1480-2003-HD/TC, LIMA ALBERTO ANTONIO FRANCO MORA, señala que uno de los límites a los cuales se encuentra sujeto el derecho de acceso a la información lo constituyen aquellas informaciones que afectan la intimidad personal. En efecto, el derecho de acceso a la información registrada en cualquier ente estatal no comprende aquella información que forma parte de la vida privada de terceros. Y la información relativa a la salud de una persona, como se establece en el inciso 5) del artículo 17° del Texto Único Ordenado de la Ley N.° 27806, Ley de Transparencia y Acceso a la Información Pública, se encuentra comprendida dentro del derecho a la intimidad personal.

[64]**CÁCERES BARROS** A. Información y Análisis Jurídicos, Derecho a la Intimidad, Nº. 126, México, 2000. p. 12.

2.2.2.4. Alcances del derecho a la intimidad.

"Aun cuando desde antiguo el hombre ha buscado un lugar de sosiego y refugio para el desarrollo de su ser interior, a buen recaudo del tumulto y frenesí de la vida en sociedad, la intimidad no se constituyó en una preocupación central sino con el desarrollo del liberalismo; serán Thomas HOBBES, John LOCKE y John STUART MILL quienes apuntarán, con matices, la necesidad de conciliar el accionar del Estado con los intereses del individuo, quien dispondrá de un margen de vida privada exento de la intervención estatal"[65]. Y "es que sólo la mutación desde una sociedad feudal a otra burguesa ofrecía las condiciones para que la disponibilidad de un ámbito de acción reservado se constituyera en una sentida necesidad de los individuos"[66].

"Este repliegue del individuo en su vida privada no dejó de causar reparos, así se percibe en la obra de Alexis de TOCQUEVILLE, quien repudia el abandono del poder en los expertos por el riesgo que representa para las minorías, e igualmente en Benjamín CONSTANT, quien, tras constatar que mientras la libertad de los antiguos se concretaba en la participación en la vida pública, para los modernos se traduce en mayores espacios de recogimiento y exclusión de aquella, exhorta a conjugar equilibradamente vida privada y pública"[67].

---

[65] En este sentido **BÉJAR,** Helena, "El ámbito íntimo. Privacidad, individualismo y modernidad", Alianza Editorial. Madrid, 1990. **MURILLO DE LA CUEVA**, Pablo. "El Derecho a la Autodeterminación Informativa. La Protección de los Datos Personales frente a la Informática." Editoriales Tecnos. Madrid, 1990, pp. 45 y ss.

[66] **MARTÍNEZ MARTÍNEZ**, Ricardo, *Tecnologías de la información, policía y Constitución*, Tirant lo blanch, Valencia, 2001, pp. 59 - 60. Yendo aún más allá, para develar la ideología subyacente en la protección de la intimidad y su evolución desde un privilegio a un valor constitucional, Cf. **PÉREZ-LUÑO,** Antonio Enrique, *"Derechos humanos, estado de derecho y constitución"*, 5ª edic., Editorial Tecnos, Madrid, 1995, pp. 317 – 344.

[67] **CONSTANT,** Benjamín, *De la libertad de los antiguos comparada con la de los modernos*, cit. por Béjar, Helena, ob. cit., pp. 41 – 49

A mediados del siglo recién pasado, el derecho a la intimidad viene a merecer reconocimiento en un instrumento internacional, cual es la Declaración Universal de Derechos Humanos de 1948, que prevé que nadie será objeto de injerencias arbitrarias en su vida privada y, a su vez, asegura a toda persona el derecho a la protección de la ley contra tales injerencias o ataques. De entonces a esta parte, con un mayor o menor desarrollo normativo, el derecho a la intimidad está previsto sistemáticamente en los tratados internacionales sobre derechos humanos y en términos más o menos explícitos en la Carta Fundamental de los diversos Estados[68].

Ahora bien, las mayores dificultades de la doctrina giran en torno a establecer los márgenes a los cuales se extiende la protección que brinda el derecho a la intimidad. En este sentido, entre los intentos por verificar una delimitación, PÉREZ-LUÑO destaca "la elaboración por la doctrina alemana de la que se ha venido en llamar teoría de las esferas, en la cual, a grandes rasgos, se distinguen ámbitos de acción del individuo de extensión radial, cuyo centro más cercano corresponde a lo secreto, su periferia a aquello que atañe a la individualidad de la persona, y una franja intermedia correspondiente a la intimidad, en que se sitúa aquellos que se desea mantener al margen de la injerencia de terceros"[69].

Sin embargo, prescindiendo del valor pedagógico que la doctrina de las esferas evidencia, muestra asimismo dificultades para establecer

---

[68] Artículo 12 de la Declaración Universal de Derechos Humanos, adoptada y proclamada por la Asamblea General de las Naciones Unidas en su resolución 217 A (III), de 10 de diciembre de 1948.

[69] **PÉREZ-LUÑO**, Antonio Enrique, *Derechos humanos, ob. cit.*, pp. 327 – 331, donde considera las elaboraciones de H. Hubmann, así como de Vittorio Frosini, entre otras. También acude a la teoría de las esferas, con cita a **LEO REISINGER**, Alvarez-Cienfuegos Suarez, José María, *"El derecho a la intimidad personal, la libre difusión de la información y el control del Estado sobre los bancos de datos"*, en *Encuentros sobre Informática y Derecho*, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1990 – 1991, p. 185.

qué ha de calificarse como intimo, lo que le fuerza a recurrir a criterios auxiliares, que no hacen sino reafirmar su escasa eficacia[70].

Para la concepción espacial o geográfica, la extensión de la intimidad está asociada con el control que se tiene sobre determinadas áreas u objetos. De tal suerte, aquello que acontece al interior de los hogares queda al amparo de intromisión alguna; por extensión, se brinda similar protección a la correspondencia y a las comunicaciones telefónicas. Sin embargo, fuera de que el criterio resulta ambiguo en determinados contextos –tal como la calificación de aquello que acontece en un restaurante–, la concepción espacial resulta excesivamente restringida, desde que circunscribe el alcance del derecho a factores externos y minusvalora la trascendencia social de las conductas desplegadas por las personas en el medio, junto con resultar insuficiente para brindar respuesta a las agresiones al derecho cometidas "a distancia", en las cuales no se verifica una invasión al medio espacial en que se desenvuelve la persona, por ejemplo mediante el empleo de cámaras con lentes de largo alcance.

De otro lado, la concepción subjetiva de la intimidad descansa en el distingo entre personaje público y funcionario público, de un lado, y persona privada, de otro. Mientras las actuaciones de aquellos, por la naturaleza de sus funciones o por la influencia que detentan, deben estimarse excluidas del abrigo del derecho a la intimidad, las de los últimos, precisamente por carecer de tales circunstancias, deben estimarse cubiertas por él. No obstante, la concepción subjetiva resulta insuficiente para precisar la extensión de la intimidad, desde que descansa en condiciones esencialmente relativas, pero fundamentalmente porque repugna a criterios de igualdad jurídica, ya que admite la privación del derecho a los funcionarios y personajes públicos con independencia de la relevancia de su comportamiento,

[70] En similar sentido, **MARTÍNEZ MARTÍNEZ,** Ricardo, *op. cit.*, pp. 62 – 64.

salvo recurra a nuevos criterios correctivos, que no hacen sino confirmar que carece de suficiencia para brindar una respuesta apropiada.

"En cambio, la concepción objetiva prescinde de consideraciones materiales o fundadas en la calidad de las personas y más bien atiende al distingo entre conductas públicas y privadas. Serán conductas privadas, y por tanto quedan al alero del derecho a la intimidad, aquellas desplegadas con el propósito de satisfacer necesidades propias; En cambio, las conductas públicas, aquellas que han tenido por finalidad satisfacer necesidades ajenas, quedarán privadas de tal cobertura y será lícita la intromisión a su respecto. Para mitigar la rigidez de esta concepción, se recurre a un factor de corrección, de tal suerte una conducta que en principio merece el calificativo de privada por su "trascendencia" puede dejar de ser tal y devenir en pública"[71].

"Con todo, la mayor parte de la doctrina apunta al carácter esencialmente casuístico que reviste la extensión que se atribuye al derecho a la intimidad"[72].

Si los medios de comunicación de masas importaban un serio riesgo para la intimidad, las nuevas tecnologías lo son aún más, desde que han generado una insospechada capacidad para recoger, procesar y transmitir información; en efecto, el progresivo incremento en el empleo de la informática por servicios públicos y particulares, ha permitido a estos disponer de más y mejor información, conforme a la cual adoptar las decisiones atinentes a sus ámbitos de competencia:

---

[71] **NOGUERA ALCALÁ**, Humberto, *"El derecho a la libertad de opinión e información y sus límites"*. Lexis-Nexis, Chile, 2002, pp.190 – 194.

[72] Entre estos, José Antonio **MARTÍN PALLÍN**, quien estima que no es posible construir un concepto de intimidad, siquiera aproximado, desde que se trataría de un bien jurídico indeterminado, con la plasticidad suficiente para adecuarse a toda subjetividad. Cf. **ROMEO CASABONA**, Carlos María, *"Poder informático y seguridad jurídica"*. FUNDESCO. Madrid, 1988, p. 12 (prólogo).

así, por ejemplo, en unos casos se tratará de la concesión de subsidios o beneficios, en otros el propósito será prever el comportamiento del mercado ante la introducción de un nuevo bien o servicio.

Como quiera que sea, disponer de información apropiada y oportuna deviene en una necesidad revestida de juridicidad, al amparo del derecho a ser informado. Sin embargo, el excesivo celo que puede mediar en la recogida de información y los abusos a que puede conducir su empleo, particularmente cuando ella se refiere a circunstancias íntimas de la persona, ha merecido el reparo del legislador.

En efecto, si el derecho es la respuesta normativa de la sociedad a la fenomenología que tiene lugar en su seno, este entramado normativo no ha podido permanecer impermeable a los cambios que se producen en ella, sino más bien debe nutrirse de las siempre cambiantes condiciones de la sociedad a la cual está llamado a reglar.

En ese orden, las estructuras normativas surgidas en la modernidad y en la etapa de la codificación no han podido sustraerse a los efectos de la creciente aplicación de las nuevas tecnologías que caracteriza a la "sociedad de la información[73]".

2.2.2.5. Protección del derecho a la intimidad.

Así pues el derecho al respeto a la vida privada o intimidad, al honor e incluso a la imagen propia, son considerados ya como derechos humanos fundamentales, establecidos por diversos instrumentos internacionales como son la Declaración Universal de los Derechos Humanos aprobada por la Asamblea general de las Naciones Unidas

[73]**PÉREZ-LUÑO,** Antonio Enrique. *Manual de Informática y Derecho*, Editorial Ariel S.A., Barcelona, 1996, p. 35.

en 1948 (artículo 12), el Pacto Internacional de Derechos Civiles y Políticos de 1966 (artículos 17 y 19), la Convención Americana sobre Derechos Humanos de 1969 (artículos 11 y 13), y en la Convención sobre los Derechos del Niño de 1989 (artículo 16), instrumentos todos estos firmados y ratificados por nuestro país (cabe señalar que también existen otros instrumentos que establecen este derecho como son: la Convención de Roma para la protección de los Derechos Humanos y las Libertades Fundamentales de 1959, la Declaración de los Derechos y libertades fundamentales aprobadas por el parlamento europeo y la Carta Africana de los Derechos del Hombre y de los Pueblos de 1981 y de los que México no es parte.)

DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS (1948)

En su artículo 12 establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o a su reputación y que toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques[74].

PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS (1966)

En su artículo 17 establece las mismas disposiciones que el artículo 12 de la Declaración Universal de los Derechos Humanos y en su artículo 19 al hablar de la libertad de expresión señala que el ejercicio de ese derecho entraña deberes y responsabilidades especiales por lo que podrá estar sujeto a ciertas restricciones fijadas por la ley y que sean necesarias para asegurar el respeto a los derechos o a la reputación de los demás, así como para proteger la seguridad nacional, el orden público, la salud o moral públicas[75].

---

[74]**GARCÍA SAYAN** Diego *Normas internacionales sobre derechos humanos y derecho interno.* Lima Comisión Andina de Juristas. 1984. p.239.
[75]**GARCÍA SAYAN** Ob. Cit. p. 273

CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS (1969) -PACTO DE SAN JOSÉ

El artículo 11 se refiere a que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad y que por tanto no deberá ser objeto de injerencias arbitrarias o abusivas en su vida privada, familia, domicilio, correspondencia, ni deberá sufrir ataques ilegales a su honra o reputación. Y establece también el derecho de la persona a ser protegida por la ley contra esas injerencias o ataques.

El artículo 13 establece la libertad de pensamiento y expresión determinando que no deberá existir previa censura, pero que el ejercicio de esos derechos estará sujeto a responsabilidades ulteriores, mismas que deberán estar expresamente fijadas por la ley y que deberán tender a asegurar entre otras cuestiones, el respeto a los derechos o a la reputación de los demás[76].

CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO (1989) En su artículo 16 menciona que ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o a su reputación; y que el niño tiene derecho también a la protección de la ley contra esas injerencias y ataques[77].

[76]**GARCÍA SAYAN** Ob. Cit. p. 298
[77]**CHUNGA LAMONGA**, Fermín. Derecho de Menores: Doctrina, comentarios al Código del Niño y Adolescente. Lima, Grijley, 3ra. Edición, 2000.p.594

2.2.2.6. ¿Puede ser considerada la privacidad como una mercancía?

La doctrina nacional, recientemente, ha realizado interesantes contribuciones que ha enriquecido el concepto de privacidad. Así, Morales Godo, opta "por la expresión derecho de la vida privada, por ser mas compresiva de la diversa gama de objetos que pueden ser motivo de ese valor jurídico. La traducción al español del right of privacy, es la expresión más cabal y deberíamos utilizarla, en vez de derecho a la intimidad. Participamos del idea que existe una relación de género a especie. En efecto, la expresión vida privada comprende lo que algunos denominan la "esfera intima" y además aquel sector de circunstancias que sin ser secretas o intimas propiamente dichas, deben ser respetadas por ser un presupuesto de la tranquilidad de la persona".[78]

Bullard, partiendo de una lógica propietarista "entiende al derecho a la privacidad como una mercancía susceptible de ser vendida en el mercado".[79] "Pone como ejemplo a los strippers, la industria pornográfica, la información privada de ciertos personajes públicos, entre otros; cada uno vende (o puede vender) cierta parte de su privacidad, afirmando que "el mercado necesita de la privacidad para operar, pues ella permite definir el ámbito de actuación de la autonomía privada. Pero una mala definición de la privacidad nis puede conducir a elevar innecesariamente los costos de transacción y

---

[78]**MORALES GODO**, *El derecho a la vida privada y el conflicto con la libertad de información*, Grijley, Lima, 1995, p. 109.

[79]Así, "uno podría, sin embargo, abordar la idea del derecho a ser dejado (solo) a partir de la teoría de los derechos de propiedad" (**BULLARD GONZÁLES**, No se lo digas a nadie ¿Se puede vender el derecho la privacidad en el mercado?, en Ius et veritas, Año IX, Nº17, Lima, 1998, 170). Con respecto a la privacidad entendida como el derecho a que cierta información no sea revelada, expresa que "la libertad seria, desde esta concepción, una alternativa o sustituto a los derechos de propiedad intelectual sobre la información referida a la vida privada (Cit., 173).

a colocar costos en quienes no tendrían porque sopórtalos".[80] Comparto la preocupación del autor por la importancia de la delimitación de la esfera privada. Discrepo con patrimonializar las situaciones jurídicas existenciales de los sujetos del derecho: las mismas se desarrollan a través de la lógica del ser, a diferencia de las patrimoniales, que se dan dentro de la categoría del tener. Lo que se puede decir respecto de la privacidad, se puede afirmar a propósito de la imagen o de la voz: se puede ceder parte de la privacidad, permitir una producción fotográfica o la grabación de la voz, a cambio de una contraprestación. Por ellos no se patrimonializan estos derechos. Esto mismo sucede cuando se lesionan y dan lugar a una indemnización (patrimonial). Debemos recordar que tanto el ser humano, como sus manifestaciones, o modalidades de ser, como decía KANT, son un fin y no un medio".

Una lógica propietarista de los derechos de las personas nos llevaría a resultados alarmantes. Rodota advirtió que el Tribunal de Berlín estableció que no son admisibles las interrupciones publicitarias como contraprestación del servicio gratuito de llamadas, particularmente cuando se trata de servicios financieros. Esto es solo un ejemplo de comercializar la esfera de la privacidad (o cualquier derecho de la persona): simple y llanamente, se termina con comercializar a la misma persona. Es por ello que se sostiene que "la conquista de una libertad engañosa consistente en comercializar cualquier información propia, tendría un precio mucho más alto que una llamada telefónica gratuita o una computadora de regalo. Significaría, perdida del a soberanía sobre si mismo y, al mismo tiempo, la renuncia a una esfera propia en la cual sea posible desarrollar la personalidad y perseguir la plenitud de la libertad".[81]

---

[80] **BULLARD GONZÁLES**, Estudios de análisis económico del derecho, Ara, Lima, 1996, 349.

[81] **RODOTA, A** Si nuestra "privacy" se convierte en una mercancía, en Revista de responsabilidad Civil, La Ley, Año I, Nº 6, Noviembre – Diciembre de 1999, Buenos Aires, p. 192.

2.2.2.7. El derecho a la inviolabilidad de las comunicaciones Privadas.

Las comunicaciones privadas son inviolables con independencia de su contenido.El objeto de protección constitucional lo constituyen el proceso de comunicación y, eventualmente, los datos que identifican la comunicación, como pueden ser los números marcados por un usuario, la identidad de los comunicantes, la duración de una llamada o, en el caso de un correo electrónico, la dirección de protocolo de internet (IP).La protección de las comunicaciones privadas persevera en el tiempo, tutelando también a los medios que conservan el contenido de las comunicaciones, de modo que, una vez finalizadas aquéllas, los soportes materiales que almacenan dicha comunicación devienen, también, inviolables.

Para que una comunicación sea inviolable, el mensaje debe transmitirse a través de un medio o artificio técnico desarrollado por la tecnología, sin importar si se trata de un telégrafo, del teléfono, del correo electrónico o de cualquier otro medio que surja por los avances de la tecnología.Todo parte del principio de la inviolabilidad de las comunicaciones privadas, no solo por parte de las autoridades, sino también por los particulares. Para que una comunicación sea inviolable, el mensaje debe transmitirse a través de un medio o artificio técnico desarrollado por la tecnología, sin importar si se trata de un telégrafo, del teléfono, del correo electrónico o de cualquier otro medio que surja por los avances de la tecnología.

2.2.2.8. El Derecho a la privacidad informática.

El iusfilósofo Pérez Luño[82], en España, como Vittorio Frosini[83] en

[82]**PEREZ LUÑO,** Antonio. *Derechos humanos, estado de derecho y constitución.* Ed. Tecnos, Madrid, 1984, p. 316

Italia, propusieron en sus diferentes ámbitos geográficos el derecho de la libertad informática, con diversos fundamentos y diferente nomen iuris (derecho fundamental y derecho de la personalidad, respectivamente); así mientras, Pérez Luño, plantea sus argumentos con base en los derechos de la libertad de información, el derecho de habeas data (acceso, rectificación --inmerso el "derecho al olvido"-- y cancelación de la información) y los derechos a la intimidad, el honor y la propia imagen de los cuales se desprende cuando entra en contacto el "uso de la informática" con el derecho; para el iusfilósofo italiano Frossini, el estudio y análisis derecho de habeas data, así como de sus fases o ciclos informáticos, lo lleva a ubicar la libertad informática, como un "derecho perteneciente a la personalidad moral, definiéndolo como el derecho de disponer de los propios datos personales, esto es, de controlar la veracidad o exactitud, de impedir la difusión si se trata de datos sensibles o reservados, de verificar la utilización para el fin autorizado".

Se considera que la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona... así(como) también, (de) derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data).

Este derecho nuevo es un derecho instrumental ordenado a la protección de otros derechos fundamentales, entre los que se encuentra, desde luego, la libertad sindical,... frente al uso torticero de la tecnología informática..., sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona. Así, se consagra aquélla dicotomía no

---

[83]**FROSINI,** Vittorio. LA PROTECCION DE LA INTIMIDAD: DE LA LIBERTAD INFORMATICA, AL BIEN JURIDICO INFORMATICO. En: Revista Derecho y Tecnología Informática No 3. Editorial Temis. Bogotá.1990

fácil de asimilar a la vez como: derecho-instrumento y derecho-autónomo. Dicotomía inexistente en la concepción de la "libertad informática", no como nuevo derecho sino como un bastión tecnológico más del derecho a la intimidad.

Pérez Luño, considera nuevo derecho fundamental de la persona humana, derivado de otros derechos de igual rango constitucional, como la intimidad personal y familiar, el honor, la propia imagen que son los tutelados, dividiremos el planteamiento en cuatro apartes y a renglón seguido haremos las glosas pertinentes. Los temas a tratar son:

- La dignidad humana como fundamento de la intimidad,
- El contenido del derecho a la intimidad,
- La relación-tensión: informática e intimidad, y
- Reconocimiento de la libertad informática, a partir del almacenamiento de datos.

2.2.2.9. Derecho comparado.

Considero que sería oportuno tomar en cuenta lo que otros países ya han hecho en lo que respecta a esta materia y que consagran en sus Constituciones como derechos fundamentales de manera expresa el derecho a la intimidad, al honor y a la propia imagen. Entre ellos podemos encontrar a Alemania, Austria, Finlandia, Portugal, Suecia y España.

ALEMANIA La Constitución alemana de 1949 en su artículo 5° manifiesta que los derechos de libertad de expresión, de prensa y de información no tendrán más límites que los preceptos de las leyes generales y las disposiciones legales para los menores y el derecho al honor personal.

AUSTRIA La Ley Constitucional austriaca sobre la protección de la libertad personal de 1988 establece que todos tendrán derecho de expresar su pensamiento pero dentro de los límites legales (artículo 13).

FINLANDIA El instrumento de gobierno de Finlandia de 1919 establece en su artículo 8 que se garantiza a todos la intimidad, el honor personal y la inviolabilidad del domicilio y que habrá una ley que establecerá normas a detalle sobre la salvaguardia de los datos de carácter personal. Dicho numeral también establece que será inviolable el secreto de la correspondencia y de las comunicaciones telefónicas y cualquier otro tipo de comunicaciones confidenciales. Por su parte, él articulo 10 que establece que todos gozarán de libertad de expresión y que la ley determinará normas sobre el desarrollo de dicha libertad de expresión pudiéndose establecer por la misma, además, las limitaciones necesarias para la protección de la infancia.

PORTUGAL Por su parte la Constitución de la República portuguesa establece en su artículo 34 la inviolabilidad del domicilio y de su correspondencia y demás medios de comunicación privada, y en el artículo 35 prevé de manera detallada reglas sobre la utilización de la informática, como son el que todo ciudadano tendrá derechos a tener conocimiento de lo que conste en forma de registros informáticos acerca de él y de la finalidad a que se destinan estos datos y podrá exigir su rectificación y actualización; Prohíbe el acceso a ficheros y registros informáticos para el conocimiento de datos personales referentes a terceros, prohíbe también la utilización de la informática para el tratamiento de datos referentes a convicciones filosóficas o políticas, afiliación a partidos o a sindicatos, fe religiosa o vida privada, salvo si se trata de datos estadísticos no identificables individualmente. Por otra parte, el artículo 37 relativo a la libertad de

expresión y de información señala que existirá completa libertad para expresar el pensamiento por diversos medios así como el derecho de informar, informarse y ser informados sin impedimentos ni discriminaciones pero que las infracciones que se cometan en el ejercicio de estos derechos quedarán sometidas a los principios del derecho penal y su apreciación competerá a los tribunales judiciales. También en este artículo se asegura a cualquier persona individual o colectiva en condiciones de igualdad y de eficacia el derecho de réplica y de rectificación, así como el derecho de indemnización por daños y perjuicios.

SUECIA La ley de 1994 que reforma el Instrumento de Gobierno de Suecia establece en su capítulo segundo, artículo 1° que todo ciudadano tendrá libertad de expresión y de información y que en lo que se refiere a la libertad de prensa y de expresión por radiodifusión, televisión y cualesquiera otros medios análogos estarán regidos por la ley de libertad de prensa y por la ley fundamental de libertad de expresión. Mientras que el artículo 13 establece que podrán limitarse la libertad de expresión y de información en atención a la seguridad del Reino, al abastecimiento de la población, orden y seguridad públicos, a la reputación de las personas, a la intimidad de la vida privada, o a la prevención y persecución de delitos.

ESPAÑA Por último considero muy interesante y quizás hasta un modelo a seguir por nosotros el artículo 18 de la Constitución española de 1978 que establece que se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen, así como también a la inviolabilidad del domicilio, el secreto de las comunicaciones de todo tipo y en especial a las postales, telegráficas y telefónicas y que la ley limitará el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Y el artículo 20 de la misma Constitución española reconoce y protege los derechos de expresión y difusión libre de pensamientos, ideas y opiniones por cualquier medio así como la libertad de información establece que dichas libertades tienen su límite en el respeto a los derechos reconocidos por la propia constitución y en las leyes que los desarrollan y específicamente consagra como límite de éstas, el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia.

ESTADOS UNIDOS También resulta importante mencionar lo que en los Estados Unidos de América se ha llamado el "derecho a ser dejado en paz" o "a ser dejado solo" (therightto be letalone), que se refiere a un derecho a la privacidad consistente en no estar obligado a participar en la vida colectiva y por tanto, el poder permanecer aislado de la comunidad sin establecer relaciones y que implica también el permanecer en el anonimato, el ser dejado en paz sin ser molestado y el no sufrir intromisiones en la soledad física que la persona reserva sólo para sí misma.

Atento a todo lo anterior, considero que sería muy importante incluir en nuestro texto constitucional de manera expresa como garantía individual el derecho a la intimidad personal y familiar y el respeto al honor y a la propia imagen contra actos no sólo de las propias autoridades sino también de otros particulares que en el ejercicio indebido y excesivo de sus derechos y libertad de expresión e información pudieran transgredir esos derechos fundamentales relativos a la vida privada.

De igual forma considero que es necesaria la creación de una ley o conjunto de éstas que regulen de manera clara y objetiva los límites de estos derechos estableciendo de manera puntual lo que se

considera vida pública y vida privada, que regulen de forma completa todo lo relativo a la recopilación, manejo, uso e información de datos sensibles (entendiendo por estos todos aquellos que revelen cuestiones de origen racial, étnico, opiniones y preferencias políticas, convicciones religiosas, filosóficas o morales, afiliaciones partidistas o sindicales, cuestiones de salud, vida sexual, etc.), inviolabilidad de comunicaciones de todo tipo (por vía verbal directa, escrita, telefónica, telegráfica, postal, electrónica, etc.), estableciendo las sanciones correspondientes por vulnerar dichos derechos y fijando de manera precisa el procedimiento para la Reparación del daño causado y las medidas necesarias para restituir al afectado en su imagen y reputación.

Deberán establecerse, a su vez, en legislación secundaria los procedimientos para que mediante la acción de habeas data o de "protección de datos personales" se le dé a conocer a la persona la información que sobre ella se encuentre en archivos, registros o bancos de datos públicos o privados y la finalidad de estos, así como también para que la persona pueda exigir su rectificación, actualización, inclusión, complementación, reserva, suspensión o cancelación (cabe señalar que al respecto existe ya una iniciativa presentada el 14 de febrero de 2001 ante la Comisión Permanente sobre una Ley Federal de Protección de Datos Personales que actualmente se encuentra en análisis y que sería oportuna su aprobación).

Por último es preciso señalar algunas de las interrogantes pendientes por resolver y que esta temática provoca y que por tanto deberán de estudiarse por los juristas, profesionales de los medios de información y sociedad en general para aportar soluciones que redunden en beneficio tanto del individuo en lo personal como de la sociedad en general.

2.2.3. FORMAS DE VULNERACION AL DERECHO A LA INTIMIDAD.

Este es uno de los temas más importantes del derecho a la intimidad, pues se va describir, según los autores, cuales son los medios o la forma de atacar al derecho a la intimidad.

Antes de mencionar a los autores, se va a considerar en primer lugar a La Conferencia de Juristas Nórdicos (realizada en Estocolmo en mayo de 1967) que no solo se refirió a determinar el concepto de derecho a la intimidad, sino también a los diversos modos que existen en el mundo que afectan a los derechos a la intimidad: El derecho al respecto de la vida privada, es el derecho de una persona a ser dejado en paz para vivir su propia vida, con el mínimo de injerencias exteriores, protegiendo frente:

a) Toda injerencia en la vida privada, familiar domestica.

b) Todo ataque a la integridad física o mental o a la libertad moral o intelectual.

c) Todo ataque al honor o a la reputación.

d) Toda interpretación perjudicial dada a sus palabras o a sus actos.

e).-La utilización del nombre, identidad o imagen de una persona.

f).-La divulgación necesaria de hechos embarazosos referentes a la vida privada.

g).-Toda actividad tendiente a espiar, vigilar o acosar a una persona.

h).- La interceptación de la correspondencia.

i).-La utilización maliciosa de las comunicaciones privadas, escritas u orales.

j).-La divulgación de información comunicadas o recibidas bajo el secreto profesional.

"En la práctica, la definición arriba mencionada comprende los casos siguientes:

a) El registro de una persona.
b).La violación y el registro del domicilio o de otros locales.
c).Los exámenes médicos obligatorios, físicos o sicológicos.
d).Las declaraciones molestas, falsas o irrelevantes a una persona.
e).La interceptación de la correspondencia.
f).La captación de los mensajes telefónicos o telegráficos.
g).La utilización de aparatos electrónicos para la vigilancia.
h).La grabación sonora y la toma de fotografías de películas.
i).El acoso por los periodistas y otros representantes de los medios de comunicación oral.
j).La divulgación publica de hechos referentes a la vida privada.
k).La divulgación de informaciones comunicadas o recibidas por consejeros profesionales o entregadasa autoridades públicas obligadas al secreto.
l).El caos de una persona, por ejemplo, vigilándola, siguiéndola o molestándola con llamadas telefónicas"[84] .

Por otro lado Prosser, dice que el right of privacy norteamericano considera como medios de ataque al a intimidad lo siguiente:

1. Actos de intrusión que perturban el retiro o soledad del individuo.
2. Divulgación publica de hechos privados embarazosos sobre el individuo.
3. Publicidad que coloca al individuo bajo una luz falsa ante el público.
4. Apropiación de la imagen o identidad de una persona para derivar algún beneficio[85].

[84]**EGUIGUREN PRAELI,** Francisco. La Libertad de expresión e información y el derecho a la intimidad personal. 1°. Ed, Lima, Palestra 2004, P. 100.

Uno de los autores que ha desarrollado este tema con profundidad es Luís Fariñas Mantoni[86], para él, ataca al derecho a la intimidad, es una lesión a la dignidad, cuya acción no puede estar permitida ni por la sociedad, Estado y por último el derecho. Luís Fariñas no solo se encargo de determinar cuáles son los instrumentos que se utilizan para atacar a este derecho, sino también de considerar al propio individuo como actuante de la agresión a este derecho.

Según Luís fariñas se puede atacar el derecho a la intimidad a través de los siguientes medios:

***1º** La actividad de "Eavesdropping" o ser un "Peeping Ton"*

Se refiere al a acción realizada por una persona de escucha tras la puerta con el fin de conocer la información que los otros comentan.

***2º** El allanamiento de Morada*

Se refiere al derecho de la inviolabilidad de domicilio, porque es en hogar donde el hombre descansa, reposa, desarrolla una parte de su vida. En este caso existe un claro ejemplo, el concurso del gran Hermano que lo transmite por ATV o la Casa de Gissela, concursos que muestran a los televidentes la intimidad de los concursantes.

***3º** Violación Postales y de otros Tipos de comunicación. Referencia especial al problema de las escuchas telefónicas.*

Se refiere que es el hombre tiene derechos a comunicarse, uno de los medios más frecuentes que se utiliza es la carta. Ya que en el

---

[85]**FARIÑAS MANTONI,**Luís Mario. Derecho al intimidad. 1º. Ed, Madrid. Ed. Trivium, 1983, P. 5

[86]Ibidem. Pág. 7

contenido de su correspondencia está relacionado con los temas íntimos de la persona.

El Teléfono es otro medio para comunicarse, pero muchas personas lo utilizan con el fin de molestar o espiar.

4º*Tests Psicológico, Polígrafo, análisis de sangre; aliento u orina, huellas digitales*

Se refiere a que los psicólogos o los terapéuticos, deben tener mucho cuidado al momento de realizarse ciertas preguntas sobre la interioridad de la persona, porque el paciente tiene derecho a la intimidad y a veces la revelación de un secreto le puede afectar a él mismo o sus familiares. Respecto al polígrafo conocido como detector de mentiras, es un aparato que consiste en determinar la culpabilidad del individuo, pues este manifiesta una repuesta involuntaria a las preguntas que se realiza, y se le detecta a través de las vibraciones del a piel. En el caso de los exámenes de sangre, orina y aliento solo puede ser permitidos por medios de una orden judicial.

5º *El Narcoanálisis*

Consiste en el empleo de una sustancia o narcótico, para provocar un estado de somnolencia llamado "Sueño Hipnótico" o "Transe hipnótico", este sustancial es frecuente utilizando por los psiquiatras para analizar el subconsciente del paciente.

6º *Lavados cerebrales, torturas indagatorias, hipnotismo, publicidad subliminal.*

El lavado del cerebro consiste en descubrir absolutamente todo respecto a la bibliografía y la intimidad de la persona.

Respecto a la tortura consiste no solo en el maltrato físico sino también psicológico, el en hipnotismo es muy importante el consentimiento de la persona a quien se le va ha realizar y consiste en colocar al sujeto en un estado de sueño temporal.

7º Aparatos e ingenios diversos.

Se refiere a todos los aparatos tecnológicos e ingeniosos, ejemplos, aparatos fotográficos miniaturizados, micrófonos prácticamente invisibles, etc. Además lo clasifica en dos grupos:

A).- Auditivos (el sonido) Son los siguientes: micrófonos tamaño de un alfiler para colocarlos dentro de la bocina del teléfono, dispositivos de microondas, técnicas de láser, micro balas que se disparan contra la ventana para que queden pegadas y se pueda escuchar la conversación dentro de la habitación, sistemas micro balas con interruptores operables por control remoto, micrófonos magnéticos que no se necesitan corriente eléctrica, micrófonos parabólico o de escopeta que pueden captar conversaciones a 150m, etc.
B).- Visuales (capta imágenes) las divide en dos grupos:

Para observación: Son las siguientes, lentes miniaturizadas, ventanas polarizadas, telescopio potente.

Para filmación o grabación: Son los siguientes: cámaras escondidas, fotografías, filmadoras.

Respecto al individuo como propio agresor a este derecho Luís Fariñas[87], "realiza una enumeración de las cuales solo he considerado las siguientes:

1º El cónyuge:
La familia está formado por la pareja, cual vive en la misma casa y por esa razón ambas personas da a descubrir ciertas situaciones intimas, pero eso no significa que la persona de a conocer su vida privada entera. Siempre tiene que tener un espacio para el mismo.

2º Parientes o Familiares:
Consiste en la familia nuclear, que está conformado por padres e hijos y donde estos últimos están sometidos a la patria potestad. Pero la tutela de las padres solo es vigente hasta los 18 años que tenga el hijo, es decir a partir de esa edad el sujeto puede mantener información que no es obligatoria que los comente a sus padres, respecto al menor de edad, el autor manifiesta que aun no tiene la madurez para tener capacidad de ejercer este derecho.

3º Vecino:
Es cierto que se mantiene una relación con el vecino, sobre todo cuando existen interese en común, sin embargo muchas veces los vecinos pueden violar nuestro derecho al a intimidad a través del Peeping ton, sino también pueden propagar información que puede ser verdadera o falsa sobre el titular de dicha información que puede causar un daño a su dignidad.

4º el amigo:
Existe una relación de confianza, donde muchas veces la persona se refugia cuando se encuentra en problemas, sin embargo

[87]**FARIÑAS MANTONI**,*Luís Mario*. Derecho al intimidad. 1º. Ed, Madrid. Ed. Trivium, 1983, Pág. 10

muchas veces el amigo puede traicionarlo haciendo público una información que afecte a la persona que le ha proporcionado esta.

5º El compañero de trabajo:
Tanto el superior como el designado pueden ser sujeto activo y pasivo viceversa de atentados contra la intimidad.

6º El Extraño:
Es cualquier persona que puede intervenir en la vida privada de otro.

Tanto la Conferencia de los Nórdicos, como los autores, han descrito a su criterio cuales son los medios que existen para tacar al derecho a la intimidad, por lo cual puede llegar a la siguiente conclusión:

a) En primer lugar que el hombre es el agresor principal hacia este derecho.

b) Uno de los medios que se ha convertido actualmente como el mayor agresor al derecho a la intimidad, son los instrumentos tecnológicos que el hombre no solo la utiliza, sino que a través de su desarrollo, lo ha ido perfeccionando cada vez más. Ejemplo de ellos son: las cámaras miniaturas, los micrófonos que son tamaño de una aguja que se coloca en la bocina del teléfono, filmaciones, lentes miniaturas; es decir todos los aparatos que solo necesite manejarse con control remoto y que se puede hacer desde largas distancias, donde nos es necesarios que la persona esté presente físicamente o lo realiza ella misma con sus propias manos.

c) El otro medio, es donde la persona actúa físicamente, es decir donde no utiliza ni un medio tecnológico para atacar el derecho a la

intimidad. Ejemplo, escuchar tras de las puertas, revisar la correspondencia, divulgar un hechos o situación, revisar los registros de las personas, exámenes médicos, los psicólogos, los médicos que propagan la información de su paciente, respecto a este punto podemos tomar como ejemplo el caso de María Julia Matilla (Miss Mundo), con el doctor Morillas, donde el doctor no respeto el contrato que realizo con la paciente, pues mostró algunas fotos en que la Miss mundo aparecía antes de sus supuestas operaciones, etc.

Pero sea los diversos medios o formas mencionadas en líneas anteriores, ninguna persona, entidad pública o privada, tiene la facultad de violar este derecho, porque es inherente al hombre, es donde se determina su personalidad que va permitir desarrollarse y aportar cada vez más a la sociedad".

2.2.4. DETERMINACIÓN DE LA PENA.

Antecedentes.

"La imposición de las penas y medidas de seguridad durante la larga trayectoria de la vida humana, ha tenido diversidad de aplicaciones, en los tiempos primitivos se imponían con tanta barbarie, recordemos que esta se inicia con la venganza privada, después la ley del Talión, posteriormente en el periodo humanitario, encontramos que se trata de eliminar a la dureza de la pena, tratando de hacer un estudio del delincuente para saber el porqué del crimen y de esta forma llevarlo a su readaptación. El antecedente inmediato es el art. 51 del CP de 1924, según el cual: «Para la aplicación de la pena los jueces apreciarán la culpabilidad y el peligro del agente, teniendo en cuenta las siguientes

circunstancias, en cuanto la ley no las considere especialmente como constitutivas o modificatorias del delito"[88]:

"1° La naturaleza de la acción; el tiempo en que se perpetró y el que hubiere transcurrido desde entonces; el lugar, los instrumentos y los medios en que se hubiere hecho uso; la preparación tranquila o la perpetración ocasional; el modo de ejecución y las circunstancias en que ésta se hubiere efectuado; la unidad o la pluralidad de agentes; el número y la importancia o especialidad de los deberes infringidos; la dificultad que hubiere para prevenirse contra el hecho punible; y la extensión del daño y del peligro causados. 2° La edad, la educación, la vida personal, familiar y social del sujeto anterior y posterior al delito, su situación económica, sus precedentes judiciales y penales, la calidad de los móviles honorables o excusables o innobles o fútiles que lo determinaron a delinquir, las emociones que lo hubieran agitado, su participación mayor o menor en el delito, la reparación espontánea que hubiere hecho del daño, o la confesión sincera antes de haber sido descubierto, y los demás antecedentes, condiciones personales y circunstancias que conduzcan al conocimiento de su carácter"[89].

Criterios básicos de determinación.

Los criterios básicos que orientan la determinación concreta de la pena son de tres órdenes:

[88]**CARO CORIA**Dino Carlos Notas sobre la individualización judicial de la pena en el código penal peruano penales. penal. Vol. I. 2ª ed. Lima, Grijley 2003, pp. 112
[89] Ibídem.

a. El criterio de la culpabilidad.

Sirve la culpabilidad para fundamentar y limitar la pena. Es un logro garantista pues, mitiga (excluye) criterios de "peligrosidad", "personalidad" o "responsabilidad del carácter"

b. El criterio preventivo general.

Es importante la estabilidad de la norma. La contingencia aversiva en que consiste la pena viabiliza la tesis llegada al ciudadano de que el Derecho penal objetivo, es uno de advertencia.

La pena cumplirá un papel instructivo conforme las propuestas del aprendizaje observacional o vicario del que ya hemos dado cuenta. Se activa en el ciudadano el sentido de la "poena" ya condicionada en él por lo de la "poenanaturalis"

Bustos Ramírez señala que "la pena es autoconstantacion de Estado (protección de su sistema, por eso en definitiva protección de los bienes jurídicos) y finalidad al imponerse, es buscar alternativas de dignificación del sujeto de aumentar su capacidad de libertad, de ser actor socia[90]l".

c. Objetivo preventivo especial

Al imponerse la pena, ella tomara en cuenta las necesidades de reeducación o resocialización del infractor.

Esto es de la resocialización sin deberá tener contenido concreto conforme el que se deriva de las modernas teorías del aprendizaje

---

[90]**BUSTOS RAMÍREZ**Juan *Manual de Derecho Penal* Barcelona Editorial Ariel. 1989. p.395.

y de los hallazgos experimentales en materia de comportamiento humano.

Marco legal de determinación de la pena.

El marco legal de la determinación judicial de la pena en el Perú se encuentra disperso en el código penal.

Encontramos cuatro tipos de normas:

1. Los principios rectores del título preliminar.
2. Los criterios de fundamentación y determinación (artículo 45°)
3. Las circunstancias genéricas y específicas (artículos 46°, 186°, 189°, 297°, etc.)
4. Las circunstancias cualificadas o privilegiadas (artículos 21°, 22°, 46° a, 46° b, 46° c, etc.)

Criterios para la determinación de la pena.

Artículo 45.

El Juez, al momento de fundamentar y determinar la pena, deberá tener en cuenta:

1. Las carencias sociales que hubiere sufrido el agente;

Ejemplo.
Teniendo en cuenta que la procesada por el delito de hurto, del establecimiento abierto al publico, sustrajo bienes perecibles, lo cuales ha demostrado fue para consumo, de su familia, resaltando las carencias sociales del agente.

2. Su cultura y sus costumbres; y

Ejemplo.

La gravedad de la pena debe estar determinada por la trascendencia social de los hechos que con ella se reprimen, de allí que resulte imprescindible la valoración de la nocividad del ataque al bien jurídico que para los efectos de las graduaciones debe tener en cuenta la forma y las circunstancias que ocurrieron.

Así teniendo en cuenta que las rondas campesinas tienen una normatividad consuetudinaria, y el castigo corporal realizado al que falto de la moral de la comunidad no puede ser considerada como lesiones, hay que tener las costumbres ancestrales de la comunidad.

3. Los intereses de la víctima, de su familia o de las personas que de ella dependen.

Ejemplo.

Respecto a la reparación civil, a SEISCIENTOS NUEVOS SOLES a favor de los intereses de la víctima, esta acorde con los daños y perjuicios ocasionados por lo procesados.

La edad, la educación, situación económica y medio social. Se considera como criterio de fundamentación y determinación de la pena que el Juez atienda las carencias sociales que hubiere sufrido el agente. Por Tanto, el órgano jurisdiccional debe incluir también en la valoración de estas circunstancias las posibilidades reales de interacción e integración que ha tenido el agente en su entorno social y con los patrones de conducta positiva imperantes en el.

Como señala Villa Stein "los criterios que se tomaran en cuenta para la determinación de la pena correspondiente al caso concreto, según las circunstancias del hecho, la culpabilidad del autor, y la función de la pena[91]"

"Como quiera que sea el Juez el llamado a precisar la pena sin apartarse de lo que la ley dice al respecto, el legislador ha establecido ciertas reglas que se deberán tomar en consideración al momento de fundamentar e imponer la pena"[92].

La dualidad expuesta en la descripción legal, significa para Hurtado Pozo que "En el art. 45, se trata del "momento de fundamentar y determinar la pena" y, en el art. 46, del momento de "determinar la pena dentro de los límites fijados por la ley". (...). Podría pensarse que la fundamentación indicada en el art. 45 no se refiere a la cuantificación de la pena (regulada en el art. 46), sino más bien a su selección a otro nivel: preferir la pena de prestación de servicios a la comunidad o la de multa a la privativa de la libertad; o la de decidir si conviene suspender la ejecución de la pena o convertirla en otra. Si este fuere el objetivo del art. 45, resultaría superfluo porque el legislador ha previsto las condiciones que el juez debe constatar para optar por una de estas alternativas"[93].

De modo similar, para Velásquez Velásquez "los arts. 45 y 46 del CP parecen referirse, respectivamente, al ámbito de la IJP en sentido amplio y a la IJP en sentido estricto. A su juicio, el

---

[91] **VILLA STEIN** Javier *Derecho Penal Parte General.* Lima Editorial San Marcos. 1998. p. 497.
[92] Ibídem.
[93] **HURTADO POZO**, José. Responsabilidad y culpabilidad. En: ADP 1993, p. 56.

contenido del art. 45 del CP enfrenta al intérprete ante dos previsiones distintas: de un lado, emplea los conceptos de fundamentación y de determinación de la pena —como una noción diversa a la de determinación de la pena "dentro de los límites fijados por la ley", consagrada en el art. 46—, y de otra parte señala tres criterios genéricos para que el funcionario judicial cumpla con dichas tareas: las carencias sociales sufridas por el agente; su cultura y costumbres; y los intereses de la víctima, de su familia, o de quienes dependen de ella. Más específicamente, entiende Velásquez que el sentido de la determinación de la pena en el art. 45 se refiere a todas las cuestiones relativas a la imposición y ejecución de la sanción penal, como las atinentes a los fenómenos de la condena condicional, la reserva del fallo condenatorio, la conversión de la pena privativa de libertad no mayor de dos años en pena de multa, o la conversión de la pena de multa no pagada en pena privativa de libertad, así como la fijación de plazos para el pago de la multa, etc.; esto es, se parte de una noción amplia de tal figura. El art. 45 no se refiere en consecuencias a la noción estricta utilizada por el art. 46, al tenor de la cual se entiende por determinación de la pena la operación mental mediante la cual el Juez, en concreto, una vez examinadas las diversas categorías del hecho punible, fija, precisa, señala cuales son las sanciones imponibles al trasgresor de la ley penal; esto es, la determinación de la pena dentro del marco punitivo, acorde con la culpabilidad por el hecho"[94].

"Esta interpretación conduce a presentar el contenido de los arts. 45 y 46 del CP como tributarios del modelo de la teoría del valor relativo de empleo"[95].

---

[94]**VELÁSQUEZ VELÁSQUEZ**, Fernando. Los criterios de determinación de la pena en el CP peruano de 1991. Ponencia presentada el 21 de agosto de 2000 en la PUCP, pp. 910.
[95]Ibid., nota 50.

"Con ello debiera estimarse que la fijación de la pena dentro del marco penal establecido por el legislador, la LJP en sentido estricto, se fundamenta en la culpabilidad del autor. En efecto, el art. 46 señala que el Juez atenderá a la «responsabilidad y gravedad del hecho punible cometido», en concordancia con el principio de prohibición de doble valoración o de inherencia («en cuanto no sean específicamente constitutivas del hecho punible o modificatorias de la responsabilidad ») y conforme a los criterios previstos en los nums. 1 al 11. En ese contexto, la referencia a la «responsabilidad» no se vincula a la responsabilidad penal por la comisión de un injusto culpable, sino al grado de culpabilidad del autor (responsabilidad en sentido estricto)"[96].

"Mientras que la mención a la «gravedad del hecho punible» tendría que estar referida a los elementos del injusto graduable[97].

"De esa forma, el art. 46 establecería dos pautas genéricas de tasación de la pena, el grado de injusto y el grado de culpabilidad. Con ello, los referentes previstos en los nums. 1 al 11 del art. 46 deben valorarse bien como criterios vinculados al grado del injusto o al grado de culpabilidad"[98]. "Aunque tales notas son «propias de un derecho penal orientado hacia la retribución entendida como límite al ejercicio del iuspuniendi del Estado, acorde con los principios del acto, de protección de bienes jurídicos, de culpabilidad y de proporcionalidad», retribución que no sólo se estima incompatible con la Constitución sino además ajena al sentido de los arts. IX y I del CP que establecen una orientación preventiva de la pena y la legislación"[99].

---

[96]**HURTADO POZO**, José. «Responsabilidad y culpabilidad», cit., pp. 53, 54.
[97]**BRAMONT ARIAS**, Luís, *Manual de Derecho Penal* Lima, San Marcos 2002, p. 248.
[98]**VELÁSQUEZ VELÁSQUEZ**, Ob. cit., p. 14.
[99]**CASTILLO ALVA**, José Luís. En: Código Penal comentado. T. I. Lima, Gaceta Jurídica 2004, p. 35.

Individualización de la Pena.

Artículo 46.

Para determinar la pena dentro de los límites fijados por la ley, el Juez atenderá la responsabilidad y gravedad del hecho punible cometido, en cuanto no sean específicamente constitutivas del hecho punible o modificatorio de la responsabilidad, considerando especialmente:

1. La naturaleza de la acción;
2. Los medios empleados;
3. La importancia de los deberes infringidos;
4. La extensión del daño o peligro causados;
5. Las circunstancias de tiempo, lugar, modo y ocasión;
6. Los móviles y fines;
7. La unidad o pluralidad de los agentes;
8. La edad, educación, situación económica y medio social;
9. La reparación espontánea que hubiere hecho del daño;
10. La confesión sincera antes de haber sido descubierto; y
11. Las condiciones personales y circunstancias que lleven al conocimiento el agente.

El Juez debe tomar conocimiento directo del agente y, en cuanto sea posible o útil, de la víctima.

Las condiciones personalesy circunstancias que llevan al conocimiento del agente. El carácter enunciativo del artículo 46° se complementa con la amplitud circunstancial que la ley le concede al juez, efectivamente el tiene, además una opción innominada y abierta para interpretar y apreciar otras circunstancias, distintas de las expresamente identificadas por cada inciso precedente de

dicha disposición legal. Ahora, para evitar contradicciones con el principio de legalidad o riesgos de arbitrariedad, el Juez deberá especificar en concreto la circunstancia que invoca y su equivalencia con las reguladas.

Debe fundamentar razonablemente como es que tal circunstancia resulta idónea para definir un perfil que permite conocer mejor la personalidaddel agente.

2.2.5. MEDIOS PROBATORIOS EN EL PROCESO PENAL.

Sánchez Velarde señala que "la prueba que sea validamente incorporada y valorada en el proceso penal debe ser licita, obtenida de acuerdo con la constitución y las leyes merecedora del valor de la autoridad jurisdiccional le asignen y de allí que bajo el marco del rigor constitucional, se repute de válida cualquier ordenamiento jurídico, ya que partimos con la idea básica que la finalidad del proceso penal, conformada por la búsqueda de la verdad, no es un fin absoluto, sino que posee un limite; el respeto de los derechos fundamentales de la persona"[100].

La prueba ilícita es aquella prueba obtenida o practicada con violación de los derechos fundamentales.

Se debe entender por prueba ilícita aquella que es obtenida o practicada con violación de derechos fundamentales, de modo que la misma deviene procesalmente inefectiva e inutilizable; como se induce de lo expresado - desde ésta concepción - cualquier infracción procesal (prueba irregular) tendrá otra consecuencia jurídica, se podría hablar de nulidad o subsanación, dependiendo de la gravedad de la infracción procesal., es por ello, la razón de

[100]**SÁNCHEZ VELARDE** Pablo *El Nuevo Proceso Penal* Lima Editorial Idemsa. 2009. p. 237.

éste trabajo que trata de traer a la discusión de que es de todo válido en el proceso penal restringir "derechos fundamentales" (grado válido de intervención) pero no se puede vulnerar o violentar a éstos (grado inconstitucional de intervención), en éste último supuesto estaríamos en los casos de "prueba ilícita" , en los otros - según el caso - se trataría de "prueba ilegal", "prueba irregular" entre otros adjetivos que puedan recibir en la doctrina.

En el 2003, el Tribunal Constitucional nacional definió la prueba ilícita en los siguientes términos: *"La prueba ilícita es aquella en cuya obtención o actuación se lesionan derechos fundamentales o se viola la legalidad procesal, de modo que la misma deviene procesalmente inefectiva e inutilizable*[101]*"*

En esta sentencia podemos apreciar que el Tribuna Constitucional ha optado por una concepción moderadamente amplia ya que considera ilícitos los medios probatorios obtenidos o actuados en violación de una norma constitucional o trasgrediendo la ley procesal. Consideramos que esta posición puede resultar demasiado amplia para los fines de la institución, por cuanto si bien dentro de las normas procesales existen normas que son garantías de un debido proceso, también dentro de ellas existen normas que son meramente formales cuya violación no importa una alteración seria al debido proceso.

En tal sentido, consideramos que el máximo intérprete de la constitución debería modificar ligeramente la jurisprudencia sentada, señalando que constituyen prueba ilícita aquellas obtenidas o presentadas en violación de normas constitucionales o en trasgresión de normas procesales que constituyan garantías de debido proceso para el procesado.

---

[101] Tribunal Constitucional: Exp. N° 2053-2003-HC/TC, sentencia del 15 de septiembre del 2003

LEGITIMIDAD DE LA PRUEBA.

Nuevo Código Procesal Penal en su Título Preliminar:

"Artículo VIII.- Legitimidad de la Prueba

Todo medio de prueba será valorado sólo si ha sido obtenido e incorporado al proceso por un procedimiento constitucionalmente legítimo.

Carecen de efecto legal las pruebas obtenidas, directa o indirectamente, con violación del contenido esencial de los derechos fundamentales de la persona.

La inobservancia de cualquier regla de garantía constitucional establecida a favor del procesado no podrá hacerse valer en su perjuicio."

Consideramos que la mención que el inciso 2 del citado artículo hace sobre "pruebas obtenidas, directa o indirectamente, con violación del contenido esencial de los derechos fundamentales" incluye dentro del concepto de prueba ilícita a las obtenidas en violación de las normas procesales que consagren garantías para el procesado

A tal concepto debemos agregar el de las pruebas ilícitas por derivación, es decir aquella que habiendo sido obtenidas o practicadas de forma legal, son inadmisibles debido al carácter ilícito del medio probatorio que les dio origen. Esta es la conocida teoría de los ***"frutos del árbol envenenado"***, cuyo origen se encuentra en la jurisprudencia de la Suprema Corte de los Estados Unidos.

Búsqueda de pruebas y restricción de derechos en particular.

La descripción de este tipo de pruebas que restringen derechos fundamentales está descrita en el N.C.P.P. precedido de preceptos generales y se efectúa en casos necesarios para lograr los fines de esclarecimiento del proceso, debiendo procederse conforme a lo dispuesto por la Ley y ejecutarse con las debidas garantías para el afectado. Estas pruebas son:

1. El control de identidad policial
2. La Vídeo vigilancia

Sánchez Velarde[102] señala que algunas de las medidas son nuevas y quizás por ello resulten de difícil aceptación, por la restricción de derechos que implica, sin embargo, se confía en la comprensión ciudadana en atención a los fines que se persiguen.

"El código recoge medidas que no requieren autorización judicial, tales como: el control de identidad policial, video vigilancia y las pesquisas, aquellas que si necesitan autorización judicial, entre las cuales están: la intervención corporal (que también puede ser dispuesta por el Fiscal, cuando medie la urgencia y el peligro en la demora) el allanamiento (fuera de los casos de flagrancia), la exhibición forzosa, la incautación, el control de comunicaciones y documentos privados, la intervención de comunicaciones y telecomunicaciones, aseguramiento e incautación de documentos privados, el levantamiento del secreto bancario y de la reserva tributaria, la clausura o vigilancia de locales e inmovilización"[103].

[102]**SÁNCHEZ VELARDE** Pablo Ob Cit. p. 287.
[103]Ibidem.

VIDEO VIGILANCIA

"La captación de imágenes y sonidos a través de videocámaras proporcionan datos personales que son fuente de información personal. Esta Directiva tiene como objeto de protección el derecho a la intimidad y la vida privada de las personas, así como sus datos personales"[104].

Las videocámaras ayudan a prevenir y a probar comportamientos delictivos y es por esto por lo que su empleo se regula como mecanismo de política criminal, pues se postula su uso como instrumento eficaz en la prevención y persecución del delito y para el mantenimiento de la seguridad ciudadana.

Ciertamente, el video vigilancia plantea numerosos problemas, pero también reporta indudables beneficios, por lo que nos encontramos ante la necesidad de equilibrar unos y otros, intentando que primen los segundos. En el lado de las ventajas se encuentran los fines que justifican su utilización por el Estado y en el de los problemas, los ya sabidos: la proliferación incontrolada de instalación de cámaras, muchas de ellas con fines privados sin contar con una regulación adecuada, el control de los ciudadanos con el consiguiente efecto aparejado de inhibición en lo que respecta a su comportamiento social, y, como a nadie se le escapa, la posibilidad de recopilar, almacenar y transmitir informaciones personales de forma ilimitada.
La conclusión de todo ello es la sensación de control total a la que estamos sometidos, un controlo vigilancia que nosotros no podemos controlar, y que, indudablemente, repercute en nuestros derechos y libertades fundamentales.

---

[104] **ABA CATORIA** Ana La video vigilancia y la garantía de los derechos individuales: su marco jurídico. Madrid. 2009. p. 48

En algunos países se han desarrollado disposiciones específicas relativas a la vigilancia por videocámaras con independencia de que ésta implique el tratamiento de datos personales. Así, existe una legislación específica que regula su implantación y utilización para captar imágenes y sonidos de las personas al margen de que haya una legislación específica de protección de datos personales, en la que, lógicamente, se regula el tratamiento de los datos que constituyen la imagen y sonidos. En otros países, la vigilancia por videocámaras no es objeto de legislación específica y las autoridades de protección de datos se afanan en garantizar la adecuada aplicación de las disposiciones generales de protección de datos a este ámbito.

En el DERECHO ESPAÑOL, el carácter sensible de los datos constituidos por la imagen y sonidos relativos a las personas físicas se pone de relieve en los Considerandos de la Directiva 95/46/C y en determinados artículos de la misma. Así, en el Considerando 14 se señala que la Directiva resulta aplicable en este ámbito por la importancia del desarrollo de las técnicas utilizadas para captar, manejar y utilizar los datos personales obtenidos a través de ellas. En este sentido, los principios de protección de datos que en ella se establecen resultan aplicables a toda información, incluida la referente a la imagen y sonido, relativa a personas identificadas o identificables, teniendo en cuenta los medios que puedan ser utilizados por el responsable del tratamiento u otra persona para identificar a aquella (art.2.a y el Considerando 26).
Así, las disposiciones aplicables son:

Calidad de los datos, que obliga a que las imágenes sean tratadas de manera leal y lícita, destinándose a fines determinados, explícitos y legítimos. En este orden de cosas, los datos deben ser

adecuados, pertinentes y no excesivos, no permitiéndose que se traten posteriormente de manera incompatible con dichos fines (art.6).

Principios relativos a la legitimación del tratamiento de datos: el tratamiento de los datos personales mediante vigilancia por videocámara ha de cumplir alguno de los requisitos establecidos en el art.7: consentimiento inequívoco, necesidad de obligaciones contractuales, necesidad de cumplimiento de obligaciones jurídicas, protección del interés vital del afectado, cumplimiento de intereses públicos, etc.

Los datos especialmente protegidos, con arreglo al art.8 presentan especialidades en su tratamiento.

La información que obligatoriamente se ha de facilitar al interesado (arts.1 y 11).

Los derechos de acceso, rectificación y cancelación y aquellos otros como el de oposición al tratamiento por razones legítimas (art.12.a y art.14).

Garantías aplicables en relación con las decisiones individuales automatizadas (art.15). Seguridad de las operaciones del tratamiento (art.17).
Notificación de las operaciones de tratamiento (arts.18 y 19).
Controles previos de las operaciones de tratamiento que puedan presentar riesgos específicos para los derechos y libertades del interesado (art.20).

Transferencia de datos a terceros países (art.25 y ss.).

El carácter específico y sensible del tratamiento de datos constituídos por la imagen y sonidos se reconoce en el último artículo de esta Directiva, en el que la Comisión se compromete a estudiar la aplicación de esta norma comunitaria a este ámbito y a presentar las propuestas que puedan ser necesarias en función de los avances que experimenten las tecnologías de la información y la sociedad de nuestros días conocida como Sociedad de la Información (art.33).

Excepciones de aplicación de la Directiva Las disposiciones contenidas en la Directiva no son aplicables al tratamiento de datos constituidos por imágenes y sonidos cuando se realizan con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades estatales en el ámbito penal, así como para el ejercicio de actividades que no están comprendidas en el ámbito de aplicación del Derecho Comunitario. No obstante, muchos Estados miembros se han preocupado por regular estos ámbitos, de manera general, aunque han establecido excepciones específicas.

Los datos personales son datos relativos a personas físicas identificadas o identificables y cuando nos concretamos en los constituidos por imagen y sonido es indiferente que: las imágenes se utilicen en el marco de un sistema de circuito cerrado y que no estén asociadas a los datos personales del interesado se refieran a personas cuyos rostros no hayan sido filmados, aunque contengan otra información captada a través de la video vigilancia el método utilizado para el tratamiento (sistemas de video fijos o móviles, como receptores de imagen portátiles, o imágenes en color o en blanco y negro), la técnica (dispositivos de cable o fibra óptica), el tipo de equipo (fijo, móvil o portátil), las características de la captación de imágenes (continua por oposición a discontinua,

tal que sucede cuando sólo se realiza en caso de que no se respete el límite de velocidad y no tiene nada que ver con la grabación de imágenes realizada de manera totalmente fortuita y asistemática) y las herramientas de comunicación utilizadas (la conexión con un centro de recepción o el envío de las imágenes a terminales remotos).

2.2.6. DERECHO A LA INFORMACIÓN.

Información.

La información ha sido una necesidad desde tiempos remotos, desde los inicios de la civilización, los detentadores del poder siempre han sido renuentes a la transparencia y proclives a la práctica del secretismo (desde los hechiceros y sacerdotes de la antigüedad hasta los gobernantes de hoy). Así se entiende el por qué la libertad de información como los otros derechos humanos son el fruto de largas y, a veces, sangrientas luchas. Aunque en un principio se la concibió como una simple derivación de la libertad de expresión, la libertad de información cada vez adquiere mayor relevancia al constituirse en uno de los pilares de toda sociedad democrática. Comúnmente se entiende que esta libertad implica solamente la facultad de difundir o recibir información; sin embargo, implica también la libertad de buscar la información a difundir.

El reconocimiento internacional de la libertad de información vino a transformar el sentido inicial o tradicional del vocablo de prensa o libertad de imprenta, en una referencia de mayor envergadura no sólo desde la perspectiva social, sino incluso conceptual. Y es que "la trascendencia social de la libertad de información es tal, que sería iluso esperar una interpretación unidireccional de sus efectos. La influencia de los medios de comunicación está

considerándolos como un eficaz medio de comunicación social en el contexto de un cambio social moderado favorable al desarrollo de la cultura, y a una interpretación dialéctica como instrumento revulsivo de las situaciones de hecho y generados de cambios sociales de importancia", expresado por Ramón Soriano en "Las libertades públicas[105]".

La libertad de información toma auge en el mundo contemporáneo a partir del 10 de diciembre de 1948, cuando surge la Declaración Universal de los Derechos Humanos, donde se establece en el artículo 19 que: "*Todo individuo tiene derecho a la libertad de expresión y de opinión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión*[106]".

Más tarde, el 16 de diciembre de 1966, esta libertad es ratificada en el artículo 10 del Pacto Internacional de Derechos Civiles y Políticos, que dispone que: "*1.- Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que puede haber injerencia de actividades públicas y sin consideración de fronteras. El presente artículo no impide que los estados sometan las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa. 2.- El ejercicio de estas libertades que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias en una sociedad democrática,*

---

[105]**SORIANO DÍAZ**. Ramón Luís Las libertades públicas: significado, fundamentos y estatuto jurídico. Madrid. Tecnos, 1990

[106]**O°DONELL** Daniel *Protección Internacional de los Derecho Humanos* Lima Comisión Andina de Juristas. 1996. P. 183.

para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial".

De la lectura del texto el artículo 19 de la Declaración Universal de Derechos Humanos y 10 del Pacto Internacional de Derechos Civiles y Políticos se puede advertir en principio que el bien jurídicamente protegido no es sólo la libertad de expresión, sino la libertad de recibir, investigar y difundir información por cualquier medio de expresión; es decir, se trata de brindar fundamento legal a lo que se conoce genéricamente como libertad de información.

El hecho de que la libertad de información se tutele legalmente hasta 1949 tiene una explicación racional que ofrece un interesante estudio de la UNESCO: "Mientras la comunicación interpersonal fue la única forma de comunicación humana, el derecho a la libertad de opinión era el único derecho a la comunicación. Y más tarde aun, a medida de que se desarrollaban los grandes medios de comunicación, el derecho a buscar, recibir e impartir información pasó a ser la preocupación principal. Desde ese punto de vista, el orden de los derechos específicos enumerados en el artículo 19, traza una progresión histórica: opinión, expresión, información[107]".

Hay un mandato explícito del artículo 5° de la Constitución en conexión con el artículo 13 de la Convención Americana de Derechos Humanos, el acceso a la información es un derecho

[107]**TRINIDAD MARTÍNEZ** Verónica , 2000; *Recuento de daños a las libertades de expresión e información en 1999*, en Revista Mexicana de Comunicación, número 64, Julio - Agosto de 2000, México DF p.86

esencial que emana de la naturaleza humana y, como tal, impone límites al ejercicio de la soberanía y se incorpora al bloque constitucional que protege la libertad de expresión. Por ello, a su juicio, resulta posible afirmar que, en cuanto a su potencial limitación o restricción, debieran aplicarse los mismos estándares que a esta última, tal como lo ha expuesto la doctrina nacional representada, en este caso, por la opinión de los profesores José Luis Cea Egaña y Alejandro Silva Bascuñan, avalada, asimismo, por pronunciamientos de la Corte Interamericana de Derechos Humanos[108].

El señor Olmedo afirma también que toda restricción al contenido del derecho a acceder a la información que obra en poder de la Administración, debe encontrarse expresamente definida en la ley y ser necesaria para asegurar tanto el respeto a los derechos o a la reputación de los demás, como la protección de la seguridad nacional, el orden público, la salud o la moral públicas.

Por su parte, la interpretación de las restricciones debe regirse, a su entender, por el principio de "proporcionalidad", consistente en que la limitación sólo debe propender a objetivos legítimos, agregando que la carga de la prueba corresponde al Estado.

Derecho a la información.

El derecho a la libertad de información se inscribe en una práctica social: el derecho del individuo a estar informado. Este derecho no se cumple solamente a través de los medios y las noticias, pues se ejerce también a través de métodos como contacto personal, estudio e investigación entre otros. Sin embargo, ninguna libertad es absoluta, y así cláusulas de conciencia y

[108] Sentencia dictada en contra del Estado de Chile en el caso Claude Reyes, de 19 de septiembre de 2006.

secreto profesional, como el que tienen los periodistas de no revelar fuentes, son parte de estas restricciones. Las Constituciones de los estados limitan el derecho a la libertad de información cuando ésta atenta contra la seguridad de las naciones, contra el honor, la intimidad y la protección de la infancia y juventud. Si no fuera así *¿por qué detener a las personas que negocian con pornografía infantil? ¿Por qué hay censura en las películas? ¿Por qué se vela la identidad de una fuente? ¿Por qué hay sigilo bancario?* En la práctica, la libertad de información también se nutre de sus propias contradicciones.

Estas restricciones a la libertad de información toman en cuenta el sentido común, el bien público e individual, el respeto y la prudencia. Para ello se toman en cuenta dos perspectivas: la jurídica, que reglamenta este derecho fundamental, y la que marca una deontología (ética profesional) en el manejo de la información poseída. ¿Por qué ciertas personas tienen derecho a datos y los usan en beneficio propio y otros no? ¿Por qué en una sociedad supuestamente abierta existe el saber secreto en medicinas, armamento, bacterias, descubrimientos? ¿La información del espionaje es pública y libre? ¿Por qué una ideología exige tolerancia para sí e intolerancia para la ajena? Parece que existe un choque entre libertad de información (postulado) y ser libre para informarse (práctica).

Juan Manuel Rodríguez[109] nos dice que "Noam Chomsky y otros prestigiosos intelectuales han puesto en duda esa libertad de información en las sociedades supuestamente libres y democráticas. Se aduce que existen monopolios mediáticos, poder económico y geopolítico detrás de los medios, que gran parte de la información es desinformación o mala información, lateralizada, superflua, dirigida. Se restringe y oculta la

[109] **TRINIDAD MARTÍNEZ** Ob. Cit. p. 72

información mediante el coste del acceso y la no divulgación para preservar la explotación e ignorancia de las masas. Se publica lo que conviene, lo extraño y espectacular ("infortáculos"). Se usa la información como contra-información y viceversa. Se banaliza cierta información para esconder otros conocimientos. ¿Podemos tener conciencia crítica de los hechos cuando gran parte de la información es sesgada, parcial, incompleta y manipulada?"

La teoría del neurolingüistaLakoff ya nos ha advertido que el cerebro funciona mediante datos y marcos mentales ("frames"). Las personas ajustan datos y marcos para estar de acuerdo. Cuando los datos chocan con los marcos, entonces prevalece la estructura mental y se omiten los hechos. Estos valores latentes se activan mediante palabras, imágenes y sonidos. Una palabra o una figura pueden desencadenar fuertes reacciones porque la información ha tocado esa parte del cerebro. Como la información no es inocente, tiene una carga ideológica, es posible que las caricaturas del profeta Mahoma hayan tenido la intención de despertar ese marco religioso que provoca una fuerte reacción emotiva. De este modo las imágenes neutras (?), que a los occidentales no indignan, se publicaron como propaganda política para despertar al león del desierto y del petróleo, ofendiéndolo e irrespetándolo. ¿Hay en ello libertad de propaganda ideológica y cultural? La historia nos remite a la caza de brujas, de comunistas, de judíos, de árabes, de indios, de cristianos, de africanos, de ucranianos, de... ¿Es inocua y aséptica esa tan celebrada libertad de información propagandística? Si como alguien decía "tenemos derecho a caricaturizar a Dios", ¿también tenemos el derecho de caricaturizar a la madre del dibujante? Creo que la información y la confrontación de ideas ayudan al desarrollo humano cuando favorecen la comunicación mediante el respeto a las diferencias. El descrédito del adversario, el insulto y

la burla de los símbolos ¿mejorarán las relaciones entre las personas? Tal vez, sí; quizás, no.

El primer bien jurídico protegido que entraña la libertad de información es el derecho de los individuos a recibir información de interés público susceptible de permitir la conformación se la llamada opinión pública libre, constancia a un estado democrático de derecho. Se trata de un derecho pasivo que demanda al mismo tiempo un deber activo y pasivo por parte del estado. Activo porque debe desarrollar acciones tendientes a evitar que intereses económicos o políticos puedan obstaculizar la libre recepción informativa. Pasivo porque debe abstenerse de crear impedimentos reglamentarios que dificulten o impidan la libre recepción de la información de interés público.

Este derecho es tutelado por 82 constituciones en el mundo, algo así como el 43% de los países del mundo.

Derecho a difundir información.

El segundo bien jurídico protegido que incorpora la libertad de información, es el derecho de los individuos a difundir información de carácter noticioso, como requisito sine qua non de la conformación de la sociedad civil sobre la que se erige un estado democrático de derecho.

Esta figura jurídica contiene una naturaleza activa en la medida en que al titular del derecho -los individuos en lo general y los periodistas en lo particular- debe brindársele, al amparo de la protección constitucional, la posibilidad de acceder a las fuentes de información de interés público. Para que ello sea posible, el estado tiene un deber esencialmente activo en tanto de llevar a

cabo las acciones necesarias para poner a disposición general los datos, documentos e información de interés público.

En el Perú según el CÓDIGO DE ÉTICA de la Sociedad Nacional de Radio y Televisión, indica en su artículo 3°, que en la prestación de los servicios de radiodifusión se rige por los siguientes principios:

a) La defensa de la persona humana y el respeto a su dignidad.
b) La libertad de expresión, de pensamiento y de opinión.
c) El respeto al pluralismo informativo, político, religioso, social y cultural.
d) La defensa del orden jurídico democrático, de los derechos humanos fundamentales y de las libertades consagradas en los tratados internacionales y en la Constitución Política del Perú.
e) La libertad de información veraz e imparcial.
f) El fomento de la educación, cultura y moral de la nación.
g) La protección y formación integral de los niños y adolescentes, así como el respeto de la institución familiar.
h) La promoción de los valores y la identidad nacional.
i) La responsabilidad social de los medios de comunicación.
j) El respeto al honor, la buena reputación y la intimidad personal y familiar.
k) El respeto al derecho de rectificación.

2.2.7. TECNOLOGÍA INFORMÁTICA.

La Tecnología Informática (IT), según lo definido por la asociación de la Tecnología Informática de América (ITAA), es "el estudio, diseño, desarrollo, innovación puesta en práctica, ayuda o gerencia de los sistemas informáticos computarizados, particularmente usos del software y hardware." En general, se

ocupa del uso de computadoras y del software electrónico de convertir, de almacenar, de proteger, de procesar, de transmitir y de recuperar la información[110].

El término tecnología informática se ha ampliado para abarcar muchos aspectos referidos a la computadora y la tecnología informática, siendo conocida generalmente como Tecnología de la Información. El paraguas de la tecnología informática puede ser grande, cubriendo muchos campos. Los profesionales realizan una variedad de deberes que se extiendan de instalar usos a diseñar redes de ordenadores y bases de datos complejas.

Algunos de los deberesque los profesionales e Ingenieros relacionados con la Tecnología de Informaciónrealizan, pueden incluir lo siguiente:

Gerencia de datos
Establecimiento de redes informáticas
Diseño de los sistemas de la base de datos
Diseño del software
Sistemas de información de gerencia
Gerencia de sistemas

La tecnología de la informática del mundo y la alianza de los servicios (WITSA) es un consorcio sobre 60 asociaciones de la industria de la tecnología informática (IT) de economías alrededor del mundo. Fundado adentro 1978 y conocido originalmente como la asociación de la industria de servicios del mundo que computaba, WITSA ha asumido cada vez más un papel activo de la defensa en las ediciones internacionales del orden público que

[110]**ASOCIACIÓN DE LA TECNOLOGÍA INFORMÁTICA DE AMÉRICA** TECNOLOGÍA INFORMATICA. En http://es.wikipedia.org/wiki/Tecnolog%C3%ADa_inform%C3%A1tica. Recuperado el 12 de Mayo del 2012.

afectaban la creación de una infraestructura de datos global robusta.

La asociación de la tecnología informática de América (ITAA) es un grupo comercial de la industria para varias compañías de la tecnología informática de los EE.UU.

Fundado en 1961 como la asociación de las organizaciones de servicios de proceso de datos (ADAPSO), la asociación de la tecnología informática de América (ITAA) proporciona el orden público global, el establecimiento de una red del negocio, y la dirección nacional para promover el crecimiento rápido continuado del IT industrial. ITAA consiste en aproximadamente 325 miembros corporativos a través de los EE.UU., y es secretaría de la tecnología informática del mundo y mantiene la alianza (WITSA), una red global de IT de los 67 países asociados.

2.2.8. INGENIERÍA SOCIAL

En el campo de la seguridad informática, la ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos.

Generalmente se está de acuerdo en que "los usuarios son el eslabón más débil" en seguridad de la información; éste es el principio por el que se rige la ingeniería social.

Un ejemplo contemporáneo de un ataque de ingeniería social es el uso de archivos adjuntos en e-mails que ejecutan código malicioso (por ejemplo, usar la máquina de la víctima para enviar cantidades masivas de spam). Ahora, luego de que los primeros e-mails maliciosos llevaron a los proveedores de software a deshabilitar la ejecución automática de archivos adjuntos, los usuarios deben activar los archivos adjuntos de forma explícita para que ocurra una acción maliciosa. Muchos usuarios, sin embargo, cliquean ciegamente cualquier archivo adjunto recibido, concretando de esta forma el ataque.

Quizá el ataque más simple que aún es efectivo sea engañar a un usuario llevándolo a pensar que uno es un administrador del sistema y solicitando una contraseña para varios propósitos. Los usuarios de sistemas de Internet frecuentemente reciben mensajes que solicitan contraseñas o información de tarjeta de crédito, con el motivo de "crear una cuenta", "reactivar una configuración", u otra operación supuestamente no maliciosa.

2.2.9. RECOLECCIÓN DE DATOS PERSONALES.

En la actualidad, cualquier usuario tiene la posibilidad de adquirir alguna aplicación que permita copiar automáticamente las direcciones de mail que figuran en las páginas web a medida que se navega, y esta facilidad ha permitido el crecimiento de un "mercado negro" de bases de datos[111].

Daniel Blasón, presidente del capítulo Database de AMDIA (Asociación de Marketing Directo e Interactivo de Argentina) explica

[111]**QUAGLIA** Juan Cómo se recopilan datos personales a través de Internet, Recuperado el 17 de Mayo del 2012 en http://www.lanacion.com.ar/1195940-como-se-recopilan-datos-personales-a-traves-de-internet

a lanacion.com el fenómeno: "A eso le llamamos mercado informal de base de datos. Una simple cadena de mails es una recopilación y validación de direcciones de correo electrónico. Si renvías una cadena de mails a tus amigos, estás validando tu mail y contribuyendo a una base de datos[112]".

Una fuente de información importante con la que cuentan las empresas para la recolección de datos personales a través de Internet son los registros de compras. Las páginas web de compra y venta tienen abundante información, que luego se utiliza con fines estadísticos o para acciones de marketing. Las redes sociales, en especial las más populares, como Facebook, constituyen otra fuente a tener en cuenta, debido a que allí los usuarios dejan abundantes indicios acerca de sus intereses y hábitos, a medida que crean y participan de grupos temáticos y páginas de fans[113].

Un mayor uso de las redes sociales permitió que las compañías puedan generar sus propias bases de datos con el comportamiento de sus usuarios.

Al respecto, Blasón comenta: "Una empresa puede construir una base de datos a través de sus clientes, o se puede generar en forma espontánea, alrededor de cualquier eje temático de una red social, como el fanatismo por determinada banda de música, determinado lugar o determinada marca. Se genera un grupo, que luego es aprovechado por alguien: por un líder de grupo, una empresa o alguien que quiere comunicar algo[114]".

La mirada de un experto en seguridad informática

---

[112]Ibidem.
[113]Ibidem.
[114]Ibidem.

La forma en que son administradas estas bases de datos y su seguridad cobran especial importancia si se toman en cuenta casos como el robo de identidad digital, los derechos de propiedad de la información personal o el robo de contraseñas por parte de piratas informáticos. César Cerrudo es investigador y experto en seguridad de aplicaciones y ha descubierto fallas en los principales programas de bases de datos, como así también en sistemas operativos.

2.2.10. POLITICA Y ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

MARCO NORMATIVO Y LEGAL:

Las Tecnologías de la Información y la Comunicación (TIC) son un conjunto de servicios, redes, software y dispositivos de hardware que se integran en sistemas de información interconectados y complementarios, con la finalidad de gestionar datos e información de manera efectiva, mejorando la productividad de los ciudadanos, gobierno y empresas, dando como resultado una mejora en la calidad de vida. Las TIC se encuentran intrínsecamente ligadas con la rutina y acciones diarias de un porcentaje significativo de los ciudadanos del mundo, siendo hoy el mayor medio de comunicación e interacción y desarrollo que tenemos a nuestro alcance. Por otro lado, nos encontramos inmersos en un proceso de globalización económica que genera una creciente interdependencia entre los países, y donde las TIC han permitido la dinamización de los procesos económicos, sociales y hasta culturales.

En la actualidad las organizaciones utilizan con más frecuencia las computadoras para manejar y almacenar su información vital que

constituye el activo más valioso, esto les trae muchos beneficios, pero también los hace vulnerables a los diferentes delitos que se pueden cometer por medio de las computadoras si no se cuentan con un sistema de seguridad. Entre ellos, se pueden mencionar el robo, destrucción o modificación de información, fraude, etc. Que son realizados por personas con algún conocimiento de computación, ya sea dentro o fuera de la organización.

Conforme ha ido insertándose la Sociedad de la Información y del conocimiento en aras de construir una sociedad de la información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, los gobiernos en todo el mundo han implementado políticas de informatización del estado; en el Perú la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) dependiente de la Presidencia del Consejo de Ministros ha formulado una serie de políticas y normas orientadas al establecimiento y consolidación del Gobierno Electrónico[115], materializándose a través de la Plataforma de Interoperabilidad del Estado (PIDE)[116], plataforma de aplicación para todas las entidades del Sistema Nacional de Informática[117], siendo de uso

[115]El Gobierno Electrónico según lo define la Organización de las Naciones Unidas (ONU), es el uso de las Tecnologías de Información y la Comunicación (TIC), por parte del Estado, para brindar servicios e información a los ciudadanos, aumentar la eficiencia y eficacia de la gestión pública, e incrementar sustantivamente la transparencia del sector público y la participación ciudadana. http://www.ongei .gob.pe

[116] Creada mediante Decreto Supremo N° 083-2011-PCM, definida como la infraestructura tecnológica que permite la implementación de servicios públicos por medios electrónicos y al intercambio electrónico de datos, entre unidades del estado a través de internet, telefonía móvil y otros medios tecnológicos disponibles.

[117] El Sistema Nacional de Informática fue creado por decreto legislativo N° 604, con el fin de organizar las actividades y proyectos que en materia de informática realizan las instituciones públicas del estado, así como su relación con otros sistemas y áreas de la Administración pública. http://www.ongei .gob.pe

obligatorio a las entidades públicas que implementen servicios públicos por medios electrónicos.

Esta situación trae como consecuencia que las empresas tanto públicas como privadas estén invirtiendo una parte de su presupuesto en la seguridad y protección de la información que maneja. Hoy en día, existen varias técnicas y herramientas para proteger la información, entre ellas cabe mencionar la implantación de políticas de seguridad tales como el uso de firewalls[118], claves de acceso, encriptación y codificación de mensajes, detectores de intrusos, filtros de contenido, entre otros.
El Estado Peruano ha venido implementando una serie de normas legales e iniciativas presentadas por diferentes organismos públicos, orientadas al establecimiento de políticas de seguridad de la información, como la ley N° 27309 que incorpora los delitos informáticos al código penal[119], la Directiva de normas y procedimientos técnicos para garantizar la seguridad de la información publicadas por las entidades de la Administración Pública, la aprobación del uso de la norma técnica peruana NTP-17799:2004/2007 EDI "Buenas prácticas para la gestión de la seguridad de la información 1ra. Edición y 2da. Edición", hasta la creación del Pe-CERT[120] con la finalidad de articular un procedimiento de respuesta entre las diferentes entidades públicas ante eventos e incidentes de seguridad de la información.
Tenemos por tanto en el marco nacional, un conjunto de normas orientadas a normar las actividades nacionales en la materia; es importante hacer mención a los esfuerzos realizados por el Estado Peruano en su legislación de manera cronológica, tal como se

[118]Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.
[119] Promulgado a través del Decreto Legislativo N° 635 , incorpora los artículos 207A, 207B y 207C, con penas que van desde los tres (03) años hasta los siete (07) años de pena privativa de la libertad.
[120] Coordinadora de Respuestas a Emergencias Teleinformáticas de Administración Pública del Perú, creada con Resolución Ministerial N° 360-2009-PCM

observa a continuación:

Ley/D.S./D.L./ R.M./Normas	Tema
Ley Nº 27269 modificada por la Ley Nº 273102000	Ley de firmas y certificados digitales, regula la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.
Ley Nª 272912000	Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica.
Ley Nº 27309 2000	Ley que incorpora los Delitos Informáticos al Código Penal incorpora los artículos 207ª, 207B y 207C, penalizando a aquellos que utilicen o ingresen indebidamente a una Base de Datos, Sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar, alterar o un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos; El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos. Estos serán reprimidos con penas privativas de la libertad.
LEY N° 28493	Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM).
LEY Nº 28530	Ley de Promoción de Acceso a Internet para personas con discapacidad y de adecuación del espacio físico en cabinas públicas de internet.

Se han formulado asimismo, diferentes iniciativas en algunos sectores las cuales han sido tomadas como documentos de consulta y referencia para la elaboración del presente documento, entre las cuales destacan:

INICIATIVA	ENTIDAD LÍDER	ALCANCE
Resolución de Contraloría Nº 072-98-CG 1998	Contraloría General de la República	Normas Técnicas de Control Interno para Sistemas Computarizados. (Norma 500- 01 al 500-08). Orientadas a la organización del área de informática, Plan de Sistemas de Información, controles de datos fuentes de entrada y salida, Mantenimiento de computadoras, seguridad de programas, de datos y equipos de computo, Plan de contingencias, aplicación de técnicas de intranet y gestión de software adquirido a medida por las entidades públicas.
Resolución Jefatural Nª 341-2001-INEI	Instituto Nacional de Estadística e Informática	Con la cual se aprueba la Directiva "Normas y Procedimientos Técnicos para garantizar la Seguridad de la Información publicadas por las

		entidades de la Administración Pública".
Resolución Jefatural Nº 386-2002-INEI	Instituto Nacional de Estadística e Informática	Con esta Resolución se aprueban las Normas técnicas para el almacenamiento y respaldo de la información procesada por las entidades de la Administración Pública.
DECRETO SUPREMO Nº 013-2003-PCM	Presidencia del consejo de Ministros	Con el cual se dictan normas para que se adopten medidas que permitan garantizar la legalidad de la adquisición del software en entidades y dependencias del Sector Público.
RESOLUCIÓN JEFATURAL Nº 053-2003365-INEI	Instituto Nacional de Estadística e Informática	Con la que se aprueba la Directiva sobre "Norma técnica para la implementación del registro de recursos informáticos en las instituciones de la administración pública".
RESOLUCIÓN JEFATURAL Nº 088-2003-INEI.	Instituto Nacional de Estadística e Informática	Mediante esta Resolución se aprueba la directiva sobre "Normas para el uso del servicio de correo electrónico en las entidades de la administración pública".
RESOLUCIÓN MINISTERIAL Nº 126-2003-PCM	Presidencia del consejo de Ministros	Constituyen el Comité Coordinador de la Infraestructura de Datos Espaciales del Perú - IDEP.
RESOLUCIÓN MINISTERIAL Nº 181-2003-PCM	Presidencia del consejo de Ministros	Crean comisión multisectorial para el desarrollo de la sociedad de la información - CODESI.
DECRETO SUPREMO Nº 043-2003-PCM	Presidencia del consejo de Ministros	Aprueba Texto Único Ordenado de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública. Todas las actividades y disposiciones de las entidades comprendidas en la presente Ley están sometidas al principio de publicidad. Los funcionarios responsables de brindar la información correspondiente al área de su competencia deberán prever una adecuada infraestructura, así como la organización, sistematización y publicación de la información a la que se refiere esta Ley.
Decreto Supremo Nº 066-2003-PCM	Presidencia del consejo de Ministros	Fusionan la Subjefatura de Informática del Instituto Nacional de Estadística e Informática - INEI y la Presidencia del Consejo de Ministros
DECRETO SUPREMO Nº 072-2003-PCM	Presidencia del consejo de Ministros	Aprueban el Reglamento de la Ley de Transparencia y Acceso a la Información Pública
RESOLUCIÓN MINISTERIAL Nº 334-2003-PCM	Presidencia del consejo de Ministros	Crean Comisión Multisectorial encargada de proponer los lineamientos para la Integración de los Sistemas Informáticos y Plataformas Tecnológicas de las diversas

		entidades del Estado y el desarrollo e implantación del piloto del Medio de Pago Virtual del Estado.
RESOLUCIÓN COMISIÓN DE REGLAMENTOS TÉCNICOS Y COMERCIALES Nº 0103-2003-CRT-INDECOPI	INDECOPI	Aprueban disposiciones complementarias al reglamento de la Ley de Firmas y Certificados Digitales
RESOLUCIÓN MINISTERIAL Nº 323-2004-PCM	Presidencia del consejo de Ministros	Crean el Sistema de Informática del Sector Defensa como parte integrante del Sistema nacional de Informática.
RESOLUCIÓN MINISTERIAL Nº 179-2004-PCM	Presidencia del consejo de Ministros	Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2004 Tecnología de la Información. "Procesos del Ciclo de Vida del Software, 1ª Edición" en entidades del Sistema Nacional de Informática.
RESOLUCIÓN MINISTERIAL Nº 224-2004-PCM	Presidencia del consejo de Ministros	Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información: Código de Buenas Prácticas para la gestión de la Seguridad de la Información. . 1ª Edición. " en entidades del Sistema Nacional de Informática
RESOLUCIÓN MINISTERIAL Nº 873-2004-DE-SG.	Ministerio de Defensa	Publican Política de Informática del Sector Defensa.
RESOLUCIÓN MINISTERIAL Nº 148-2005-PCM	Presidencia del consejo de Ministros	Aprueban y autorizan la publicación del "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana".
DECRETO SUPREMO N° 031-2006-PCM	Presidencia del consejo de Ministros	Aprueban Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana.
RESOLUCIÓN MINISTERIAL Nº 274-2006-PCM	Presidencia del consejo de Ministros	Aprueban la Estrategia Nacional de Gobierno Electrónico.
DECRETO SUPREMO Nº 004-2007-PCM	Presidencia del consejo de Ministros	Aprueban Reglamento de la Ley de Firmas y Certificados Digitales.
RESOLUCIÓN MINISTERIAL Nº 246-2007-PCM	Presidencia del consejo de Ministros	Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
RESOLUCION MINISTERIAL Nº 381-2008-PCM	Presidencia del consejo de Ministros	Aprueban lineamientos y mecanismos para implementar la interconexión de equipos de procesamiento electrónico de información entre las entidades del

		Estado
RESOLUCION MINISTERIAL Nº 360-2009-PCM	Presidencia del consejo de Ministros	Crean el Grupo de Trabajo denominado Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (Pe-CERT)
DECRETO SUPREMO Nº 025-2010-PCM	Presidencia del consejo de Ministros	Decreto Supremo que modifica el numeral 10 del artículo 2° del Decreto Supremo N° 027-2007-PCM que define y establece las Políticas Nacionales de obligatorio cumplimiento para las entidades del Gobierno Nacional.
RESOLUCIÓN MINISTERIAL Nº 197-2011-PCM	Presidencia del consejo de Ministros	Establecen fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información"
DECRETO SUPREMO Nº 070-2011-PCM	Presidencia del consejo de Ministros	Decreto Supremo que modifica el Reglamento de la Ley Nº 27269, Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo Nº 681 y ampliatorias
DECRETO SUPREMO Nº 069-2011-PCM	Presidencia del consejo de Ministros	Crean el Portal de Información de Datos Espaciales del Perú (GEOIDEP)
DECRETO SUPREMO Nº 066-2011-PCM	Presidencia del consejo de Ministros	Aprueban el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0"
DECRETO SUPREMO Nº 083-2011-PCM	Presidencia del consejo de Ministros	Crean la Plataforma de Interoperabilidad del Estado - PIDE

En el plano internacional, se puede destacar como los principales instrumentos internacionales en materia de ciberseguridad y ciberdefensa a:

INSTRUMENTO	MATERIA
Convenio sobre Ciberdelincuencia14 del Consejo de Europa – CCC (conocido como en convenio sobre cibercriminalidad de Budapest) Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004.	El objetivo principal del convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas. Único instrumento vinculante vigente sobre el tema en el ámbito internacional y su protocolo para la criminalización de actos de racismo y xenofobia cometidos a través de sistemas informáticos. El Consejo considera que el delito

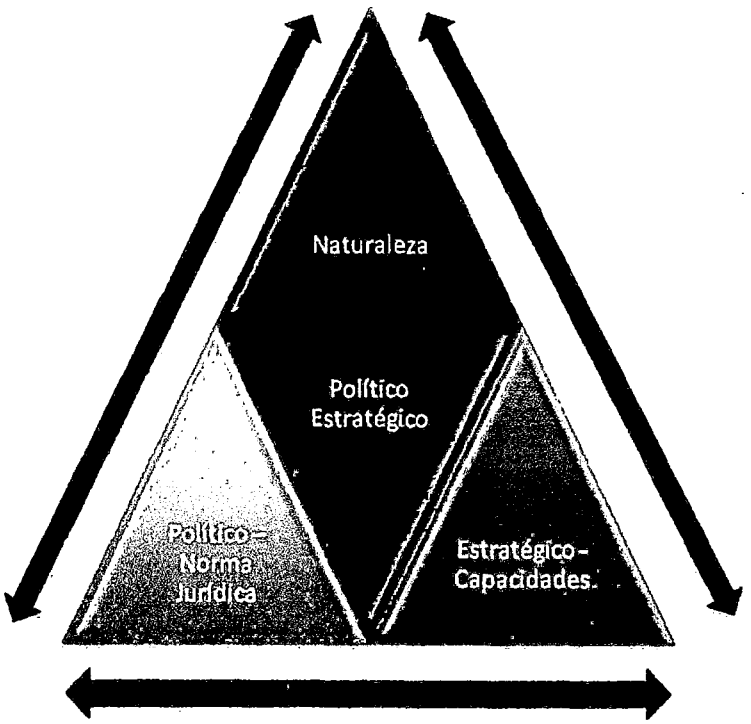
	cibernético exige una política penal común destinada a prevenir la delincuencia en el ciberespacio15 y en particular, hacerlo mediante la adopción de legislación apropiada y el fortalecimiento de la cooperación internacional. Cabe resaltar que si bien el CCC tuvo su origen en el ámbito regional europeo, es un instrumento abierto para su adhesión a todos los países del mundo.
Resolución AG/RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos.	Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética. Estipula tres vías de acción: • Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores - CSIRT16. Este cometido fue asignado al Comité Interamericano Contra el Terrorismo - CICTE. • Identificación y adopción de normas técnicas para una arquitectura segura de Internet. Esta labor es desarrollada por la Comisión Interamericana de Telecomunicaciones. • Adopción y/o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información de los delincuentes y los grupos delictivos organizados que utilizan estos medios, a cargo de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas - REMJA.
Decisión 587 de la Comunidad Andina, adoptada el 10 de julio de 2004.	Por la cual se establecen los lineamientos de la Política de Seguridad Externa Común Andina. Dentro de los objetivos de dicha política se encuentra el prevenir, combatir y erradicar las nuevas amenazas a la seguridad y cuando corresponda sus interrelaciones, a través de la cooperación y coordinación de acciones orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina.
Consenso en materia de ciberseguridad17 de la Unión Internacional de Telecomunicaciones - UIT, en el seno de Naciones Unidas, en desarrollo del programa de acciones de Túnez para la sociedad de la información de 2005.	Busca la promoción del examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.
Resolución 64/25 "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional" Asamblea General de las Naciones	La Asamblea General exhorta a los Estados miembros a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de

Unidas. (2009)	información Esta resolución continúa el seguimiento de la Asamblea, con las resoluciones 53/70, de 4 de diciembre de 1998; 54/49, de 1° de diciembre de 1999; 55/28, de 20 de noviembre de 2000; 56/19, de 29 de noviembre de 2001, 57/53, de 22 de noviembre de 2002; 58/32, de 8 de diciembre de 2003; 59/61, de 3 de diciembre de 2004; 60/45, de 8 de diciembre de 2005; 61/54, de 6 de diciembre de 2006; 62/17, de 5 de diciembre de 2007; y 63/37, de 2 de diciembre de 2008.

NATURALEZA DEL ACCIONAR DEL ESTADO EN EL CIBERESPACIO

Los Estados por su naturaleza siempre están asociados a la preservación de la existencias las sociedades que los constituyen, desde los albores de la humanidad la protección de los cotos de caza, las fuentes de alimentos y agua así como de otras formas de desarrollo de estas sociedades derivaban en el desarrollo de capacidades que permitirán proteger estos bienes. En la actualidad la naturaleza de los Estados se asocia al marco jurídico que le da legalidad a sus actividades y que les permite el desarrollo de capacidades para materializar la razón de su existencia, entendida como su naturaleza.

En el caso particular del Estado Peruano, su naturaleza se sustenta en la Constitución Política del Estado y las Leyes, que permiten el desarrollo de un conjunto de capacidades en diferentes campos con la finalidad de proporcionar el Bien Común y el Bienestar General, (Educación, Salud, Justicia, Defensa, etc.). Si trasladamos este concepto a las actividades en el ciberespacio, observamos que existen un conjunto de normas internacionales y nacionales que establecen la necesidad de desarrollar capacidades para detectar, mitigar, reaccionar y recuperar las actividades en el ciberespacio.



La gráfica muestra como se relaciona la naturaleza de las cosas con su marco jurídico y el desarrollo de capacidades, articulado con u marco político estratégico.

La gráfica que se muestra, nos expresa que cuando deseamos cambiar la naturaleza debemos cambiar las normas jurídicas y esto repercute en las capacidades a desarrollar, lo que demuestra la interdependencia entre estos tres componentes.

La Política Nacional de Seguridad y Defensa Nacional aprobada con D.S. Nº OO1-B-2004-DE/SG del 10-03-2004, presenta el siguiente escenario: *"...**El uso de la telemática contra los intereses del Estado**...La guerra cibernética se ha convertido en una realidad. Actualmente es posible vulnerar la información clasificada de un Estado penetrando sus computadoras. Pero, más aún, es posible paralizar un país emitiendo ondas electromagnéticas que interfieran sus comunicaciones, destruyan la información de sus computadoras, penetren en la información reservada de los bancos, confundan las señales de los*

aeropuertos, ferrocarriles y demás medios de transporte, etc., creando un verdadero caos en un país. Contra esta amenaza debemos estar preparados ya que constituye una nueva forma de hacer la guerra...".

En este escenario se presentan una serie de amenazas que se manifiestan en una serie de formas como (Denegación de servicio, Desfacing, Hacking, etc.); este escenario descrito, está asociado al objetivo: "*...Mantenimiento de la independencia, soberanía, integridad territorial y defensa de los intereses nacionales...*" y ala política "*...Garantizar la seguridad telemática del Estado...*", la cual tiene carácter vinculante.

USO DE LAS TECNOLOGIAS DE INFORMACION Y COMUNICACIONES

Ahora bien, en el Perú se ha incrementado considerablemente el uso de tecnologías de la información y las comunicaciones elevando su nivel de exposición a amenazas cibernéticas. El 32.1 por ciento de los hogares de Lima metropolitana tiene servicio de internet al trimestre julio, agosto, setiembre del año 2011, lo que representa un crecimiento de 2.5 por ciento respecto a similar período del año pasado, informó el Instituto Nacional de Estadística e Informática (INEI). Según el informe técnico denominado *"Las tecnologías de información y comunicación en los hogares"*, correspondiente al trimestre mencionado, elaborado por el INEI sobre la base de los resultados de la Encuesta Nacional de Hogares (ENAHO)[121], reveló que la cobertura de este servicio en el área urbana fue de 12.5 por ciento y en el área rural, 0.2 por ciento, cifras que al

[121] Información tomada del informe Técnico N° 4 Diciembre 2011, Las Tecnologías de Información y Comunicación en los Hogares, Trimestre julio, agosto, setiembre 2011 (en comparación a similar trimestre del año 2010.

compararlas con similar trimestre del año anterior presentaron incrementos de 4.2 y0.1 puntos porcentuales, respectivamente. Por otro lado, a nivel nacional, el 13.4 por ciento de los hogares tiene acceso al servicio de internet, representando un aumento de 3 por ciento respecto a similar trimestre de 2010.

25.2% de hogares tiene computadora. El documento refiere también que el 25.2 por ciento de los hogares del área urbana (no incluye a Lima metropolitana) cuenta por lo menos con una computadora, cifra que representó un incremento de 2.1 puntos porcentuales respecto a similar trimestre del año anterior. Asimismo, por área de residencia, el 41.5 por ciento de los hogares de Lima metropolitana cuenta con por lo menos una computadora, lo que representó un aumento de tres puntos porcentuales respecto a lo observado en similar período del año anterior; en tanto que en el área rural sólo el 4.5 por ciento de los hogares cuenta con por lo menos una computadora.

Los resultados de la ENAHO para el trimestre bajo análisis, nos revelan que el 61,7% de los jóvenes entre 19 a 24 años de edad usan Internet y un 61,6% de la población de 12 a 18 años hacen uso de este servicio. Entre los niños de 6 a 11 años este porcentaje es de 30,6%, mientras que entre los adultos mayores el 4,8% usa Internet.

Según la Internet *WorldStats–Usage and PopulationStatistics*[122], con datos propocionados por el *Bureau para Censos de los Estados Unidos*[123], a diciembre de 2011 se aprecia que el Perú

[122] Internet WorldStats es un sitio internacional que cuenta hasta la fecha acceso a través de Internet de información de todo el mundo, produciendo estadísticas de población y datos en general para la producción de Investigaciones de Mercado, en más de 233 países y regiones del mundo.
[123] US Bureau Census, La Oficina del Censo de los Estados Unidos de Norteamérica, es la entidad gubernamental encargada de recopilar información censal, que sirve como la principal fuente de información de calidad acerca de las personas de su nación y su economía.

ocupa el 10mo. Puesto a nivel latinoamericano en cuanto al nivel de penetración del internet en la población, se puede apreciar como hay países que con menor población tienen un mayor volumen de penetración de internet, esto redunda drásticamente en las necesidades de seguridad de la información e incrementa los riesgos a sufrir ataques, dado que al informatizarse la sociedad, se incrementa también la necesidad de servicios en línea, tal como se aprecia en cuadro siguiente.

LATIN AMERICA COUNTRIES / REGIONS	Population (Est. 2011)	Internet Users, 30-Jun-11	% Population (Penetration)	Users % in Region	Facebook 31-Dec-11
Argentina	41,769,726	**27,568,000**	66.0 %	13.0 %	17,581,160
Uruguay	3,308,535	**1,855,000**	56.1 %	0.9 %	1,479,580
Chile	16,888,760	**9,254,423**	54.8 %	4.4 %	9,020,800
Colombia	44,725,543	**22,538,000**	50.4 %	10.6 %	15,799,320
Costa Rica	4,576,562	**2,000,000**	43.7 %	0.9 %	1,638,420
DominicanRepublic	9,956,648	**4,116,870**	41.3 %	1.9 %	2,514,120
Venezuela	27,635,743	**10,421,557**	37.7 %	4.9 %	9,579,200
Brazil	203,429,773	**75,982,000**	37.4 %	35.8 %	35,158,740
Puerto Rico	3,989,133	**1,486,340**	37.3 %	0.7 %	1,361,020
Peru	**29,248,943**	**9,157,800**	**31.3 %**	**4.3 %**	**7,886,620**
Mexico	113,724,226	**34,900,000**	30.7 %	16.4 %	30,990,480
Panama	3,460,462	**959,90**	27.7 %	0.5 %	895,7
Ecuador	15,007,343	**3,352,000**	22.3 %	1.6 %	4,075,500
El Salvador	6,071,774	**1,035,940**	17.1 %	0.5 %	1,257,380
Paraguay	6,459,058	**1,104,700**	17.1 %	0.5 %	954,98
Guatemala	13,824,463	**2,280,000**	16.5 %	1.1 %	1,740,660
Cuba	11,087,330	**1,605,000**	14.5 %	0.8 %	n/a
Bolivia	10,118,683	**1,225,000**	12.1 %	0.6 %	1,482,800
Honduras	8,143,564	**958,50**	11.8 %	0.5 %	1,067,560
Nicaragua	5,666,301	**600,00**	10.6 %	0.3 %	663,5
TOTAL	579,092,570	**212,401,030**	36.7 %	100.0 %	145,147,740

A nivel de instituciones públicas el incremento del uso de Tecnologías de Información en los procesos principales se ha venido incrementando, si bien no existen cifras oficiales se puede afirmar que la adopción de medidas e iniciativas como la creación de la Plataforma de Interoperabilidad del Estado – PIDE, la aprobación del Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0 y la creación del Portal de Información de Datos Espaciales del Perú (GEOIDEP), nos hacen pensar que el incremento del uso de las TI en el estado peruano va en aumento, teniendo en consideración la evolución del internet específicamente el paso de la web 1.0 a la web 2.0 y lo que se prevé como futuro web 3.0 y web 4.0, no se trata únicamente de la evolución de una serie de herramientas tecnológicas, ni hay que confundirla con Internet2[124], la Web 2.0 es un concepto más que un término de moda con el que se busca identificar una serie de procesos sociales y culturales que se están desarrollando en virtud de la capacidad conectiva de Internet. Esta cultura, que es calificada por algunos como Cultura 2.0, la desarrollan actualmente los usuarios, la sociedad y las organizaciones.

Bajo este marco, *O'Reilly Media,* empresa de innovación tecnológica y *MediaLive International*, empresa de soluciones de marketing, a mediados de 2004, elaboran una evaluación sobre el desplome de las empresas de Internet comparando las razones por las que muchas de éstas habían dejado de operar y por qué otras, en cambio, habían subsistido. El producto del análisis, que puede verse en el Gráfico 1, se organiza separando dos categorías para reconocer a las empresas que habían colapsado, Web 1.0, y las otras con futuro, Web 2.0.

[124]Consorcio sin fines de lucro, **UCAID** (*UniversityCorporationforAdvanced Internet Development*), cuyo objetivo principal es desarrollar tecnologías de fibra óptica que permita la trasferencia de información a altas velocidades con una gran fiabilidad.

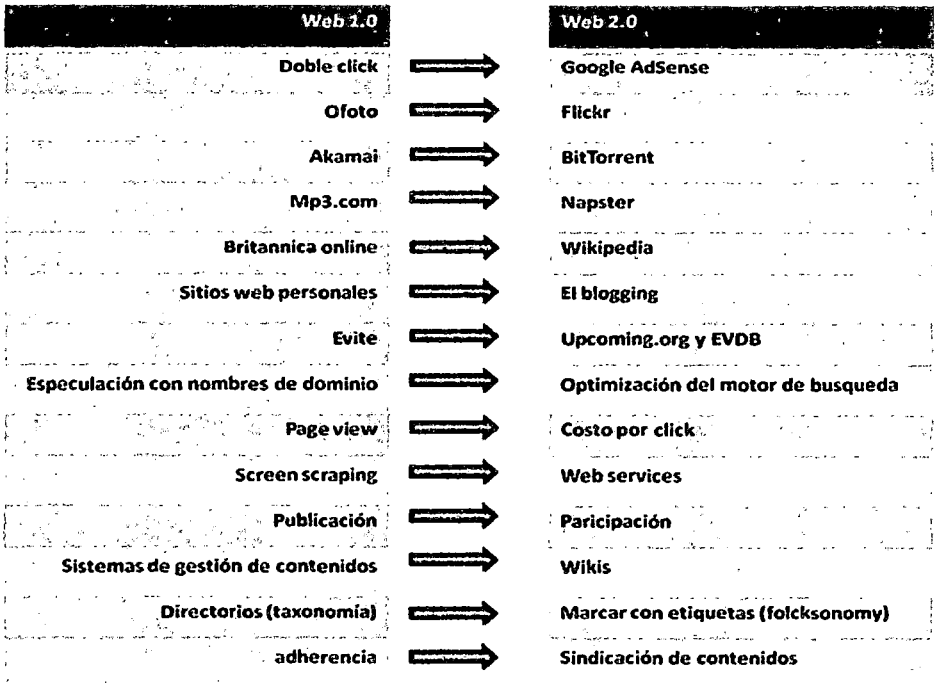


Ilustración 1 Análisis comparativo entre las aplicaciones Web 1.0 y Web 2.0 - fuente O`Riley, 2005

Si bien, en general, se asocia el término al de Web Semántica(acuñado por Tim Berners-Lee, quien inventó la Web a principios de los 90), cabe acotar que **no existe total consenso acerca de lo que significa la Web 3.0.** Aunque se coincide en que esta etapa añadirá significado a la Web, no hay acuerdo sobre cuáles son los caminos más apropiados para su desarrollo.

Dado que los avances de esta disciplina son demasiado lentos y dificultosos, la solución podría estar en la combinación de las técnicas de **inteligencia artificial** con el acceso a la capacidad humana de realizar tareas extremadamente complejas para un ordenador. En cualquier caso, el aumento de la interactividad y de la movilidad son dos factores que muchos señalan como decisivos en esta nueva etapa de la Web.

En la figura 2 se muestra el proceso evolutivo que seguirá la web

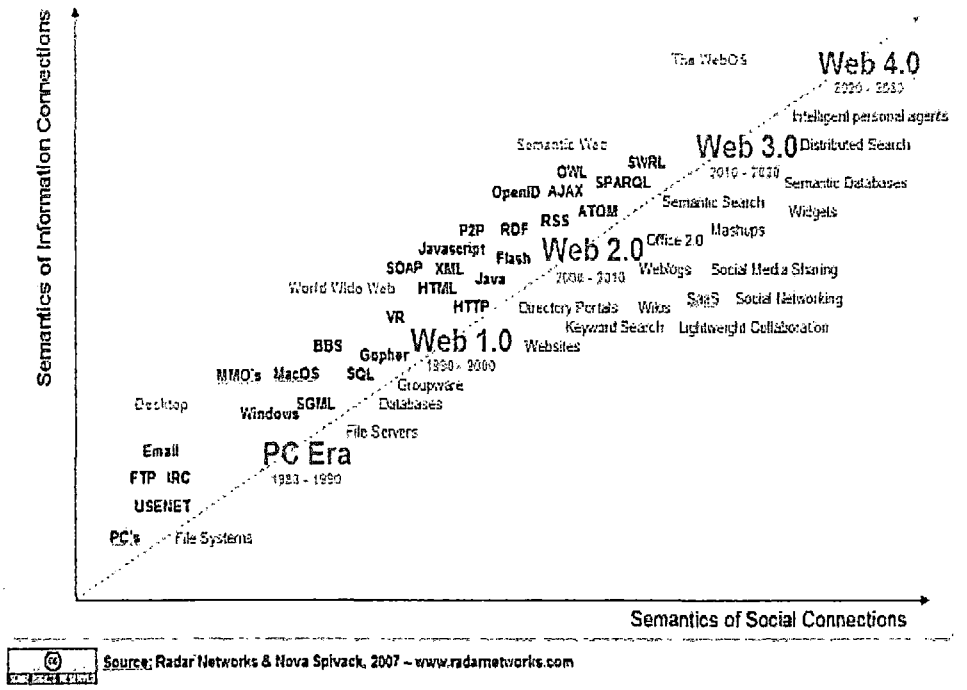
de cara al 2020, la Web Semántica[125] *TWINE WEB 3.0*[126] desarrollada por *Radar Networks*[127] es una Web extendida, dotada de mayor significado en la que cualquier usuario en Internet podrá encontrar respuestas a sus preguntas de forma más rápida y sencilla gracias a una información mejor definida. Al dotar a la Web de más significado y, por lo tanto, de más semántica, se pueden obtener soluciones a problemas habituales en la búsqueda de información gracias a la utilización de una infraestructura común, mediante la cual, es posible compartir, procesar y transferir información de forma sencilla. Esta Web extendida y basada en el significado, se apoya en lenguajes universales que resuelven los problemas ocasionados por una Web carente de semántica en la que, en ocasiones, el acceso a la información se convierte en una tarea difícil y frustrante.

---

[125]La **Web Semántica** es la nueva generación de la **Web**, que intenta realizar un filtrado automático preciso de la información. Para ello, es necesario hacer que la información que reside en la **Web** sea entendible por las propias máquinas. Especialmente su contenido, más allá de su simple estructura sintáctica.
Con lo cual, podemos determinar que la **Web Semántica** trata sobre diferentes ámbitos, por un lado es un conjunto de lenguajes y procedimientos para poder añadir esa **semántica** a la información para que sea entendible por los agentes encargados de procesarla. Y por el otro lado trata, el desarrollo y la construcción de los agentes encargados de procesar esa información y filtrar la que es útil para los usuarios o para agentes que tienen que realizar una determinada función.

[126]Con una estructura semejante a la de una Wiki, Twine trata de establecer una "red de conocimiento" que ponga en contacto a personas de acuerdo con el conocimiento extraído de sus contribuciones. La infraestructura utilizada por Twine contiene todos los elementos propios de la Web semántica

[127] Radar Networks es una empresa pionera en la concepción de la Web Semántica, o "Web 3.0. que ha desarrollado Twine Web 3.0, una web semántica que define como la "sabiduría de las masas unida a la de las máquinas". Fundada por el visionario Nova Spivack "dispone de una tecnología que detecta relaciones entre bits de información rastreando la Red. La empresa que trabaja para explotar el contenido de páginas de software social, que permiten a los usuarios colaborar para recabar y sumar sus ideas a una amplia gama de contenidos



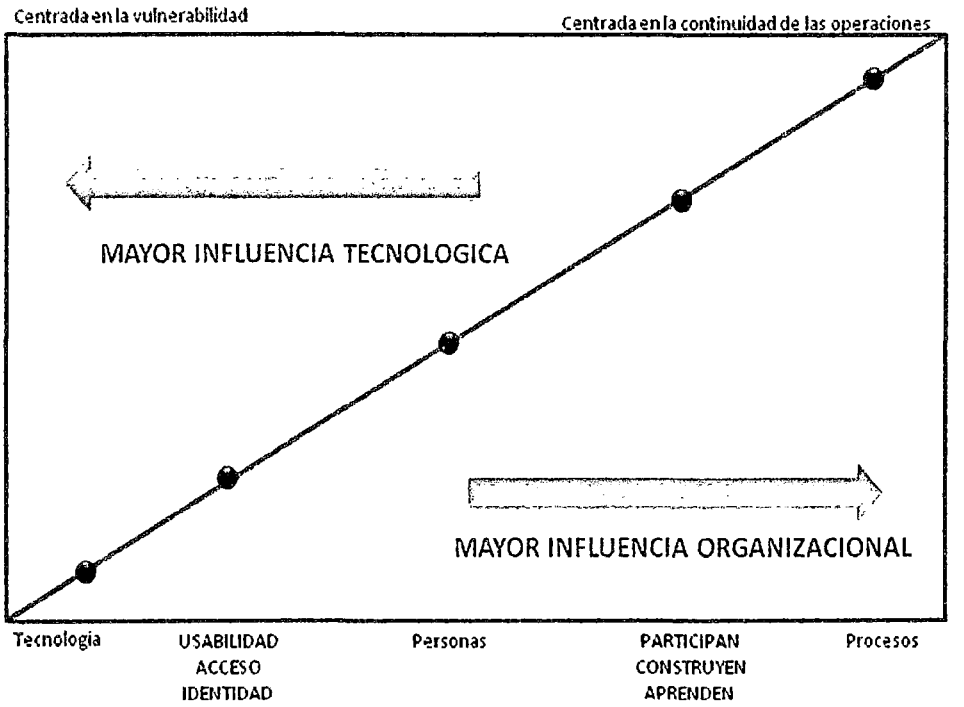
Source: Radar Networks & Nova Spivack, 2007 – www.radarnetworks.com

Ilustración 2 la evolución de la Web desde la era de la PC hasta Web 4.0 representa un salto tecnológico que transformará a la humanidad

Todo esto nos lleva a establecer la asimetría de la inseguridad de la información, que es la razón misma de la existencia de la seguridad informática. Un continuo de experiencias que permiten tanto a profesionales de la seguridad como a curiosos de la inseguridad compartir en un mismo escenario la pasión para descubrir día a día lo sorprendente de la inevitabilidad de la falla.

Es aquí donde se manifiesta el ecosistema tecnológico emergente compuesto por tres elementos: la tecnología, las personas y los procesos; en el entendido que entre personas y tecnología se dan eventos tales como la usabilidad y el acceso a la tecnología, así mismo las personas participan en la identificación de procesos, su construcción y normalización, los aprenden y aplican, creando una identidad entre estos tres elementos, cuanto mayor acceso, usabilidad e identificación con la tecnología se manifestará en las

organizaciones una mayor influencia tecnológica, por tanto la información estará centrada en las vulnerabilidades que proporciona el uso de la tecnología; cuando la relación de las personas es más estrecha con los procesos, entonces habrá una mayor influencia organizacional, por lo tanto la información estará centrada en las operaciones, la ilustración grafica más claramente este fenómeno.



Se aprecia gráficamente la asimetría de la inseguridad de la información; información tomada de UPB – CIBSI 2011 JeimiJ.Cano M. Ph. D. "Cibercrimen 2.0 – evolución y retos para la próxima década 2010-2020"

El objetivo principal del cibercrimen y la guerra de la desinformación (informationwarfare) es manipular la información y las redes de comunicaciones, según indica J. Olson en su tesis de maestría no publicada *Thethreat of systematic and organizedcybercrime and informationwarfare* (2004. American University. Washington D.C. Estados Unidos). Revisada esta afirmación en el contexto de una taxonomía de la inseguridad

informática en sistemas de información, podría decirse que no solamente es manipulación, sino posiblemente fraude, negación del servicio, acto no intencionado o destrucción. Por tanto, la criminalidad informática, cibercrimen, delitos por computador o cualquier denominación semejante, implica comprender no sólo la vulnerabilidad propia explotada, sino el objetivo final perseguido por el infractor.

Los constantes avances tecnológicos y los altos niveles de conocimientos técnicos involucrados en los nuevos desarrollos electrónicos y computacionales, establecen un reto para presentar una definición general de lo que puede denominarse un computercrime o delito por computador o semejante. En este sentido, existen múltiples interpretaciones y sugerencias que buscan modelar esta naciente y conflictiva área para el derecho y las tecnologías de información.

El no contar con una definición concreta sobre el tema desestima los esfuerzos para una adecuada detección, investigación y judicialización de este tipo de conductas en medios electrónicos y computacionales. A pesar de que las estadísticas actuales nos muestran un importante incremento de eventos relacionados con explotación de vulnerabilidades informática en diferentes ramos y campos, dejando pérdidas millonarias para las organizaciones y grandes vacíos en la sociedad sobre las acciones que el Estado toma al respecto, no se han evidenciado avances significativos, ni estrategias desde el punto de vista jurídico, que articulen los limitados esfuerzos adelantados desde la perspectiva de la Administración de la seguridad de la información.

RELACIÓN ENTRE LA CIBERSEGURIDAD Y LA SEGURIDAD NACIONAL

La Seguridad Nacional se desarrolla dentro del ámbito del Ciberespacio para la protección de las infraestructuras críticas, territorio, organizaciones públicas y privadas y los ciudadanos, en términos de asegurar el funcionamiento de las infraestructuras públicas y privadas, que representan centros de gravedad dentro del funcionamiento del estado y cuya neutralización ocasionaría suspender servicios esenciales. La vigilancia y protección del territorio nacional involucra el empleo intensivo de Tecnología de Información y Comunicaciones, el desarrollo de proyectos como el Sistema de Vigilancia Amazónico y Nacional (SIVAN), se constituye como el gran centro proveedor de información para todas las agencias del estado y para el sector privado así como centros de investigación científica, su protección se enmarca dentro de los alcances de esta política dado que representa una plataforma para el desarrollo. El desarrollo de iniciativas como el PIDE, la implementación de la Agenda Digital 2.0, Gobierno Electrónico y Gobierno Abierto, representa desafíos para el estado en términos de garantizar la seguridad dado que se sostienen en Tecnologías de Información y Comunicaciones, por lo que el desarrollo de la capacidad de Ciberdefensa representan un asunto de carácter estratégico para el país.

El diagrama muestra los elementos fundamentales a proteger por el Estado por el uso intensivo de tecnología

Finalmente, los ciudadanos representan el fin supremo del estado, garantizar el acceso a la información pública, transparencia de la información, trámites automatizados, la tendencia a la automatización de todos los procesos del Estado, entre otros aspectos constituye una necesidad de protección por parte del Estado.

2.2. MARCO CONCEPTUAL

Apropiación del nombre o imagen de una persona en provecho propio:

Las bases de datos pueden contener un retrato o fotografía de las personas; que utilizada sin autorización puede implicar una falsa percepción por la imagen proyectada sobre ella.

Intrusión en la intimidad o en los asuntos privados de una persona:

Se refiere a toda forma de recolección de datos que implicará una indagación precisa y ofensiva de los aspectos personales y familiares de una persona.

Revelación Pública de la información privada:

El desarrollo de los registros informáticos y las bases de datos con la creación de redes nacionales e internacionales de trasmisión de datos constituye una amenaza a que la información privada se filtre y sea conocida por el público

Publicidad que genera una falsa percepción del público:

Se presenta en los casos en que una persona se considera ofendida por haberse difundido información erronea sobre ella; cuando la información difundida sea correcta pero ha sido utilizada fuera del contexto adecuado ocasionando una falsa percepción y que la información se a inexacta por su antigüedad sin haber sido actualizada o rectificada.

Honor.

Con respecto al honor, se ha establecido que se trata de un derecho derivado de la dignidad humana, que consiste en no ser escarnecido o humillado ante uno mismo o ante los demás.

Honor interno

El honor interno estaría representado por la estimación que cada persona tiene de sí misma, mientras que el honor externo estaría integrado por el reconocimiento que los demás hacen de nuestra dignidad. De tal distinción se concluye, sin embargo, que la dimensión interna resultaría del todo subjetiva al apelar a las apreciaciones de cada persona que se vea afectada en tal derecho.

Derecho al honor

El derecho al honor protege, entonces, la intangibilidad de la dignidad en la dinámica social de un tiempo determinado. Como ha sostenido nuestro par español, en criterio que hacemos nuestro, el contenido del derecho al honor, que la Constitución garantiza como derecho fundamental (...) es, sin duda, dependiente de las normas, valores e ideas sociales vigentes en cada momento. Tal dependencia se manifiesta tanto con relación a su contenido más estricto, protegidos por regla general con normas penales, como a su ámbito más extenso, cuya protección es de naturaleza meramente civil.

Bombas

Se denominan así a los virus que ejecutan su acción dañina como si fuesen una bomba. Esto significa que se activan segundos después de verse el sistema infectado o después de un cierto tiempo (bombas

de tiempo) o al comprobarse cierto tipo de condición lógica del equipo. (Bombas lógicas).

Camaleones

Son una variedad de virus similares a los caballos de Troya que actúan como otros programas parecidos, en los que el usuario confía, mientras que en realidad están haciendo algún tipo de daño. Cuando están correctamente programados, los camaleones pueden realizar todas las funciones de los programas legítimos a los que sustituyen (actúan como programas de demostración de productos, los cuales son simulaciones de programas reales).

Reproductores

Los reproductores (también conocidos como conejos-rabbits) se reproducen en forma constante una vez que son ejecutados hasta agotar totalmente (con su descendencia) el espacio de disco o memoria del sistema.

Gusanos (Worms)

Los gusanos son programas que constantemente viajan a través de un sistema informático interconectado, de PC a PC, sin dañar necesariamente el hardware o el software de los sistemas que visitan.

Backdoors

Son también conocidos como herramientas de administración remotas ocultas. Son programas que permiten controlar remotamente la PC infectada. Generalmente son distribuidos como troyanos.

Virus en archivos "fantasmas"

Estos virus basan su principio en que DOS, al tener dos archivos con el mismo nombre, ejecuta primero el archivo COM y luego el EXE, siempre y cuando, claro está, ambos archivos se encuentren en el mismo directorio. Al infectar la computadora, el virus crea un archivo COM con el mismo nombre y en el mismo lugar que el EXE a infectar.

Virus de boot sector o sector de arranque

Infectan el sector de booteo o arranque de discos rígidos o diskettes. Las PC se infectan cuando se arranca el equipo con el diskette infectado puesto en la disketera, siempre y cuando el setup de la PC esté programado para arrancar primero desde el drive A:. Si por el contrario el setup inicia primero desde el disco rígido, no es necesario preocuparse por este tipo de virus.

Virus de archivos ejecutables

Infectan los archivos que la PC toma como programas: *.EXE, *.DRV, *.DLL, *.BIN, *.OVL, *.SYS e incluso BAT Estos virus se reproducen por diversas técnicas, infectando al archivo al principio o al final. Siempre es necesario arrancarlos una primera vez dentro del ordenador para que se activen.

"Virus" Bug-Ware

Son programas que en realidad no fueron pensados para ser virus, sino para realizar funciones concretas dentro del sistema, pero debido a una deficiente comprobación de errores por parte del programador, o por una programación confusa que ha tornado desordenado al código final, provocan daños al hardware o al software del sistema.

Los Virus de Macro:

Según la International Security Association, los virus macro conforman el 80% de todos los virus circulantes en el mundo y son los que más rápidamente han crecido en la historia de las computadoras los últimos 7 años.

Virus de e-mail:

Dentro e este grupo, incluyo a dos tipos de virus: los que junto a un mail hacen llegar un atachado que necesariamente debe abrirse o ejecutarse para activar el virus, y dentro de ellos menciono a Melissa como el precursos de esta variedad, y también englobo a los gusanos (worms) que aprovechan los agujeros de seguridad de programas de correo electrónico para infectar a las computadoras, de los cuales BubbleBoy fue el precursor.

Virus de MIRC:

Al igual que los bug-ware y los mail-bombers, no son considerados virus, pero los nombro debido a que tienen características comunes. Son una nueva generación de programas que infectan las PC's, aprovechando las ventajas proporcionadas por internet y los millones de usuarios conectados a cualquier canal IRC a través del programa Mirc y otros programas de chat.

Virus de la WEB:

El lenguaje de programación JAVA, que permite generar los applets para las páginas web y los controles Active X, son lenguajes orientados especialmente a Internet. El ASP es otro tipo de lenguaje basic orientado al desarrollo de aplicaciones basadas en la web.

Virus de arquitectura cliente / servidor:

Esta es una clasificación muy particular, que afecta a usuarios de internet . En este apartado contemplo de manera especial a los troyanos, que más que virus, son verdaderas aplicaciones cliente / servidor, por las cuales cualquier persona, y con la configuración adecuada, puede controlar los recursos de una PC a distancia y a través de una conexión a internet.

Troyanos

Es un programa potencialmente peligroso que se oculta dentro de otro para evitar ser detectado, e instalarse de forma permanente en nuestro sistema. Este tipo de software no suele realizar acciones destructivas por sí mismo, pero entre muchas otras funciones, tienen la capacidad de capturar datos, generalmente contraseñas e información privada, enviándolos a otro sitio.

Correo basura y Spyware

En esta parte vamos a profundizar en dos conceptos: el correo basura (spam) y el spyware (software espía). Además, os ofreceremos una serie de consejos prácticos sobre navegación por la Red y utilización del cliente de correo.

CAPITULO III
CUERPO DE TESIS

3.1. INTRODUCCION

El presente trabajo es una investigación Descriptivo - Explicativo.

Es Descriptiva por cuanto está orientada al conocimiento de la realidad tal como se presenta en una situación espacio – tiempo dado, tiene la capacidad de seleccionar las características fundamentales del objeto de estudio y su descripción detallada de las partes, categorías o clases de dicho objeto.

Es Explicativa por cuanto está orientada al descubrimiento de los factores causales que han podido incidir o afectar la ocurrencia de un fenómeno, en la medida que se analizan las causas y efectos de la relación entre variables. POLIT-HUNGLER (2000)

Diseño: Consideramos que sigue un diseño no experimental, descriptivo correlacional.

Es no experimental porque no existe manipulación de la variable independiente.

Asimismo describe la relación entre dos o más categorías, conceptos o variables en un momento determinado, ya sea en términos correlacionales, o en función de la relación causa-efecto. HERNÁNDEZ (2003:120).

Para ello se hará un análisis de la teoría del derecho a la intimidad, y cuales son las situaciones donde se vulneran el derecho a la intimidad, por la desprotección de los datos personales de los cibernautas peruanos.

Población:

La población de estudio está constituida por los 120 cibernautas que utilizan Internet y que conocen de su ámbito.

Se recurrirá a practicar una encuesta a un sector seleccionado de los cibernautas peruanos, ingenieros informáticos, abogados, operadores informáticos de las instituciones de gobierno.

Muestra:

30 cibernautas

Se efectuará el análisis de los datos mediante la tabulación de los resultados obtenidos de la encuesta practicada.

Presentados los resultados, se procederá a someterlos a técnicas estadísticas que permitan aceptar o rechazar las hipótesis propuestas.

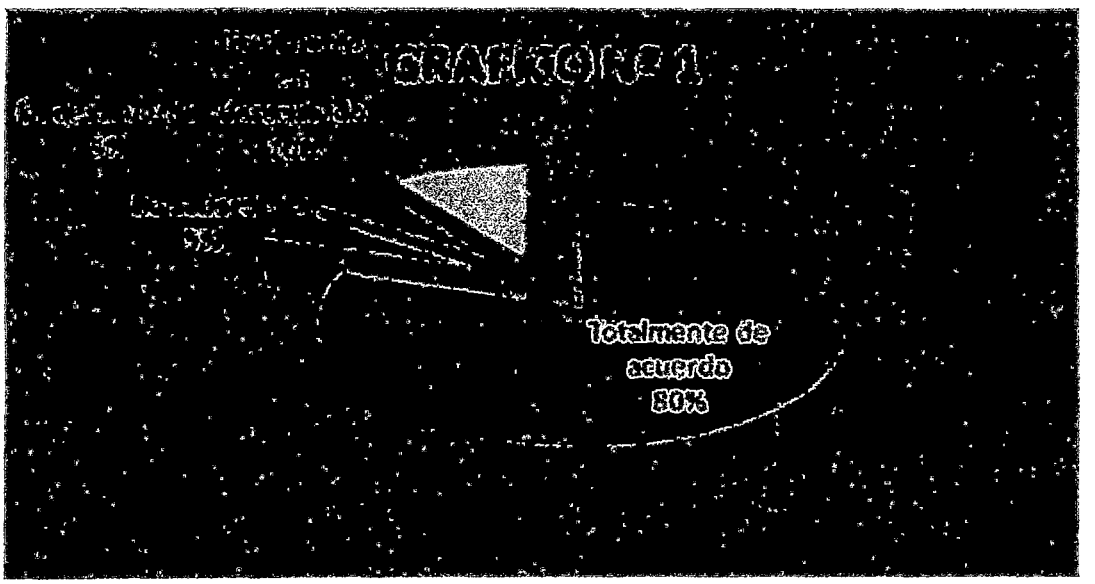
3.2. DESARROLLO DEL TRABAJO DE INVESTIGACION

ACTIVIDADES	TIEMPO (MESES)																	
	Oct.2012		Nov.2012		Dic.2012		Ene2012		Feb2012		Mar.2012		Abr.2012		May.2012		Jun.2012	
	Semanas		Semanas		Semanas		Semanas		Semanas		Semanas		Semanas		Semanas		Semanas	
	1 2	3 4	1 2	3 4	1 2	3 4	1 2	3 4	1 2	3 4	1 2	3 4	1 2	3 4	1 2	3 4	1 2	3 4
1. Elaboración del plan de investigación.	x x	x x	x x	x x	x x													
2. Elaboración y prueba de los instrumentos.						x x												
3. Recolección de los datos.							x x	x x	x x									
4. Tratamiento de los datos.								x x	x x	x x	x x							
5. Análisis de las informaciones.									x x	x x	x x	x x						
6. Constrastación de hipótesis y formulación de conclusiones.										x x	x x	x x	x x					
7. Formulación de propuesta de solución.											x x	x x	x x	x x				
8. Elaboración del informe final.						x x	x x	x x	x x	x x	x x	x x	x x	x x	x x			
9. Correcciones al informe final.							x x	x x	x x	x x	x x	x x	x x	x x	x x			
10. Presentación.																x x		
11. Revisión de la tesis.																x x		
12. Sustentación (**)																x x	x x	x

3.3. PRESENTACION E INTERPRETACION DE RESULTADOS

1.- ¿Esta de acuerdo usted, que en nuestro país, se presenta una desprotección de los datos personales de los cibernautas peruanos, los cuales son expuesto a código malicioso, incide en la vulneración al derecho a la intimidad?

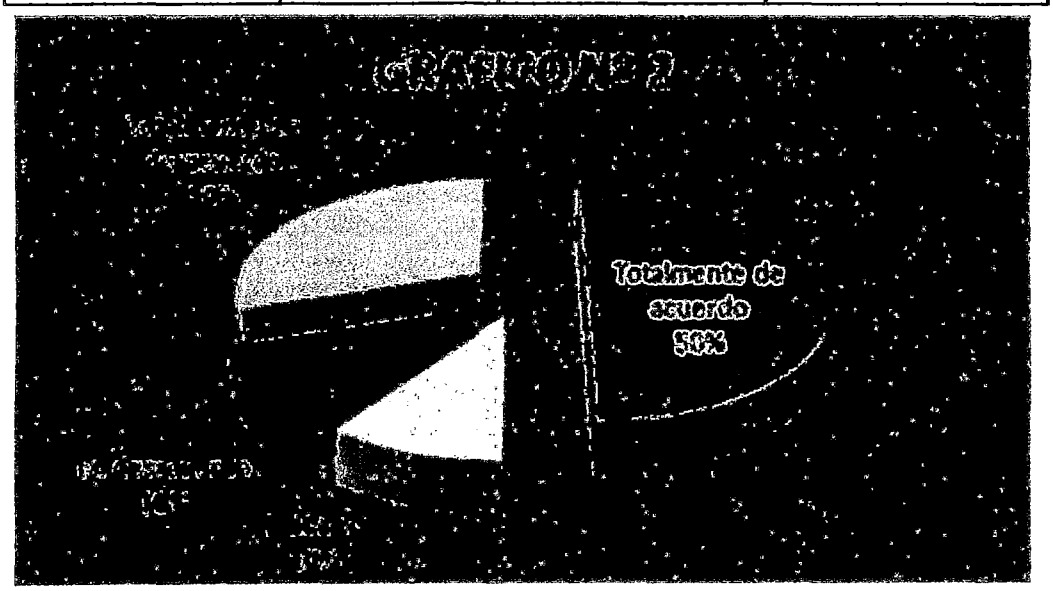
Categorías	Encuestados	Total	%
Totalmente de acuerdo	32	32	80 %
De acuerdo	2	2	5 %
Indeciso			
En desacuerdo	2	2	5 %
Totalmente en desacuerdo	4	4	10 %
Total	40	40	100 %



Teniendo una población de 40 Encuestados, están totalmente de acuerdo en un 80 % que en nuestro país, se presenta una desproteccion de los datos personales de los cibernautas peruanos, los cuales son expuestos a código malicioso, incide en la vulneración al derecho a la intimidad. El desacuerdo es mínimo, así como está totalmente en desacuerdo un 10 % de los encuestados.

2.- ¿Considera usted que la vulnerabilidad de los sistemas de información de la administración publica, aumenta los riesgos que afectan la infraestructura tecnológica y la integridad, confiabilidad y disponibilidad de la información de las entidades gubernamentales?

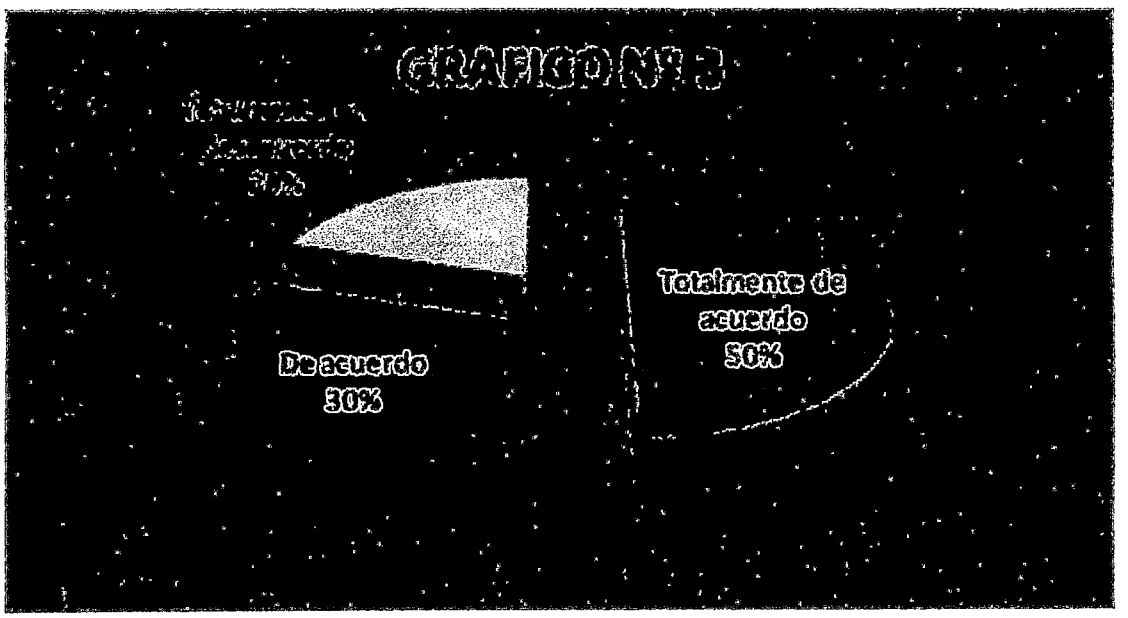
Categorías	Encuestados	Total	%
Totalmente de acuerdo	20	20	50 %
De acuerdo			
Indeciso	4	4	10 %
En desacuerdo	4	4	10 %
Totalmente en desacuerdo	12	12	30 %
Total	40	40	100 %



La respuesta de los Encuestados es diversa aunque hay un 50 % que están de acuerdo que nuestro país, la vulnerabilidad de los sistemas de información de la administración publica, aumenta los riesgos que afectan la infraestructura tecnológica y la integridad, confiabilidad y disponibilidad de la información de las entidades gubernamentales, destacando que un significativo 30 % está totalmente en desacuerdo.

3.- ¿Cree usted que los entes encargados de sancionar a quienes hacen uso ilegal y delictivo de las herramientas informáticas, no tengan cómo judicializar a las nuevos modalidades en contra de los cibernautas?

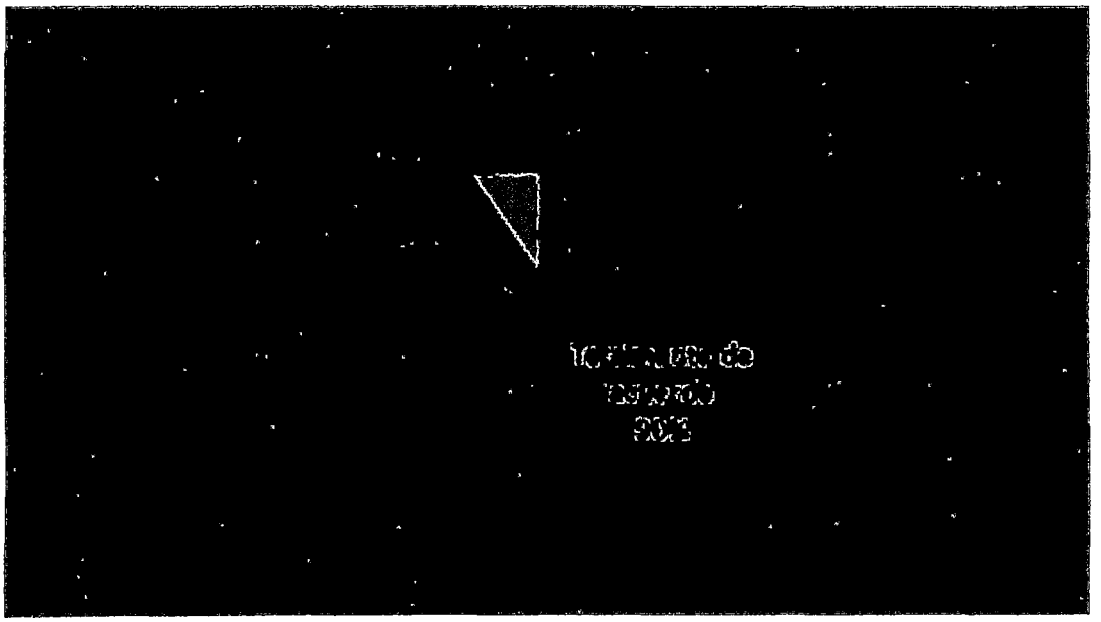
Categorías	Encuestados	Total	%
Totalmente de acuerdo	20	40	50 %
De acuerdo	12	12	30 %
Indeciso			
En desacuerdo			
Totalmente en desacuerdo	8	8	20 %
Total	40	40	100 %



La opinión es diversa pues la mitad de los Encuestados considera quelos entes encargados de sancionar a quienes hacen uso ilegal y delictivo de las herramientas informáticas, no tengan cómo judicializar a las nuevos modalidades en contra de los cibernautas.

4.- ¿Considera usted que el estado no tiene una eficaz procedimiento y políticas de seguridad de la información, que hace vulnerable los datos almacenados?

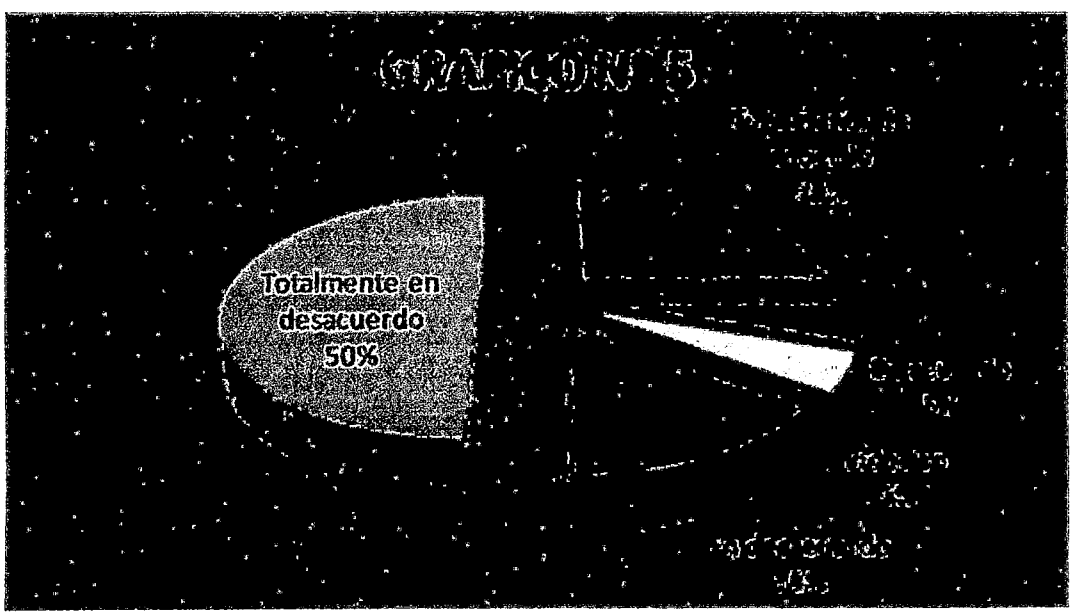
Categorías	Encuestados	Total	%
Totalmente de acuerdo	36	36	90 %
De acuerdo			
Indeciso			
En desacuerdo	2	2	5 %
Totalmente en desacuerdo	4	4	5 %
Total	40	40	100 %



Los Encuestados en esta interrogante es casi unánime un 90% considera que el estado no tiene una eficaz procedimiento y políticas de seguridad de la información, que hace vulnerable los datos almacenados, totalmente en desacuerdo es el 5%. Y en desacuerdo es un 5%.

5.- ¿Esta de acuerdo usted que el estado debe imponer sanciones penales a las personas que incurran en las conductas que vulneren el derecho a la intimidad?

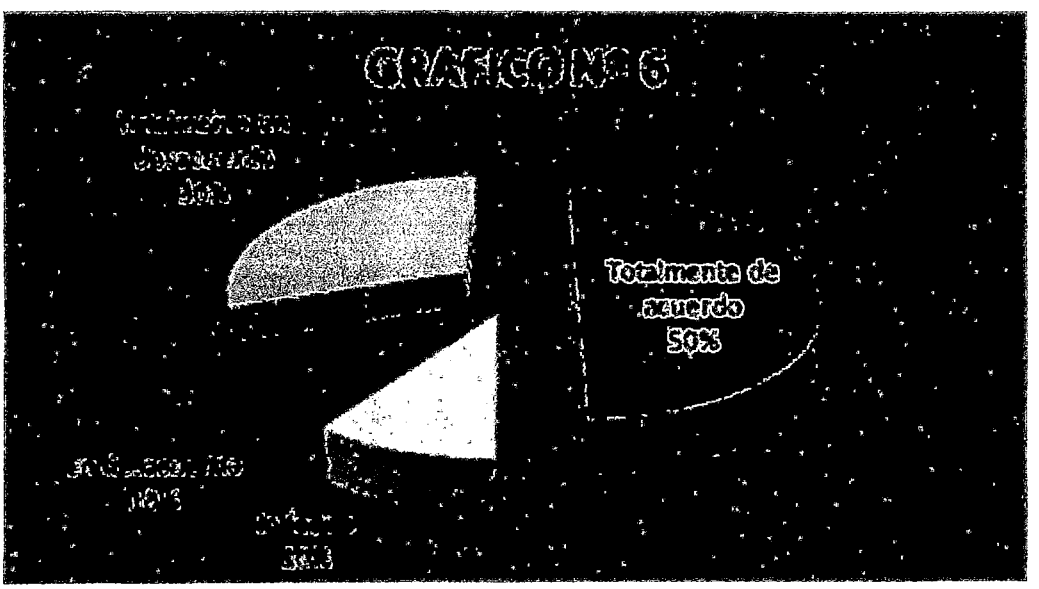
Categorías	Encuestados	Total	%
Totalmente de acuerdo	10	10	25 %
De acuerdo	2	2	5 %
Indeciso	2	2	5 %
En desacuerdo	6	6	15 %
Totalmente en desacuerdo	20	20	50 %
Total	40	40	100 %



Es una de las preguntas más controversiales en donde los Encuestados no se ponen de acuerdo, solo un 25 % acepta queel estado debe imponer sanciones penales a las personas que incurran en las conductas que vulneren el derecho a la intimidad, destacando que un 50 % está totalmente en desacuerdo.

6.- ¿Esta de acuerdo usted que hay una necesidad de contar con un derecho que regule la libertad de información como factor indispensable para el desarrollo del individuo y la sociedad y que manifieste sus límites para defender los márgenes de la intimidad necesarios para el normal desarrollo de la personalidad humana?

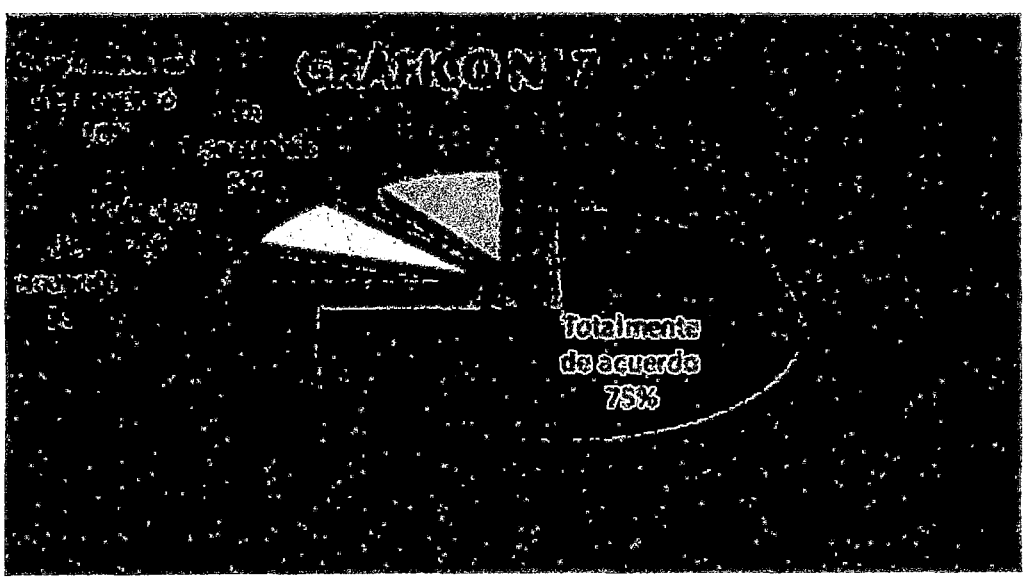
Categorías	Encuestados	Total	%
Totalmente de acuerdo	20	20	50 %
De acuerdo			
Indeciso	4	4	10 %
En desacuerdo	4	4	10 %
Totalmente en desacuerdo	12	12	30 %
Total	40	40	100 %



La mitad de los Encuestados entrevistados han señalado que hay una necesidad de contar con un derecho que regule la libertad de información como factor indispensable para el desarrollo del individuo y la sociedad y que manifieste sus límites para defender los márgenes de la intimidad necesarios para el normal desarrollo de la personalidad humana, aunque hay un porcentaje elevado que no está totalmente en desacuerdo.

7.- ¿Considera usted que se deben ofrecer soluciones mediante la criptografía, programas que permitan nuestro anonimato o nuevos protocolos de comunicación que nos permitan dirigir a quiénes entregamos información y dosificarla verdaderamente?

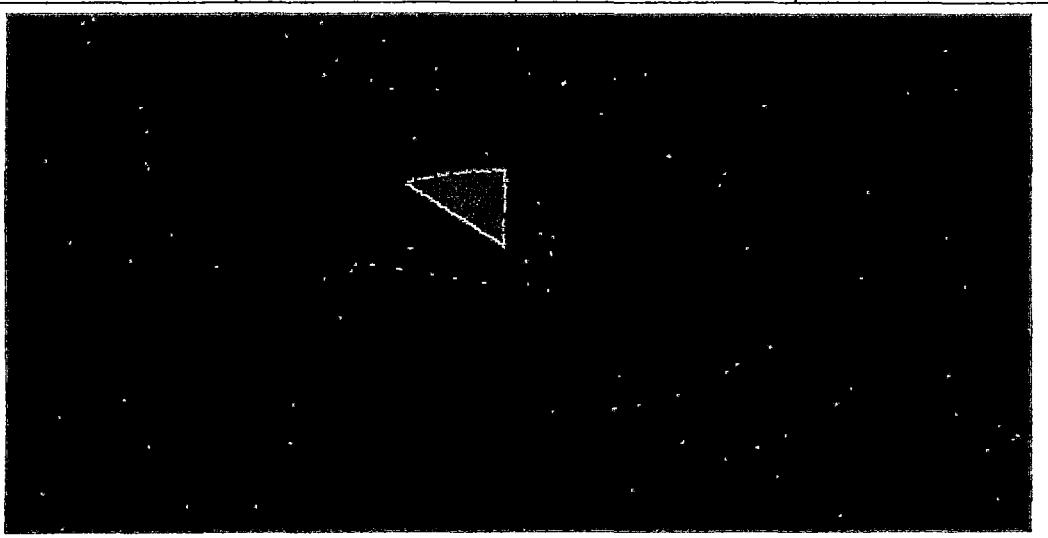
Categorías	Encuestados	Total	%
Totalmente de acuerdo	30	30	75 %
De acuerdo	2	2	5 %
Indeciso	3	3	7.5 %
En desacuerdo	1	1	2.5 %
Totalmente en desacuerdo	4	4	10 %
Total	40	40	100 %



Los Encuestados, ante la interrogante, que se deben ofrecer soluciones mediante la criptografía, programas que permitan nuestro anonimato o nuevos protocolos de comunicación que nos permitan dirigir a quiénes entregamos información y dosificarla verdaderamente, resaltan un alto porcentaje de aprobación (75 % está de acuerdo), sumado al tímido 5 % que está de acuerdo.

8.- ¿Considera usted que Respecto al consentimiento que debe brindar el cibernauta en la red informática, se debe establecer que el consentimiento expreso y escrito motivo por el cual los sitios Web que registren usuarios deberán tener la posibilidad de que el usuario otorgue su consentimiento inequívoco en forma previa a realizar su registró, aceptando las condiciones de la misma?

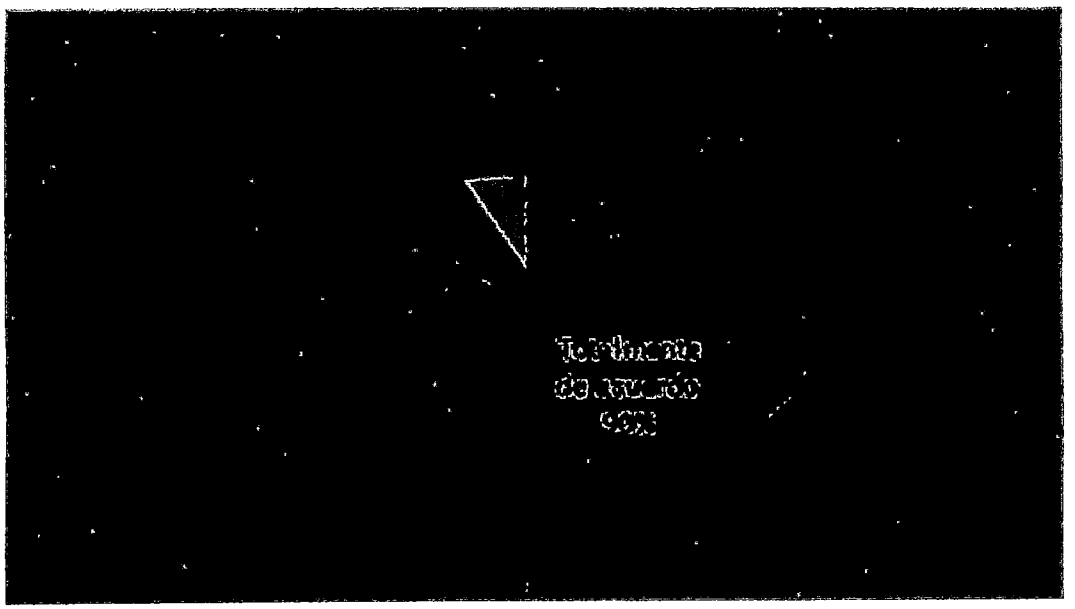
Categorías	Encuestados	Total	%
Totalmente de acuerdo	32	32	80 %
De acuerdo	4	4	5 %
Indeciso			
En desacuerdo	2	24	5 %
Totalmente en desacuerdo	2	2	10 %
Total	40	40	100 %



Interrogante de una abrumadora respuesta, un 80 %, considera que respecto al consentimiento que debe brindar el cibernauta en la red informática, se debe establecer que el consentimiento expreso y escrito motivo por el cual los sitios Web que registren usuarios deberán tener la posibilidad de que el usuario otorgue su consentimiento inequívoco en forma previa a realizar su registró, aceptando las condiciones de la misma, el desacuerdo es mínimo solo un 10 %.

9- ¿Esta de acuerdo usted que los sitios que no realizan registro pero que captan datos deberán dejar claro cuales son las condiciones de uso del sitio a través de algún vínculo, para que el cibernauta esté informado de los datos que recabarán?

Categorías	Encuestados	Total	%
Totalmente de acuerdo	36	36	90 %
De acuerdo	2	2	5 %
Indeciso			
En desacuerdo			
Totalmente en desacuerdo	2	2	5 %
Total	40	40	100 %



Otra abrumadora respuesta donde los encuestados en un 80% están totalmente de acuerdo que los sitios que no realizan registro pero que captan datos deberán dejar claro cuales son las condiciones de uso del sitio a través de algún vínculo, para que el cibernauta esté informado de los datos que recabarán.

Los resultados de las encuestas dirigidas a los profesionales inmersos en nuestra investigación, como en este caso, son cibernautas que utilizan Internet y que conocen su ámbito, los encuestados, tienen una lectura diferente del tema de nuestra investigación, se han planteado interrogantes con la finalidad, que los entrevistados, a través de sus respuestas, den su apreciación, sobre nuestra propuesta, tema, que, como hemos resaltado novísimo, que no tiene antecedentes, ni propuestas, pero como hemos demostrado en el diagnostico sobre nuestra problemática, urge que se legisle y se desplieguen estrategias.

Vemos de la respuesta de los encuestados, se presenta la necesidad de una legislación, pero, ¿qué se debe legislar?: ¿toda la red?, ¿sólo algunos aspectos?, ¿cuáles de ellos? (propiedad intelectual, copyright, delitos a través de la red, intimidad); la ética y la moral ¿deben tener algún papel?

Otros entendidos opinan que, para sancionar los delitos que se puedan cometer en Internet, basta con las leyes penales actuales y que, en todo caso, lo que se debe hacer es actualizar las leyes que ya existen.

La Unión Europea, por ejemplo, no ha establecido ninguna ley especial sobre Internet, salvo una relacionada con el comercio electrónico: http://europa.eu.int/eur-lex/es/lif/dat/2000/es_300L0031.html .

El primer país de la Unión Europea en elaborar un proyecto de ley que regule expresamente el tema de los contenidos en Internet fue Alemania.

Por su parte, otros países desarrollados como Canadá y Estados Unidos han creado desde hace varios años políticas legales en cuanto a la regulación de los contratos de compraventa a través de Internet http://publicaciones.derecho.org/redi/No._39_-_Octubre_del_2001/2.

El sistema que se aplica es el mismo que se utiliza en el caso de las transacciones realizadas telefónicamente.

Francia, a su vez, trabaja en un anteproyecto de ley acerca de la sociedad de la información, que se puede consultar en la página http://www.iris.sgdg.org/documents/rapport-lsi-apl/. También países latinoamericanos, como Argentina, trabajan para concebir un marco regulatorio en relación con la conectividad y el acceso a Internet (http://www.it-cenit.org.ar/Seminarios/DerEconDIG2000/material/ /marcreg/marcreg.htm).

En este sentido, Argentina ha empezado a desarrollar legislaciones relacionadas con los proveedores de acceso a Internet o la libertad de expresión a través de la red. Otros países, por ejemplo Chile, han creado leyes de protección legal de datos personales frente al tratamiento computacional (Ley 19.628, de agosto de 1999) y de espionaje informático (previsto en la Ley chilena 19.223).

Uno de los primeros problemas que se presenta a la hora de establecer leyes para el ciberespacio es que ni siquiera hay acuerdo acerca de los conceptos básicos. Por ejemplo en el caso del comercio electrónico no hay acuerdo ni entre los países de la Unión Europea ni para otros fuera de ella. Algunos consideran que la información es un producto comercial, mientras otros opinan que la información debe estar libre de toda presión política y comercial; aseguran que la información es un derecho.

Cada país tiene una sensibilidad concreta, una acentuación especial en asuntos de moral y también de seguridad, en definitiva, cada uno tiene una personalidad. Siendo esto importante, no lo es menos la supranacionalidad de la red, que va más allá de los Estados, más allá de las naciones, de los pueblos; esto sucede al mismo tiempo que

todos están presentes en Internet; se podría decir que los engloba a todos pero sin ponerles uniforme.

Los legisladores son conscientes de que las leyes de cada país deben tener en cuenta al país vecino y al de más allá. Si es posible deben evitar casos como el acontecido entre Francia y EE.UU., por las subastas de artículos nazis a través de la sede del portal Yahoo en los Estados Unidos. Un juez francés dictaminó la retirada de dicha subasta, pero otro juez estadounidense rechazó el dictamen, alegando que no podía privar a sus ciudadanos de un derecho tan importante como la libertad de expresión. Al final, Yahoo retiró esos artículos por voluntad propia, no porque lo dijera un juez desde Francia.

A diferencia de otros asuntos, como las leyes laborales, sanitarias o de educación, que los técnicos de los partidos políticos discuten y elaboran sin ninguna -o casi ninguna- participación de los ciudadanos, en todas las cuestiones legales sobre Internet son los ciudadanos los que ponen al día a los políticos sobre la red. Estos saben que no se enfrentan a sus adversarios, sino a los internautas, a los ciudadanos (http://www.internautas.org, http://www.aui.es, http://www.aece.org y http://www.kriptopolis.com/net/). El colectivo inglés GreenNet (http://www.gn.apc.org, en inglés), como otros de Europa y de EE.UU., se oponen al carácter policial del proyecto de legislación británica sobre Internet.

Sea como fuere, las nuevas leyes referidas al fenómeno Internet y demás tecnologías no deben perder de vista a las más necesitadas y débiles de nuestra sociedades. Más bien al contrario, las leyes deben dar prioridad a la protección de algunos grupos de la población más vulnerables o más expuestos a las amenazas de una Internet "sin límites". Los niños, por ejemplo, son susceptibles de ser abandonados a su suerte, pues algunos países tienen unas leyes de protección a la

infancia, pero no todas se pueden aplicar a Internet; la venta de pornografía está más o menos prohibida, pero si en la práctica no se cumple la prohibición, ¿qué sentido tienen? y ¿quién puede garantizar que una ley -si es que existe- se cumpla en Internet?

3.4. CONTRASTACION DE HIPOTESIS

De lo hasta aquí desarrollado a lo largo de la presente investigación, con la información doctrinaria expuesta y la información estadística presentada en los anteriores capítulos y las encuestas o cuestionarios aplicados a los cibernautas; hemos podido demostrar la hipótesis planteadas al inicio del presente trabajo como respuesta tentativa a esta investigación-

El análisis y contrastación de las variables independientes y dependientes correspondiente a nuestras hipótesis objeto de la presente tesis, nos permitió determinar lo siguiente:

HIPÓTESIS GENERAL.

SI SE VIENE DANDO UNA DESPROTECCION DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS, EXPUESTOS A CÒDIGO MALICIOSO ENTONCES NO SE EVITARA LA VULNERACIÓN DE LA INTIMIDAD DE LAS PERSONAS.

VI: DESPROTECCION DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS EXPUESTOS A CÒDIGO MALICIOSO.

Como se ha destacado en nuestro planteamiento, el desarrollo de la tecnología viene acompañado casi siempre de consecuencias negativas por su equivocado uso, inclusive de carácter moral y ético, toda vez que, el uso frecuente de computadoras y de la posibilidad de

su interconexión a nivel global da lugar a un verdadero fenómeno de nuevas dimensiones. Lo que resulta incuestionable es que tenemos que asumir y estar preparados para enfrentarnos en algún momento la posibilidad de ser víctimas de la vulneración de nuestra intimidad, de nuestros datos personales que son expuestos a código malicioso.

Bastaría para realizarlo tener una computadora conectada a una red de transmisión de datos, y descubrir aunque sea a veces, por casualidad la clave de acceso a la información ingresando de esta manera indebidamente a un sistema informático para así consumar el delito, -sin contar claro - con la ayuda de los numerosos manuales de navegantes piratas.

Desde el momento que nos conectamos a Internet, nuestro equipo se encuentra vulnerable a diversos tipos de ataques, desde virus, hasta intrusiones.

Debido al continuo desarrollo de nuevos virus, y al descubrimiento de fallos de seguridad en los sistemas operativos, actualmente es imposible garantizar al cien por cien la inmunidad de un ordenador. Lo único que podemos hacer es reducir el riesgo lo máximo posible. Además, también habría que recalcar que la mayoría de los ataques son aleatorios, aunque últimamente son más los que buscan una información concreta o la obtención de un servicio gratuito.

Por ello en la obtención de passwords, códigos y claves. este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que

prueban millones de posibles claves hasta encontrar la password correcta. Es muy frecuente crackear una password explotando agujeros en los algoritmos de encriptación utilizados, o en la administración de las claves por parte la empresa.

Por ser el uso de passwords la herramienta de seguridad mas cercana a los usuarios, es aquí donde hay que poner énfasis en la parte "humana" con políticas claras (¿como se define una password?, a quien se esta autorizado a revelarla?) y una administración eficiente (cada cuanto se están cambiando?) No muchas organizaciones están exentas de mostrar passwords escritas y pegadas en la base del monitor de sus usuarios, u obtenerlas simplemente preguntando al responsable de cualquier PC, cual es su password?.

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" han sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de red, browsers de Internet, correo electrónico y todas clases de servicios en LAN o WANs.

Sistemas operativos abiertos como Linux tienen agujeros más conocidos y controlados que aquellos que existen en sistemas operativos cerrados, como Windows Server. Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad (y herramientas de hacking que los explotan), por lo que hoy también se hace indispensable contar con productos que conozcan esas debilidades y puedan diagnosticar un servidor, actualizando su base de datos de periódicamente.

Además de normas y procedimientos de seguridad en los procesos de diseño e implementación de proyectos de informática

VD. VULNERACIÓN DE LA INTIMIDAD DE LAS PERSONAS.

Se desprende de nuestra investigación que el Estado no cumple con garantizar el derecho a la vida privada, "*el derecho a que lo dejen a uno tranquilo*". El derecho del individuo a impedir la intromisión no autorizada de los funcionarios públicos o de otros individuos en su propia casa, en su correspondencia o en sus pensamientos, su derecho a proteger el hogar, sus comunicaciones, incluso su tiempo libre, es un elemento esencial de la libertad personal.

El derecho a la intimidad, como un derecho reconocido por nuestra Carta Política Nacional, debe de ser respetado inescrupulosamente por todos aquellos, que de alguna forma, con la manipulación de ciertos datos, a través de la informática, tienen acceso a dicha información, máxime cuando casi la totalidad de bases de datos por no decir todas se encuentran digitalizadas, es decir que todos nosotros queramos o no, ya formamos parte de una cadena de datos, almacenados en un computador, y que quien tenga acceso a ello, debe pues respetar los parámetros normativos que protegen el sagrado derecho a la intimidad personal; y que si bien la informática ha permitido procesar, almacenar y tener acceso a ingentes cantidades de información, ello también a conllevado a una vulneración del derecho a la intimidad y privacidad, trastocando con ello el equilibrio normativo que existía antes de la irrupción de la tecnología en este campo.

Si bien las conductas ilícitas que trastocan el normal desarrollo del derecho a la intimidad, tienen un protección en nuestra Constitución y en el actual Código Penal, ello no es óbice para que se implementen campañas de concienciación respecto a la debida protección de la información y sobretodo en salvaguarda del derecho a la intimidad, dado a que muchas veces somos testigos de la presencia de centenares de normas, y que el ciudadano hace un saludo a la

bandera de tales disposiciones, radicando ello en un problema de persona, el cual se debe de corregir a través de tales difusiones.

Las redes sociales disponibles en Internet suponen un foco importante de documentación y datos para los delincuentes informáticos, ya que en ellas se obtiene gran cantidad de información personal. El peligro radica en que no sólo afecta a la integridad del usuario, sino a la de los allegados, ya que al agregarlos como "amigos" en estas redes sociales, ponen a disposición del delincuente datos que usará sin consentimiento.

Otro peligro añadido es que parte de los usuarios son menores de edad, por lo que se considera que la única medida eficaz contra la violación de la intimidad es la educación por la prevención en el mundo virtual. Los delitos informáticos tienen difícil resolución debido a la insuficiente legislación y la operatividad de las investigaciones.

Se producen delitos informáticos de diversa índole como la estafa, la pornografía, el acoso a las parejas o el ciberterrorismo, también llamado "guerra de cuarta generación". Debido a la gran variedad de delitos y a la ausencia de datos fiables, las estadísticas de resolución es escasa, aunque en los últimos años las denuncias por violación de derechos a través de la red se han incrementado en un 25 ó 30 por ciento. Por último, la necesidad de tener bien protegido el ordenador personal y controlar la cesión de datos para evitar estas situaciones.

La participación en estas redes no esta exenta de riesgos, como los robos de identidad. O la averiguación de antecedentes o conductas por parte de los actuales o posibles empleadores de algún usuario. Puede leer más sobre estos temas en la nota relacionada al final.

Esta falta de privacidad abre nuevas oportunidades de negocio para desarrolladores de software que proveen servicios de redes sociales privadas a organizaciones que deben mantener relaciones con un gran número de personas en forma periódica.

Hipótesis 1

La vulnerabilidad de los sistemas de información de la administración publica, por la falta de una legislación eficaz, aumenta los riesgos que afectan la infraestructura tecnológica y la integridad, confiabilidad y disponibilidad de la información de las entidades gubernamentales.

VI: VULNERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA ADMINISTRACIÓN PÚBLICA

Asistimos progresivamente un paulatino incremento de los procedimientos administrativos que se pueden iniciar por vía telemática. Por ejemplo, las declaraciones tributarias del impuesto sobre la renta, determinadas solicitudes en materia de corporaciones locales, declaraciones a efectos de cotizaciones de trabajadores, registros públicos, etc.

Los datos que se aportan en dichas transmisiones son altamente sensibles, en muchas ocasiones. La información que viaja por la red nos puede permitir conocer detalles realmente íntimos de las personas.

Ante esto, nos encontramos con el problema de la seguridad del viaje y almacenamiento de la información. Está claro que LA INVERSIÓN EN SEGURIDAD DEBE DE SER UNA PRIORIDAD DE LA ADMINISTRACIÓN. Las "medidas de seguridad digitales" deben de ser tan importantes como lo son los sistemas de alarma y vigilantes

que se ubican en los espacios físicos donde se encuentra la documentación administrativa.

Desde aquí queremos lanzar a debate si por parte de las administraciones se invierte lo suficiente en la seguridad en los procedimientos telemáticos administrativos. No olvidemos que está al alcance de la mano de una persona que sepa aprovechar cualquier vulnerabilidad de los sistemas un caudal enorme de información sensible.

VD: RIESGOS QUE AFECTAN LA INFRAESTRUCTURA TECNOLÓGICA Y LA INTEGRIDAD, CONFIABILIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN DE LAS ENTIDADES GUBERNAMENTALES.

La información que se considera dato personal es muy amplia, ya que es cualquier información asociada a una persona física. Todos los días generamos datos personales, pues todos los días efectuamos transacciones, facilitamos números de teléfono, y a la vez estamos en contacto con los datos, escuchamos programas de televisión con confidencias y rumores sobre personas, y así un sinfín de conductas.

El control de los datos por las administraciones implica por tanto, un poder de conocimiento sobre nuestra vida, conocimiento que precisa de unas garantías en su utilización. Si se tiene acceso indiscriminadamente a nuestras cuentas bancarias con la excusa de investigar un supuesto blanqueo, a nuestra historia clínica para localizar lesiones en tal día, a la relación de vuelos y desplazamientos en tren que hemos hecho, a las habitaciones de hotel en las que hemos estado por las reservas, fácilmente se podrá saber la vida de una persona "al dedillo".

La línea fronteriza entre la intimidad/privacidad y la seguridad como bien emergente en el siglo XXI, hasta que punto es legítimo el acceso a los distintos datos informatizados que se esparcen por todas partes para combatir los delitos organizados, es sin duda, el debate prevalente en la sociedad cuando hablamos de tratamiento de los datos personales por la Administración. Es muy importante, por ello, obtener unas conclusiones claras y bien fundamentadas sobre el tema, pues mucho me temo que es la moda que se avecina.

El volumen de información que acumulan las organizaciones públicas es cada vez mayor. Y esto no es precisamente una tendencia a la baja, todo lo contrario, cada vez es más intenso y mayor. Progresivamente van aumentando nuestras obligaciones de declarar o facilitar datos, registrarnos, etc.

No es para nada descabellado pensar que en no mucho tiempo, la Administración – en singular – tendrá un conocimiento exhaustivo sobre la vida de las personas, lo que unido al desarrollo tecnológico hace que potencialmente –y en un futuro no muy lejano – en un vistazo se podrá llegar a disponer de un perfil de nuestra personalidad.

Las comunicaciones son la base de los negocios modernos, pues sin las mismas ninguna empresa podría sobrevivir. Por tal razón, es necesario que las organizaciones mantengan sus servidores, datos e instalaciones lejos de los hackers y piratas informáticos.
La temática de la privacidad de las redes ha ido cobrando, desde hace más de una década, un lugar bien importante en el entorno del desarrollo de la informática, ya que las empresas se sienten amenazadas por el crimen informático y busca incansablemente tecnologías que las protejan del mismo, para lo cual destinan partidas en sus presupuestos para fortalecer la seguridad de la información y de las comunicaciones.

El mantener una red segura fortalece la confianza de los clientes en la organización y mejora su imagen corporativa, ya que muchos son los criminales informáticos (agrupaciones, profesionales, aficionados y accidentales) que asedian día a día las redes. De forma cotidiana estos hackers aportan novedosas técnicas de intrusión, códigos malignos más complejos y descubren nuevos vacíos en las herramientas de software.

Las redes son sistemas de almacenamiento, procesamiento y transmisión de datos que están compuestos de elementos de transmisión (cables, enlaces inalámbricos, satélites, encaminadores, pasarelas, conmutadores, etc.) y servicios de apoyo (sistema de nombres de dominio incluidos los servidores raíz, servicio de identificación de llamadas, servicios de autenticación, etc.).

Conectadas a las redes existe un número cada vez mayor de aplicaciones (sistemas de entrega de correo electrónico, navegadores, etc.) y equipos terminales (servidores, teléfonos, computadoras personales, teléfonos móviles, etc.).

Así pues, las redes en las empresas, son los medios que permiten la comunicación de diversos equipos y usuarios, pero también están propensas a ser controladas o accesadas por personas no autorizadas. Cuando nos referimos a la privacidad de la red, se evoca al cuidado o medidas establecidas para que la información de los sistemas como puede ser datos de clientes, servicios contratados, reportes financieros y administrativos, estrategias de mercado, etc., no sea consultada por intrusos.

Las redes deben cumplir los siguientes requisitos o características para mantener su privacidad y poder ser más seguras ante las posibilidades de intrusión.

Hipótesis 2

Mientras los entes encargados de sancionar a quienes hacen uso ilegal y delictivo de las herramientas informáticas, no tengan cómo judicializar a las nuevos modalidades en contra de los cibernautas.

VI: ENTES ENCARGADOS DE SANCIONAR A QUIENES HACEN USO ILEGAL Y DELICTIVO DE LAS HERRAMIENTAS INFORMÁTICAS.

El estado que es el encargado de velar por la protección de los derechos fundamentales de las personas.

A nivel operacional, el rol del fiscal es relevante, unido a la responsabilidad de la Policía Nacional del Perú, representada por la DIVINDAT, tiene la gran responsabilidad, no sólo de dar solución al impacto de los delitos informáticos, como medida represiva, sino también implementar cambios, respecto a la verificación de la utilización de herramientas de control, evaluación de riesgos, así como en el establecimiento de medidas de protección que ayuden a las personas naturales y/o jurídicas a minimizar las amenazas que presentan los delitos informáticos. La ocurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que éstas se beneficien de todo lo que proveen las tecnologías de información (comunicación remota, Interconectividad, comercio electrónico, etc.); sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

VD: JUDICIALIZACIÓN A LAS NUEVOS MODALIDADES EN CONTRA DE LOS CIBERNAUTAS.

Obviamente no hay una legislación especializada en este tipo de accionar genuino, No solo basta con dotar de normas legales que sancionen las conductas que afecten a cualquier bien jurídico mediante el uso de alguna herramienta informática, es necesario establecer todo un sistema normativo que desarrolle y regule los mecanismos básicos que se emplean en los manejos a nivel electrónico.

Hipótesis 3

A una aplicación efectiva de procedimientos y políticas de seguridad de la información; que utiliza el estado y, se podrá determinar las acciones penales contra las personas que incurran en las conductas que vulneren el derecho a la intimidad.

VI: APLICACIÓN EFECTIVA DE PROCEDIMIENTOS Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN QUE UTILIZA EL ESTADO

La Seguridad Informática, es un compromiso de las instancias técnicas por estar preparadas para actuar y regular el efecto que dicho incidente puede ocasionar a la empresa u organismo gubernamental. Administrar un incidente de seguridad requiere experiencia y habilidades técnicas para controlar las acciones del atacante, pero al mismo tiempo habilidad y pericia para establecer los rastros y registros de dichas acciones con las cuales relacionar las acciones y efectos ocasionados por el intruso dentro del sistema. Es necesario que toda institución cree una política simple y genérica para su sistema, de forma que los usuarios puedan entenderla y seguirla con facilidad. Esta política deberá proteger los datos y también la privacidad de los usuarios. Algunas preguntas que son necesarias

tener en cuenta para la creación de una política de seguridad son las siguientes:

¿Quién tiene acceso al sistema?

¿A quién le está permitido instalar software en el sistema?

¿Quién es el responsable de los datos?

¿Quién tiene la capacidad de recuperar la máquina de un ataque ya sea por virus o por individuos?

¿Quién analiza si el sistema esta siendo utilizado apropiadamente?

VD: ACCIONES PENALES CONTRA LAS PERSONAS QUE INCURRAN EN LAS CONDUCTAS QUE VULNEREN EL DERECHO A LA INTIMIDAD.

Dentro del Código Penal se tipifican los siguientes delitos que tienen aplicación directa en el campo informático, y que se considera que guardan relación con el concepto general de los delitos informáticos:

a. Delito de Violación a la Intimidad En el artículo 154 está tipificado el Delito de violación a la intimidad, establece que: "el que viola la intimidad de vida personal y familiar ya sea observando, escuchando oregistrando un hecho, será reprimido con pena privativa de libertad aumentando la pena cuando publica la intimidad conocida.

La base de datos computarizados se considera que están dentro del precepto de "cualquier archivo que tenga datos", en consecuencia estaría tipificado el delito de violación a la intimidad utilizando la informática y la telemática a través del archivo, sistematización y transmisión de archivos que contengan datos privados que sean divulgados sin consentimiento.

Delito de hurto, agravado por Transferencia Electrónica de fondos, telemática en general y empleo de clavessecretas.

El artículo 185 establece: "el que, para obtener provecho, se apodera ilegítimamente de un bien total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. Se equipara a bien mueble la energíaeléctrica, el gas, el agua y cualquier otro elemento que tenga valor económico, así como el espectro electromagnético".

El artículo 186, segundo párrafo numeral 3 modificado por la Ley 26319 – dispone además "la pena será no menor de cuatro años ni mayor de ocho si el hurto es cometido mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas".

El delito de hurto agravado por transferencia electrónica de fondos tiene directa importancia en la actividad informática. El sistema de transferencia de fondos, en su conjunto, se refiere a la totalidad de las instituciones y prácticas bancarias que permiten y facilitan las transferencias interbancarias de fondos.
Uno de los medios de transferencia electrónica de fondos se refiere a colocar sumas de dinero de una cuenta a otra, ya sea dentro de la misma entidad financiera o una cuenta en otra entidad de otro tipo, ya sea pública o privada. Con la frase "telemática en general" se incluye todas aquellastransferencias u operaciones cuantificables en dinero que pueden realizarse en la red informática ya sea con el uso de Internet, por ejemplo en el Comercio Electrónico o por otro medio. Cuando se refiere a "empleo de claves secretas" se está incluyendo la vulneración de password, de niveles de seguridad, de códigos o claves secretas.

La figura penal peruana de hurto informático carece de antecedentes legales, lo que patentiza el esfuerzo técnico legislativo por aprehender en un solo tipo penal comportamientos matizados y complementarios entre síLas dificultades para ubicar sistemáticamente bajo el contexto típico del hurto a los ilícitos electrónicos de transferencias de fondos o de activos patrimoniales en general, obstaculizados por la idea de la corporeidad y asibilidad del bien mueble, no han encontrado mayores dificultades en el contexto del tipo peruano de hurto, que cataloga también como bienes muebles a las energías y elementos que tengan valor económico, en la medida que éstos puedan ser reconducibles o registrables; y transferibles en el caso del hurto informático.

El hurto informático, sin embargo, no agota en modo alguno las diversas expresiones de delictividad informática y telemática; quedan numerosas hipótesis necesitadas de regulación punitiva. Esta afirmación no implica querer rebasar la subsidiariedad del derecho penal, ni el principio de última ratio, sino que expresa necesidades que se patentizarán en el curso de la mayor internacionalización y globalización de la economía peruana, y el crecimiento de los usuarios del ciber mercado, los contratos informáticos ydemás operaciones en red.

c. Delito de Falsificación de documentos informáticos El Decreto Legislativo 681 modificado por la Ley 26612, es la norma que regula el valor probatorio del documento informático, incluyendo en los conceptos de microforma y micro duplicado tanto al microfilm como al documento informático. El artículo 19 de esta norma establece que: "la falsificación y adulteración de microformas, micro duplicados y microcopias sea durante el proceso de grabación o encualquier otro momento, se reprime como delito contra la fe pública, conforme las normas pertinentes del Código Penal".

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

PRIMERO. El ciberespacio es un mundo virtual en el cual los defectos y actos ilegales del ser humano se reproducen con la misma facilidad que sus virtudes y negocios legales. Con el uso de las nuevas tecnologías, la masificación de las computadoras y la creciente difusión de Internet, las posibilidades de vulneración de la intimidad de los cibernautas, las empresas y de la sociedad en general, se acrecientan. Por lo cual, creemos que un acercamiento al tema desde el punto de vista legal es necesario, buscando dar una visión general sobre esta problemática.

SEGUNDO. A nivel jurídico el estudio de los herramientas que se utilizan para conocer los actos ilícitos, es limitado puesto es un tema básicamente informático, esto es, de la especialidad de un Ingeniero de Sistemas, sin embargo, el derecho al regular las conductas humanas y los medios que emplea, esnecesario conocer en forma general las herramientas y mecanismos utilizados.

TERCERO. Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. En vista de lo anterior aquel porcentaje de personas que no

conocen nada de informática, pueden ser engañadas si en un momento dado poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la Internet, correo electrónico, etc.

CUARTO. La falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática.La vulnerabilidad de los sistemas de información de la administración publica, por la falta de una legislación eficaz, aumenta los riesgos que afectan la infraestructura tecnológica y la integridad, confiabilidad y disponibilidad de la información de las entidades gubernamentales.

QUINTO. El avance tecnológico, se puede decir ha sido la causante de que nuestro estilo de vida haya cambiado por completo en las dos últimas décadas, estamos frente a nuevas modalidades de lesión a los derechos fundamentales, como la intimidad, debido concretamente, a que antes no había un adelanto informático y electrónico de grandes magnitudes como ahora, lo cual nos lleva a dos conclusiones, la primera, que paralelamente al avance tecnológico, hay un avance más desarrollado en el delincuente, ya que este, tiene que tener un amplio conocimiento de dichos avances, los cuales, no los ocupan en realizar el bien sino a delinquir; y la segunda, que debido a la falta de una completa tipificación de los delitos cometidos con ayuda de la tecnología, estos delincuentes pueden seguir cometiendo este tipo de actos ilícitos, sin temor a recibir alguna sanción o privación de su libertad, es así que la población debe ser orientada en lasmedidas de seguridad para evitar ser víctimas de delitos informáticos.

SEXTO. Es conveniente y necesario establecer que no existe una herramienta de control que abarque todas las necesidades y sea infalible, aunque el único plan de seguridad eficaz es el que utiliza muchas capas de seguridad. Un ejemplo de ello es el empleo de un firewall, el cual es un

componente importante de un plan de este tipo, proporcionando protección al perímetro de la Red, pero no puede protegerla frente a muchos tipos de brechas de seguridad, como las internas, las físicas o las intrusiones causadas por la divulgación de contraseñas de los usuarios, siendo esta la principal medida de seguridad para evitar ser víctima de delitos informáticos.

RECOMENDACIONES:

PRIMERO. El legislador debe crear una legislación donde se incluyan las conductas desarrolladas en la nueva tipología del delito informático de mayor gravedad, al existir una pluralidad de bienes jurídicos afectados, donde se ven afectados diversos valores tan importantes como la intimidad,las bases de datos personales, el patrimonio, la economía, las infraestructuras críticas, el sistema informático nacional regentado actualmente por la Oficina Nacional de Gobierno Electrónico - ONGEI, en consecuencia hay pues, una pluralidad de bienes jurídicos afectados, todos ellos dignos de ser protegidos por el sistema legal.

SEGUNDO. No sólo basta con dotar de normas legales que sancionen las conductas que afecten a cualquier bien jurídico mediante el uso de alguna herramienta informática, es necesario establecer todo un sistema normativo que desarrolle y regule los mecanismos básicos que se emplean en los manejos a nivel electrónico.

TERCERO. Se propone que tanto las empresas como las personas físicas que cuenten con medios electrónicos por medio de los cuales utilicen el Internet (conjunto de elementos tecnológicos que permite enlazar masivamente redes de diferentes tipos para que los datos puedan ser transportados de una a otra red), sean motivadas a tomar conciencia de seguridad e instalen un firewall (escudo de protección básico y primera línea de defensa para prevenir accesos no autorizados), ya que este escudo, puede proporcionar protección a nivel perímetro de la red.

CUARTO. Establecer una LEY PARA PROTEGER LOS DATOS PERSONALES DE LOS CIBERNAUTAS EN INTERNET.

Legislación que contendrá los siguientes lineamientos:

ARTICULO 1. DATOS DE CARÁCTER PERSONAL Y FAMILIAR

Que es "cualquier información concerniente a personas físicas identificadas o identificables" Persona identificable, es "aquella a quien puede determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos de su identidad física, fisiológica, psíquica, cultural o social

En términos iusinformáticos, las expresiones "cualquier información" deben interpretarse como una unidad de datos (sea textual, gráfica, imágenes fijas o móviles, auditivas o vídeo-auditivas) representada en forma o por el sistema binaria (ceros y unos: 0-1) en el tratamiento electromagnético o computarizado (especialmente en su almacenamiento --storage--y teletrasmisión en unidas compatibles de discos fijos o "duros", de discos de de video digital o "DVD", o de discos compactos "Compac Disc" o medios informáticos de software o hardware, respectivamente) y relacionada con una persona natural o física. La información recolectada, seleccionada, organizada, procesada, almacenada y recuperada mediante consulta o transferencia, total o parcialmente por medios no simplemente "automatizados", sino por dispositivos o aparatos eléctricos, electrónicos o electromagnéticos (telecomunicaciones y ordenadores, básicamente).

ARTICULO 2.PRINCIPIOS DE PROTECCIÓN DE LOS DATOS

a) Manera y propósitos de la recolección de información, b) Solicitud de información por parte del individuo concernido o involucrado, c) Solicitud de información general o de dominio público, d) Almacenamiento y seguridad de la información, e) Información relativa a los datos registrados ante una

autoridad competente, f) Acceso a los datos que contienen información personal, g) Alteración de los datos registrados que contienen información de las personas, h) Verificación de la exactitud de los datos que contienen información personal antes de ser utilizados, i) Límites al uso de la información personal, j) Límites en el descubrimiento o divulgación de la información personal, y k) Límites al uso de cierta información, tal como los que revelen el origen racial o étnico, opiniones políticas, creencias religiosas, salud o vida sexual. J) En el caso de los límites al uso de información sobre la historia delictiva de las personas. En estos últimos casos, sólo se procederá por la autoridad competente, persona autorizada o responsable de un banco de datos, previo consentimiento expreso, escrito y libre otorgado por el concernido o cuando la ley lo autorice, o mediante el establecimiento de un código de protección de datos, respectivamente.

ARTICULO 3. FICHERO AUTOMATIZADO

Los ficheros o programas de computador serán controladas por una autoridad erigida al efecto y representada por una "persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán, se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

ARTICULO 4. MANIPULACION DEL FICHERO AUTOMATIZADO

El fichero como conjunto estructurado de datos, tiene una tratamiento informático previo, que se concreta en cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados, y

aplicadas a los datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por trasmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción. Dicho tratamiento puede ser realizado por una persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento

ARTICULO 5. PROTECCION DE DATOS BAJO CONTROL, MANEJO Y ADMINISTRACIÓN, INSTITUCIÓN PÚBLICA O PRIVADA.

Será responsable la INSTITUCIÓN PÚBLICA O PRIVADA de:

a) Que la variada información considerada de carácter personal, sea compilada, clasificada, organizada en forma legítima, por personas naturales o jurídicas o instituciones públicas y privadas para fines actuales o a posteriori lícitos de recuperación, transferencia (cesión o divulgación) por medios informáticos, electrónicos o telemáticos, por quien , a su vez , esté autorizado por mandato judicial, disposición legal o porque le concierne a él;

b) Para que permanente, continua y corrientemente, se actualice, modifique, aclare, cancele o borre la información, siempre que preste su consentimiento el titular de la información o el concernido, o lo imponga un mandato judicial o por disposición de la ley;

c) Para que el acceso a la información estructurada lógicamente en un banco de datos, sea fácil, rápido, eficaz, oportuno, libre obstáculos técnicos y engorrosos (característicos de la información compilada en forma manual o mecánica), por parte de los usuarios, siempre que se disponga de medios informáticos idóneos o telemáticos idóneos, autorización legal o por mandato judicial, y más aún, sin estar físicamente presente en el lugar o espacio

locativo donde se encuentre el banco de datos, si el acceso o recuperación de datos es requerido por un usuario que se halla en un espacio territorial diferente o que no coincide en nada con la división geopolítica del país donde se halla la

d) Que los sistemas de acceso como de recuperación de información por medios informáticos sea idóneo y permitan una vez dentro del contenido de la base de datos la búsqueda fácil y ordenada por palabras claves, descriptores, términos relacionados, prefijos o sufijos relacionales, etc. En fin, que permita al usuario acceder y recuperar los datos de forma clara,precisa y actualizada;

e) Que se incremente la seguridad jurídica y unidad de materia compilada legítimamente en un banco de datos y toda clase de medidas, instrumentos y mecanismos de protección y garantía de los derechos, libertades públicas e intereses legítimos, básicamente para el concernido, los usuarios y los responsables del control, manejo y administración de los bancos (personas naturales o jurídicas, institucionales o corporativas de carácter particular o público);

f) Que se estructure lógicamente toda información considerada personal, salvo la que por disposición del mismo ordenamiento jurídico vigente, se prohíba, limite o restrinja su compilación o se sometan al procedimiento de disociación para que el dato no se asocie a una persona determinada v.gr. Los denominados "datos sensibles" o correspondientes al "núcleo duro de la privacidad ", tales como el origen racial o étnico, ideología, religión, creencias, salud o vida sexual, inicialmente está prohibido su tratamiento por medios informáticos, electrónicos o telemáticos, podrían compilarse en bancos deinformación considerada legalmente personal (o "sensible" por la doctrina) y los Bancos de datos con información personal pero con acceso colectivo a la misma por primar en esta última clase de información el interés público sobre el privado. En efecto, sobre la información de tipo económico,

estadístico o científico, cuya esencia es la de ser impersonales, prevalecerá el derecho a la información "a través del reconocimiento del derecho al acceso colectivo a los bancos de datos, entendiendo que este derecho constituye hoy una de las manifestaciones más importantes del derecho a la información, en cuanto derecho activo o derecho-participación en los procesos decisorios de la ordenación política, económica o social de una comunidad".

ARTICULO 6. LEGIMITACION DE TRATAMIENTO DE DATOS.

El titular de los datos, permitirá el tratamiento informatizado de datos personales, siempre que: a) haya dado su consentimiento de forma inequívoca; b) sea necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado; c) sea necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento; d) sea necesario para proteger el interés vital del interesado; e) sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos; y, f) sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieren protección, en particular el derecho a la intimidad.

ARTICULO 7. DERECHOS DE RECTIFICACIÓN, ACTUALIZACIÓN Y CANCELACIÓN DE DATOS.

Constituyen derechos determinables e identificables por separado, pero que siendo derechos subsecuentes del derecho al acceso de la información o los datos contenidos en un fichero o banco de datos, constituyen una especie de

derechos en cascada e innegablemente complementarios y de efectos jurídicos recíprocos. En efecto, el derecho a la rectificación que tiene toda persona titular de los datos personales que le conciernen, consiste en la facultad o capacidad que aquél tiene para solicitar al responsable del fichero, a fin de que mantenga la exactitud de los datos, rectificando o cancelando los datos personales que resulten incompletos, inexactos, inadecuados o excesivos, según fuere el caso. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación y cancelación efectuada al cesionario.

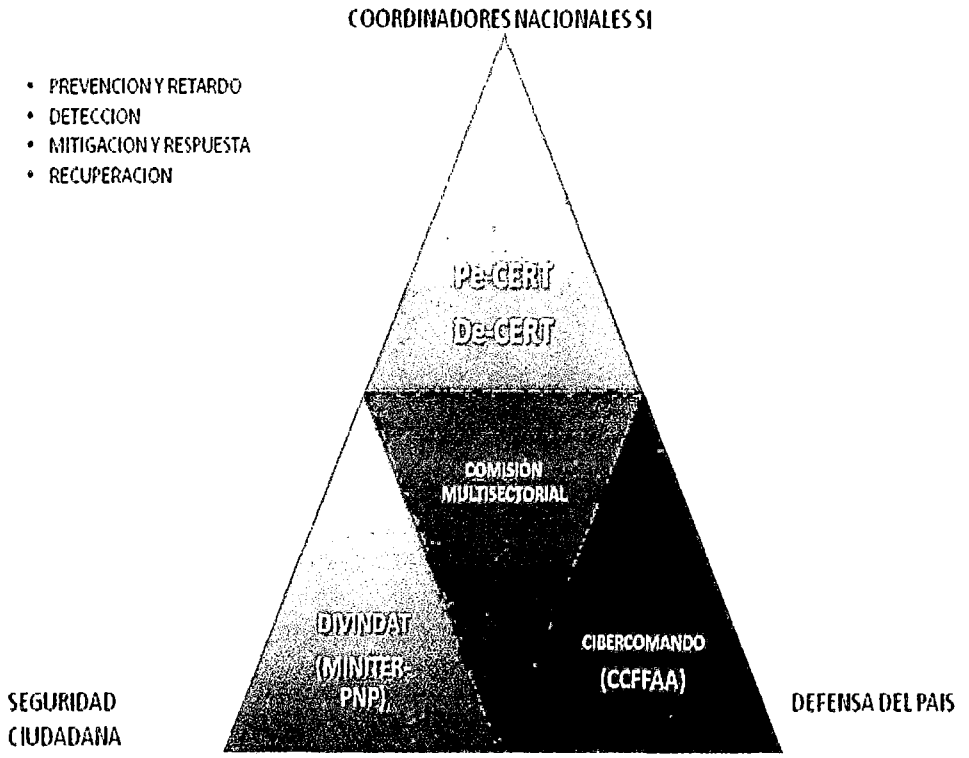
CONSENTIMIENTO EXPRESO QUE DEBE BRINDAR EL CIBERNAUTA

Se establece el consentimiento expreso que debe brindar el cibernauta en la red informática, motivo por el cual los sitios Web que registren usuarios deberán tener la posibilidad de que el usuario otorgue su consentimiento inequívoco en forma previa a realizar su registró, aceptando las condiciones de la misma. Los sitios que no realizan registro pero que captan datos deberán dejar claro cuales son las condiciones de uso del sitio a través de algún vínculo, para que el cibernauta esté informado de los datos que recabarán.

ARTICULO 8. RESPECTO A LA POLITICA Y ESTRATEGIA NACIONAL DE CIBERSEGURIDAD, se propone lo siguiente:

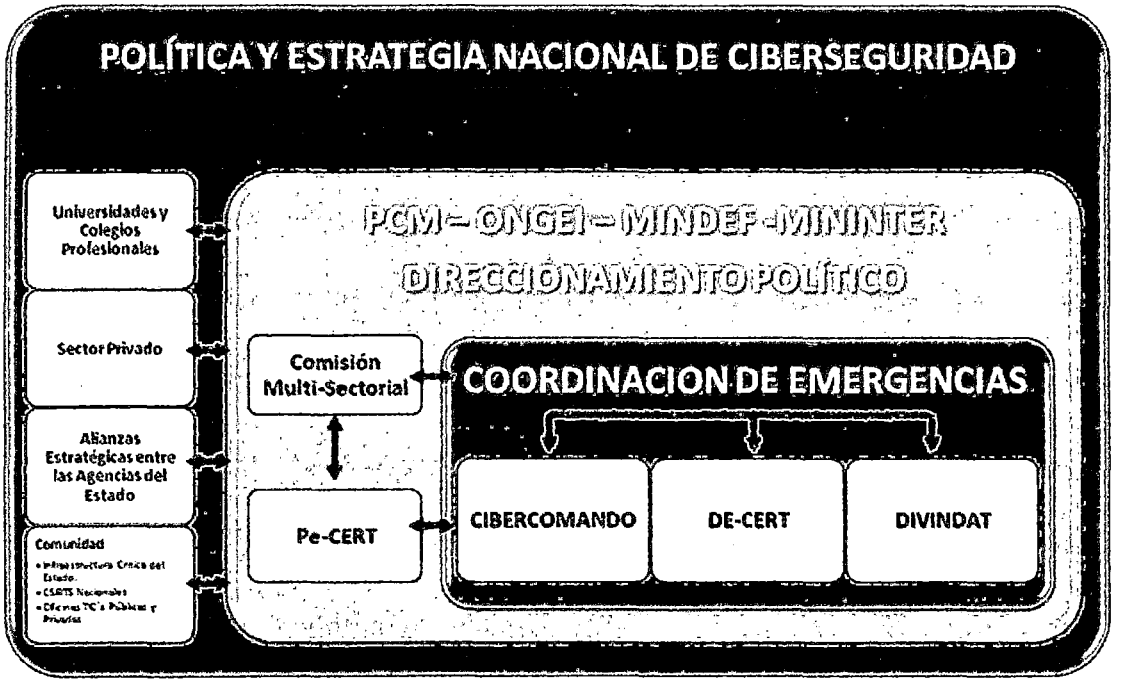
1. Fortalecer las capacidades del Estado para enfrentar el escenario del empleo de la Telemática en contra de sus intereses y a las amenazas que se presenten en el ciberespacio, que atentan contra su seguridad y defensa (ciberseguridad y ciberdefensa), garantizando la seguridad telemática, creando el ambiente y condiciones necesarias para brindarle protección.

(a) Establecimiento de un modelo que permita articular a las diferentes instancias y elementos encargados de dar respuesta por parte del Estado ante eventos no deseados en el ciberespacio.



Esquema de funcionamiento para los diferentes elementos que actúan en defensa del estado en el ciberespacio.

(b) Establecimiento de un esquema de articulación que permita integrar a todas las agencias del Estado, lideradas por la Coordinadora de Respuestas ante incidentes Teleinformáticas de la Administración Pública (Pe-CERT), que articule a los elementos operativos del Ministerio de Defensa y del Ministerio de Interior en el ciberespacio (De-CERT), Cibercomando, DIVINDAT; los que a través de una comisión multisectorial se integrarán con las Universidades, colegios profesionales, la Comunidad a proteger, tanto pública como privada.



Esquema de articulación de la Política Nacional de Ciberseguridad

2. Brindar educación, instrucción y capacitación especializada orientada a generar una conciencia de seguridad en el ciberespacio.

   a. Establecimiento de programas de educación para alcanzar competencias en ciberseguridad y ciberdefensa dirigidos a funcionarios públicos y privados encargados de tecnologías de Información.
   b. Incentivar la participación de las Universidades y Colegios Profesionales en la generación y transmisión de conocimiento en la materia.
   c. Incentivar en las Universidades programas de investigación y desarrollo tecnológico en TIC dentro del marco de la ciberseguridad y la ciberdefensa.
   d. Diseño e implementación de campañas de sensibilización y concientización en temas relacionados a la ciberdefensa y ciberseguridad, dirigidos funcionarios de alto nivel.

3. Fortalecer la Legislación Nacional en materia de delitos Informáticos, Ciberseguridad y Ciberdefensa.

   a. Establecimiento de iniciativas en el Congreso de la República en materia de Ciberseguridad y Ciberdefensa tendientes a la formulación y reforma de leyes que garanticen un marco legal adecuado.
   b. Proponer las modificaciones necesarias al Código Penal para prevenir el Ciberdelito, facilitando su interpretación y aplicación.
   c. Adhesión a los instrumentos internacionales vigentes en materia de protección de datos, ciberdefensa, ciberseguridad y seguridad de información.
   d. Desarrollo de programas de investigación y judicialización de delitos informáticos.

GLOSARIO DE TERMINOS

VIRUS

Es un pequeño programa capaz de reproducirse a sí mismo, infectando cualquier tipo de archivo ejecutable, sin conocimiento del usuario. El virus tiene la misión que le ha encomendado su programador, ésta puede ser desde un simple mensaje, hasta la destrucción total de los datos almacenados en el ordenador.

TROYANOS

Los troyanos son programas que aparentan ser útiles, por ejemplo parches, cuando en realidad son malignos. Pueden formatear el disco rígido, borrar archivos, o permitir a hackers entrar en nuestras máquinas. Pero a no desesperarse.

HACKER

(del inglés hack, recortar) es el neologismo utilizado para referirse a un experto en programación que puede conseguir de un sistema informático cosas que sus creadores no imaginan; así, es capaz de pensar y hacer cosas que parecen "magia" con los ordenadores. Se suele llamar hackeo y hackear a las obras propias de un hacker.

GUSANO O WORM

Son programas que tratan de reproducirse a si mismo, no produciendo efectos destructivos sino el fin de dicho programa es el de colapsar el sistema o ancho de banda, replicándose a si mismo.

JOKE PROGRAM

Simplemente tienen un payload (imagen o sucesión de estas) y suelen destruir datos.

BOMBAS LÓGICAS O DE TIEMPO

Programas que se activan al producirse un acontecimiento determinado. la condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o un estilo técnico Bombas Lógicas), etc... Si no se produce la condición permanece oculto al usuario.

RETRO VIRUS

Este programa busca cualquier antivirus, localiza un bug (fallo) dentro del antivirus y normalmente lo destruye.

EL MÓDULO DE REPRODUCCIÓN

se encarga de manejar las rutinas de "parasitación" de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse subrepticiamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.

EL MÓDULO DE ATAQUE

es optativo. En caso de estar presente es el encargado de manejar las rutinas de daño adicional del virus. Por ejemplo, el conocido virus Michelangelo, además de producir los daños que se detallarán más adelante, tiene un módulo de ataque que se activa cuando el reloj de la computadora indica 6 de Marzo. En estas condiciones la rutina actúa sobre la información del disco rígido volviéndola inutilizable.

EL MÓDULO DE DEFENSA

Tiene, obviamente, la misión de proteger al virus y, como el de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la remoción del virus y retardar, en todo lo posible, su detección.

INFECTORES DE ARCHIVOS EJECUTABLES

Afectan archivos de extensión EXE, COM, BAT, SYS, PIF, DLL, DRV

INFECTORES DIRECTOS

El programa infectado tiene que estar ejecutándose para que el virus pueda funcionar (seguir infectando y ejecutar sus acciones destructivas)

INFECTORES RESIDENTES EN MEMORIA

El programa infectado no necesita estar ejecutándose, el virus se aloja en la memoria y permanece residente infectando cada nuevo programa ejecutado y ejecutando su rutina de destrucción

INFECTORES DEL SECTOR DE ARRANQUE

Tanto los discos rígidos como los disquetes contienen un Sector de Arranque, el cual contiene información específica relativa al formato del disco y los datos almacenados en él. Además, contiene un pequeño programa llamado BootProgram que se ejecuta al bootear desde ese disco y que se encarga de buscar y ejecutar en el disco los archivos del sistema operativo. Este programa es el que muestra el famoso mensaje de "Non-system Disk or Disk Error" en caso de no encontrar los archivos del sistema operativo. Este es el programa afectado por los virus de sector de arranque.

MACROVIRUS

Son los virus más populares de la actualidad. No se transmiten a través de archivos ejecutables, sino a través de los documentos de las aplicaciones que poseen algún tipo de lenguaje de macros. Entre ellas encontramos todas las pertenecientes al paquete Office (Word, Excel, Power Point, Access) y también el Corel Draw.Cuando uno de estos archivos infectado es abierto o cerrado, el virus toma el control y se copia a la plantilla base de nuevos documentos, de forma que sean infectados todos los archivos que se abran o creen en el futuro...

DE HTML

Un mecanismo de infección más eficiente que el de los Java applets y Actives controls apareció a fines de 1998 con los virus que incluyen su código en archivos HTML. Con solo conectarse a Internet, cualquier archivo HTML de una página web puede contener y ejecutar un virus. Este tipo de virus se desarrollan en Visual Basic Script. Atacan a usuarios de Win98, 2000 y de las últimas versiones de Explorer. Esto se debe a que necesitan que el Windows Scripting Host se encuentre activo. Potencialmente pueden borrar o corromper archivos.

BIBLIOGRAFIA

REFERIDO AL DERECHO A LA INTIMIDAD

1. **ALCANTARA** José F. *La sociedad de control: Privacidad, propiedad intelectual y el futuro de la libertad.* Barcelona. 2008.
2. **ABA CATORIA** Ana La video vigilancia y la garantía de los derechos individuales: su marco jurídico. Madrid. 2009.
3. **ABAD,** Samuel: "El hábeas data y conflicto entre órganos constitucionales: dos nuevos procesos constitucionales". En: La Constitución de 1993. Análisis y comentarios, Lima, Comisión Andina de Juristas, 1994, serie Lecturas Temas Constitucionales Nº 10.
4. **ASENCIO MELLADO**, J.M. *Introducción al Derecho Procesal.* Editorial Tirant lo Blach. Valencia. 2004.
5. **BÉJAR,** Helena, El ámbito íntimo. Privacidad, individualismo y modernidad, Alianza Editorial. Madrid, 1990.
6. **BRAGE CAMAZANO** Joaquín*Aproximación a una Teoría General de los Derechos Fundamentales En El Convenio Europeo De Derechos Humanos*/. -Madrid: Centro de Estudios Políticos y Constitucionales - CEPC, 2005.
7. **BRAMONT ARIAS**, Luís, *Manual de Derecho Penal* Lima, San Marcos 2002.

8. **BULLARD GONZÁLES,** No se lo digas a nadie ¿Se puede vender el derecho la privacidad en el mercado?, en Ius et veritas, Año IX, N°17, Lima, 1998. P.183
9. **BULLARD GONZÁLES**, Estudios de análisis económico del derecho, Ara, Lima, 1996.
10. **BUSTOS RAMÍREZ**Juan *Manual de Derecho Penal* Barcelona Editorial Ariel. 1989. P.678
11. **CABANELLAS** Guillermo *Diccionario de Términos Jurídicos* Buenos Aires Editorial Alternativas. 1978.
12. **CÁCERES BARROS** A. Información y Análisis Jurídicos, Derecho a la Intimidad, N°. 126, México, 2000.
13. **CARO CORIA**Dino Carlos Notas sobre la individualización judicial de la pena en el código penal peruano penales. penal. Vol. I. 2ª ed. Lima, Grijley 2003.
14. **CASTILLO ALVA,** José Luís. En: Código Penal comentado. T. I. Lima, Gaceta Jurídica 2004.P. 467
15. **CUAUHTÉMOC** M. De DienheimBarrigueteEl *Derecho a la Intimidad, al Honor y a la Propia Imagen*. México UNAM. 2006. P.353
16. **CHUNGA LAMONGA**, Fermín. Derecho de Menores: Doctrina, comentarios al Código del Niño y Adolescente. Lima, Grijley, 3ra. Edición, 2000.P.487
17. **DE VEGA** Pedro, *Neoliberalismo y Estado*, en *Pensamiento Constitucional*, Año IV, N° 4, Pontificia Universidad Católica del Perú – Maestría en Derecho Constitucional, Fondo Editorial, Lima, 1997.P.134
18. **EGUIGUREN,** Francisco. *Estudios constitucionales*, Lima, Ara Editores, 2002. P.235
19. **EGUIGUREN**, Francisco. *La jurisdicción constitucional y los procesos para la protección de los derechos fundamentales*. En: Manual del sistema peruano de justicia. Villavicencio, Alfredo (coordinador), Lima, Consorcio Justicia Viva. 1990. P.124.

20. **EGUIGUREN PRAELI,** Francisco. La Libertad de expresión e información y el derecho a la intimidad personal. 1°. Ed, Lima, Palestra 2004. P.256
21. **ESPINOZA ESPINOZA,** *Juan.* Derecho de las personas. *Editorial Rodhas,* Lima 1999. P.341
22. **EZAINE CHÁVEZ,** Amado: Diccionario de Derecho Penal, Ediciones Jurídicas Lambayecanas, 1992, P.476.
23. **FARIÑAS MANTONI,**Luís Mario. Derecho a la intimidad. 1°. Ed, Madrid. Ed. Trivium, 1983. P.389.
24. **GARCÍA SAYAN** Diego *Normas internacionales sobre derechos humanos y derecho interno.* Lima Comisión Andina de Juristas. 1984. P.323
25. **HURTADO POZO**, José. «Responsabilidad y culpabilidad». En: ADP 1993. P.223
26. **LEO REISINGER**, Alvarez-Cienfuegos Suarez, José María, *"El derecho a la intimidad personal, la libre difusión de la información y el control del Estado sobre los bancos de datos"*, en *Encuentros sobre Informática y Derecho*, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1990.
27. **MARTÍNEZ MARTÍNEZ**, Ricardo, *Tecnologías de la información, policía y Constitución*, Tirant lo blanch, Valencia, 2001. P.245
28. **MORALES GODO** Juan *Comentarios al Código Civil* Gaceta Jurídica, Lima, 2005. P. 687
29. **MORALES GODO**, *El derecho a la vida privada y el conflicto con la libertad de información*, Grijley, Lima, 1999. P.321
30. **MURILLO DE LA CUEVA**, Pablo. "El Derecho a la Autodeterminación Informativa. La Protección de los Datos Personales frente a la Informática." Editoriales Tecnos. Madrid, 1990. P.452
31. **NOGUERA ALCALÁ**, Humberto, *"El derecho a la libertad de opinión e información y sus límites"*. Lexis-Nexis, Chile, 2002. P.235

32. **O°DONELL** Daniel *Protección Internacional de los Derecho Humanos* Lima Comisión Andina de Juristas. 1996. P. 454
33. **TRINIDAD MARTÍNEZ** Verónica, *Recuento de daños a las libertades de expresión e información en 1999*, en Revista Mexicana de Comunicación, número 64, Julio - Agosto de 2000, México DF. P.234
34. **PÉREZ LUÑO,** Antonio. Derechos Humanos. Estado de Derecho y Constitución. 4ta. ed.: Tecnos, Madrid, 1991.P. 438.
35. **PÉREZ-LUÑO,** Antonio Enrique. *Manual de Informática y Derecho*, Editorial Ariel S.A., Barcelona, 1996 P. 549.
36. **RODOTA,** Si nuestra "privacy" se convierte en una mercancía, en Revista de responsabilidad Civil, La Ley, Año I, N° 6, Noviembre – Diciembre de 1999, Buenos Aires. P.123
37. **ROMEO CASABONA**, Carlos María, *"Poder informático y seguridad jurídica".* FUNDESCO. Madrid, 1988 P.237.
38. **SAN MARTÍN CASTRO** Cesar *Derecho Procesal Penal* Editorial Grijley. Lima 1999. P.698.
39. **SÁNCHEZ VELARDE** Pablo *El Nuevo Proceso Penal* Lima Editorial Idemsa. 2009. P.556
40. **SORIANO DÍAZ**. Ramón Luís Las libertades públicas: significado, fundamentos y estatuto jurídico. Madrid. Tecnos, 1990. P.456
41. **VIDAL RAMÍREZ,**Fernando, *El Acto Jurídico*, Ed. "El Búho E.I.R.L, 6ta edición, Lima. 2005. P.387.
42. **VILLASEÑOR GOYZUETA** Claudia Contenido esencial de los derechos fundamentales y jurisprudencia del Tribunal Constitucional Español. Madrid: Universidad Complutense, 2003. P.359
43. **VILLA STEIN** Javier *Derecho Penal Parte General.* Lima Editorial San Marcos. 1998. P.698.
44. **VELÁSQUEZ VELÁSQUEZ**, Fernando. Los criterios de determinación de la pena en el CP peruano de 1991. Ponencia presentada el 21 de agosto de 2000 en la PUCP.

Sentencias:

45. Tribunal Constitucional: Exp. N° 2053-2003-HC/TC, sentencia del 15 de septiembre del 2003
46. Sentencia dictada en contra del Estado de Chile en el caso Claude Reyes, de 19 de septiembre de 2006.
47. caso de FERNANDO SAMUEL ENRIQUE VÁSQUEZ WON; de Lambayeque con número de expediente 4168-2006-PA/TC.
48. Informe N.° 216-2007/SUNAT-2L0200, de fecha 14 de junio de 2007,
49. SENTENCIA DEL TRIBUNAL CONSTITUCIONAL DE HABEAS DATA EXP. N° 666-96-HD-TC

Páginas web:

50. **GARCÍA-VILLEGAS** Sánchez-Cordero Paula María La libertad de expresión y algunos de sus límites, articulo en http://www.scjn.gob.mx/NR/rdonlyres/D18C6F32-BF5E-4D34-B398-DB1EC4F72DA3/0/PAULAMAGARCIAVILLEGAS SANCHEZCORDERO.pdf, P.9, CONSULTADO EL X/XI/2011

REFERIDO A LOS DATOS EN INTERNET.

1. **RONDINEL SOSA**, Rocío. Informática Jurídica. De la Teoría a la Práctica. Lima: PREAI. 1995. P.42.
2. **GALLOUEDEC-GENUYS**, Francoise & LEMOINE, Philippe. La informatización: riesgos culturales. Barcelona: Mitre. P.47.
3. **CARRASCOSA LOPEZ.** Derecho a la Intimidad e Informática. EN: Informática y Derecho. Mérida: Universidad Nacional de Educación a distancia. 1992.
4. **GALLOUEDEC-GENUYS**, Francoise & LEMOINE, Philippe. Op. Cit.. p. 41-42. Ver también: PRIETO ACOSTA, Margarita Gabriela.

Informática Jurídica: el derecho ante un gran reto. Bogotá: Pontificia Universidad Javeriana. 1984. P.104.

5. **CARRASCOSA LOPEZ**. Derecho a la Intimidad e Informática. EN: Informática y Derecho. Mérida: Universidad Nacional de Educación a distancia. 1992. P.13
6. **PEREZ** LUÑO, Antonio Enrique. Manual de Informática y Derecho. Barcelona: Ariel. 1996. P.49.

7. **CRIPTONOMICON**. ¿Qué hay de verdad en eso de las cookies?. http://www.estrelladigital.es/ciberestrella/secciones/saber/saber16.htm
8. **CASACUBERTA**, David. La privacidad en los nuevos medios electrónicos. Aspectos técnicos y sociales. Redi Nº 11. Revista electrónica de derecho informático.
9. **MURILLO DE LA CUEVA**, Pablo Lucas. El derecho a la autodeterminación informativa. La protección de los datos personales frente al uso de la informática. Madrid: Tecnos. 1990.
10. **DE URIOSTE,** Mercedes. Protección de Datos Personales. REDI Nº 23. Junio del 2000
11. **HANCE**, Olivier. Leyes y Negocios en Internet. México: Mc Graw Hill. 2008
12. **CASACUBERTA,** David. La privacidad en los nuevos medios electrónicos. Aspectos técnicos y sociales. EN: REDI-Revista Electrónica de Derecho Informático. Nº 11. http://www.alfa-redi.org/rdi.shtml
13. **GARDNER**, ELIZABETH. El anonimato en la Red. EN: Internet World en español. 1999. Año 5 Nº 11.

14. **RAMOS SUAREZ.** ¿Es legal el uso de cookies? EN: REDI Nº 8. Agosto 1998.
15. **TICS CONSULTING** -www.ticsconsulting.es. Recuperado el 12 de Febrero del 2012.

REFERIDO A LA METODOLOGIA.

1. **GONZALES GALVÁN,** Jorge A. La Construcción del Derecho. Métodos y Técnicas de Investigación. Instituto de Investigaciones. Universidad Nacional Autónoma de México. México, 2006.
2. **TAMAYO,** Mario. El proyecto de investigación. Serie Aprender a Investigar. ICES, Ed. Feriva. S.A. Bogotá, 1995.
3. **TOKESHI SHIROTA,** Alberto. Planifique, desarrolle y apruebe su tesis. Guía para mejores resultados. Universidad de Lima. Fondo Editorial. 1 edición. Lima, 2008.
4. **AP CONTANDRIOPOULOS.** *Et al.* "Preparar un proyecto de investigación". Barcelona, 1991.
5. **RAMOS NUÑEZ,** Carlos. Cómo hacer una tesis de Derecho y no envejecer en el intento. Gaceta Jurídica. Primera edición, Lima, 2000.
6. **TAFUR PORTILLA,** Raúl. La Tesis universitaria. La tesis doctoral – La tesis de Maestría El Informe. Editorial Mantaro. Lima, 1994.
7. **ARELLANO GARCÍA,** Carlos. «Métodos y Técnicas de la Investigación Jurídica. Elaboración de Tesis de Licenciatura, Maestría y Doctorado, Tesinas y otros trabajos de Investigación Jurídica». Tercera edición, Editorial Porrúa, México, 2004.

ANEXOS

CUESTIONARIO N° 01

TESIS: "LA DESPROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS, EXPUESTOS A CÓDIGO MALICIOSO Y SU INCIDENCIA EN LA VULNERACIÓN AL DERECHO A LA INTIMIDAD"

Agradeceré a usted responder este breve y sencillo cuestionario, su aporte es muy importante para el logro del siguiente objetivo.	**OBJETIVO:**DETERMINAR EN QUE MEDIDA LA DESPROTECCION DE LOS DATOS PERSONALES DE LOS CIBERNAUTAS PERUANOS, EXPUESTO A CÒDIGO MALICIOSO, INCIDE EN LA VULNERACIÓN AL DERECHO A LA INTIMIDAD.

GENERALIDADES: Esta información será utilizada en forma confidencial, anónima y acumulativa; por lo que agradeceremos a las personas entrevistadas proporcionarnos informaciones veraces, solo así serán realmente útiles para la investigación.	**INFORMANTES:** La presente Encuesta esta dirigida a cibernautas peruanos, ingenieros informáticos, abogados, operadores informáticos de las instituciones de gobierno.

1.- ¿Esta de acuerdo usted en la información que en nuestra país, hay una desprotección de los datos personales de los cibernautas peruanos, expuesto a código malicioso, incide en la vulneración al derecho a la intimidad?

1. Totalmente de acuerdo.
2. De acuerdo.
3. Indeciso.
4. En desacuerdo.
5. Totalmente en desacuerdo.

2.- ¿Considera usted que a vulnerabilidad de los sistemas de información de la administración publica, aumenta los riesgos que afectan la infraestructura

tecnológica y la integridad, confiabilidad y disponibilidad de la información de las entidades gubernamentales?

1. Totalmente de acuerdo.
2. De acuerdo.
3. Indeciso.
4. En desacuerdo.
5. Totalmente en desacuerdo.

3.- ¿Cree usted que los entes encargados de sancionar a quienes hacen uso ilegal y delictivo de las herramientas informáticas, no tengan cómo judicializar a las nuevos modalidades en contra de los cibernautas?

1. Totalmente de acuerdo.
2. De acuerdo.
3. Indeciso.
4. En desacuerdo.
5. Totalmente en desacuerdo.

4.- ¿Considera usted que el estado no tiene una eficaz procedimiento y políticas de seguridad de la información, que hace vulnerable los datos almacenados?

1. Totalmente de acuerdo.
2. De acuerdo.
3. Indeciso.
4. En desacuerdo.
5. Totalmente en desacuerdo.

5.- ¿Esta de acuerdo usted que el estado debe imponer sanciones penales a las personas que incurran en las conductas que vulneren el derecho a la intimidad?

1. Totalmente de acuerdo.
2. De acuerdo.
3. Indeciso.
4. En desacuerdo.
5. Totalmente en desacuerdo.

6.- ¿Esta de acuerdo usted que hay una necesidad de contar con un derecho que regule la libertad de información como factor indispensable para el desarrollo del individuo y la sociedad y que manifieste sus límites para defender los márgenes de la intimidad necesarios para el normal desarrollo de la personalidad humana?

1. Totalmente de acuerdo.
2. De acuerdo.
3. Indeciso.
4. En desacuerdo.
5. Totalmente en desacuerdo.

7.- ¿Considera usted que se deben ofrecer soluciones mediante la criptografía, programas que permitan nuestro anonimato o nuevos protocolos de comunicación que nos permitan dirigir a quiénes entregamos información y dosificarla verdaderamente?

1. Totalmente de acuerdo.
2. De acuerdo.
3. Indeciso.
4. En desacuerdo.
5. Totalmente en desacuerdo.

8.- ¿Considera usted que Respecto al consentimiento que debe brindar el cibernauta en la red informática, se debe establecer que el consentimiento expreso y escrito motivo por el cual los sitios Web que registren usuarios deberán tener la posibilidad de que el usuario otorgue su consentimiento inequívoco en forma previa a realizar su registró, aceptando las condiciones de la misma?

1. Totalmente de acuerdo.
2. De acuerdo.
3. Indeciso.
4. En desacuerdo.
5. Totalmente en desacuerdo.

9- ¿Esta de acuerdo usted que los sitios que no realizan registro pero que captan datos deberán dejar claro cuales son las condiciones de uso del sitio a través de algún vínculo, para que el cibernauta esté informado de los datos que recabarán?

1. Totalmente de acuerdo.
2. De acuerdo.
3. Indeciso.
4. En desacuerdo.
5. Totalmente en desacuerdo.