



**TECNOLÓGICO UNIVERSITARIO DE MÉXICO
INCORPORACIÓN UNAM 3079-09**

**“LA INTIMIDAD Y SU TRANSGRESIÓN MEDIANTE EL
USO INDEBIDO DE EQUIPOS INFORMÁTICOS”**

GABRIELA MORALES ROMERO

LICENCIADA EN DERECHO

NUMERO DE CUENTA: 40551341-5

ASESOR: LIC. MARINO VILLAR VALVERDE

MÉXICO,D.F.

2010



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

A DIOS

POR CONCEDERME LA VIDA Y CON ELLA, UNA MADRE Y UN PADRE INMENSAMENTE MARAVILLOSOS;

POR ILUMINAR MI CAMINO CUANDO MÁS CLARIDAD NECESITABA;

POR DOTARME DE PACIENCIA Y VALOR;

POR BRINDAR PAZ EN MÍ MENTE;

POR MOSTRARME EL VERDADERO SIGNIFICADO DE AMARME A MI MISMA;

POR PERMITIRME CONOCER A LAS PERSONAS ADECUADAS;

POR COLOCARME OBSTÁCULOS CADA DÍA;

POR DEDICARME TODO TU TIEMPO;

POR ESTAR SIEMPRE A MI LADO, AÚN Y CUANDO NO LO HE MERECIDO;

POR INUNDARME DE ESPERANZA Y FUERZA;

POR SER MI ALIADO EN LA VIDA;

POR DARMER LA OPORTUNIDAD DE LLEGAR HASTA AQUÍ;

POR OTORGARME MÁS DE LO QUE PUDIERA DESEAR.

A TI SEÑOR DIOS, GRACIAS.

A MI MADRE

EL SER QUE ME HA BRINDADO TODO SIN ESPERAR NADA A CAMBIO;

QUIEN SE HA CONVERTIDO EN UN EJEMPLO DE LUCHA Y ENTREGA;

LA COMPAÑERA QUE SIGUE MIS PASOS Y QUE JAMÁS ME DEJA CAER;

LA AMIGA ENTRAÑABLE QUE SIEMPRE CONFÍA EN MÍ;

LA PERSONA QUE SIEMPRE ME ALIENTA EN CADA MOMENTO;

LA DAMA MÁS HERMOSA, CARIÑOSA, GENTIL Y ESPECIAL QUE HA
INVADIDO MI VIDA DE ALEGRÍA;

LA MUJER QUE ME HA INCULCADO VALORES Y ME HA ENSEÑADO LO
FUERTE QUE PUEDO SER;

LA PARTÍCIPE DE UN LOGRO MÁS.

A TÍ MAMÁ ¡GRACIAS POR CREER EN MÍ!

A MI PADRE

EL HOMBRE FUERTE Y ENÉRGICO QUE SIEMPRE MANTUVO SU INTERÉS EN MI FUTURO, QUE A BASE DE ESFUERZOS ME HA BRINDADO LOS MEDIOS PARA SEGUIR ADELANTE, QUIEN TODOS LOS DÍAS SE PREOCUPA POR MÍ Y NO ME PERMITE DECAER.

LA PERSONA QUE ME HA DADO TODO, AÚN SIN MERECKERLO, EL AMIGO QUE SIEMPRE HA QUERIDO LO MEJOR PARA MÍ.

A TÍ PAPÁ, QUE NO TE HE SABIDO VALORAR, GRACIAS POR TU PACIENCIA, CONSEJOS Y SOBRE TODO POR ESTAR SIEMPRE A MI LADO, CON TODO MI CARIÑO Y RESPETO, TE DEDICO ESTA TESIS PROFESIONAL.

¡MIL GRACIAS POR TODO PAPÁ!

A MI DISTINGUIDA Y SUPREMA CASA DE ESTUDIOS

TECNOLÓGICO UNIVERSITARIO DE MÉXICO

**QUIENES ADMITIERON MÍ ESTANCIA Y ME BRINDARON LAS
BASES PARA CONFORMARME COMO UNA PROFESIONISTA.**

TODA MI ENTEREZA SE LA DEBO A ELLA

**A MÍ HERMANO Y MÍ CUÑADA:
FELIPE MORALES ROMERO Y MARÍA ISABEL HERNÁNDEZ
CAPETILLO.**

**POR ESTAR SIEMPRE CONMIGO, BRINDÁNDOME SU CARIÑO, APOYO,
TIEMPO Y DEDICACIÓN,
GRACIAS POR SER MÍ FAMILIA.**

**A MÍS SOBRINOS:
JUAN CARLOS MORALES HERNÁNDEZ Y JORGE LUÍS MELO
HERNÁNDEZ.**

**POR SU AMISTAD, AFECTO Y ÁNIMO.
GRACIAS POR CONFIAR EN MÍ.**

**A MÍ ASESOR DE TESIS:
LIC. MARINO VILLAR VALVERDE**

**AGRADEZCO LA PACIENCIA, TIEMPO Y DEDICACIÓN QUE TUVO PARA
LA CULMINACIÓN DE ESTE TRABAJO.**

A MÍS SINODALES

CON TODO RESPETO Y ADMIRACIÓN, GRACIAS.

AL LIC. ABRAHAM GARCÍA LICONA:

**QUE CON GRAN ENTEREZA, ENSEÑANZA Y MOTIVACIÓN ME IMPULSO
EN LA REALIZACIÓN DE ESTA TESIS PROFESIONAL.**

AL LIC. ORLANDO PÉREZ GONZÁLEZ:

**POR HABER SIDO QUIEN ME IMPULSO EN LA REALIZACIÓN DEL
PRESENTE TRABAJO, GRACIAS POR SU INTERÉS Y APOYO.**

A LA LIC. NORMA ESPEJO VALLE

POR SU INSTRUCCIÓN, AMISTAD Y CONSEJOS.

A MÍS FUTUROS HIJOS:

**QUE AÚN DIOS NO LOS SITÚA EN MÍ VIDA, PERO DESDE ESTE
MOMENTO HAN SIDO UNA INSPIRACIÓN, CON TODO MI CARIÑO A
ELLOS, ESPERO QUE ESTE ESFUERZO SEA UNA MOCIÓN PARA QUE
EN UN FUTURO LOGREN TODAS SUS METAS.**

EN GENERAL, A TODA MI FAMILIA:

**A QUIENES DIRECTA O INDIRECTAMENTE ME ALENTARON A LLEGAR A
ESTE ÉXITO Y ME BRINDARON SU INCONMENSURABLE AFECTO.**

¡GRACIAS!

“LA INTIMIDAD Y SU TRANSGRESIÓN MEDIANTE EL USO INDEBIDO DE EQUIPOS INFORMÁTICOS”

ÍNDICE

INTRODUCCIÓN	1
---------------------	----------

CAPÍTULO PRIMERO

GENERALIDADES DE LA INTIMIDAD, INFORMACIÓN Y DATOS PERSONALES

1.1 DIVERSAS ACEPCIONES DEL CONCEPTO DE INTIMIDAD.	6
1.2 CONCEPTOS AFINES CON LA INTIMIDAD.	7
A) SECRETO.	7
B) CONFIDENCIALIDAD.	7
C) PRIVACIDAD.	8
1.3 DIFERENCIAS ENTRE INTIMIDAD Y PRIVACIDAD.	9
1.4 QUE DEBEMOS ENTENDER POR DERECHO.	10
1.5 BREVES ANTECEDENTES DEL DERECHO A LA INTIMIDAD.	11
1.5.1 DERECHO A LA INTIMIDAD.	13
1.6 CONCEPTO DE INFORMACIÓN PÚBLICA E INFORMACIÓN PRIVADA.	16
1.6.1 DERECHO A LA INFORMACIÓN Y SU CONTROL.	18
1.7 DATOS PERSONALES.	20
A) DATOS PERSONALES ÍNTIMOS.	20
B) DATOS PERSONALES PÚBLICOS.	21

CAPÍTULO SEGUNDO

NOCIONES GENERALES DE LA INFORMÁTICA, Y SUS VARIANTES EN RELACIÓN CON LA INTIMIDAD

2.1 BREVE ANÁLISIS DE EQUIPOS INFORMÁTICOS.	22
2.1.1 CONCEPTO DE INFORMÁTICA.	25
2.2 CARACTERÍSTICAS FUNDAMENTALES DEL DERECHO. INFORMÁTICO	26
2.3 LA INTERNET Y SU IMPORTANCIA EN LAS DIFERENTES ÁREAS DE NUESTRA VIDA.	27
2.3.1 LA INTERNET COMO UNA VÍA PARA EL MAL USO DE LA INFORMACIÓN PERSONAL.	30
2.4 SERVICIOS INFORMÁTICOS MÁS USADOS QUE CONLLEVAN UN INTERCAMBIO DE DATOS PERSONALES E ÍNTIMOS.	31
A) CORREO ELECTRÓNICO.	31
B) MESSENGER .	34
C) HI5	35
D) FACEBOK.	37
F) MySpace.	39
2.5 INTIMIDAD INFORMÁTICA.	39
2.6 INFORMÁTICA JURÍDICA.	41
2.7 RIESGOS INFORMÁTICOS.	43

CAPÍTULO TRES

GENERALIDADES DEL DERECHO PENAL APLICADOS AL ESTUDIO DE LA PROTECCIÓN A LA INTIMIDAD

3.1 EL DERECHO EN GENERAL	44
3.1.1 DERECHO PENAL	44
3.2 ELEMENTOS DEL DELITO	46
3.2.1 CONDUCTA Y ACCIÓN	48
3.2.1.1 AUSENCIA DE CONDUCTA	49
3.2.2 TIPICIDAD	49
3.2.2.1 ATIPICIDAD	50
3.2.3 ANTIJURIDICIDAD	51
3.2.3.1 CAUSAS DE JUSTIFICACIÓN	51
3.2.4 CULPABILIDAD	51
3.2.4.1 INCULPABILIDAD	52
3.2.5 IMPUTABILIDAD	52
3.2.5.1 INIMPUTABILIDAD	52
3.2.6 PUNIBILIDAD	53
3.3 BREVE ESTUDIO DOGMÁTICO DEL DELITO DE VIOLACIONES A LA INTIMIDAD	53
3.4 LA TENTATIVA	56
3.5 LA CONSUMACIÓN	58

CAPÍTULO CUARTO

LOS DELINCUENTES INFORMÁTICOS Y SU TRASCENDENCIA EN EL ÁMBITO INTERNACIONAL

4.1 CONCEPTO DE DELITO Y DELINCUENTE	59
4.2 LOS DELINCUENTES INFORMÁTICOS	59
A) EL HACKER	59
B) EL CRACKER	60
C) OTROS	61
4.3 LA IMPORTANCIA DE UNA REGULACIÓN JURÍDICA RESPECTO AL FLUJO INTERNACIONAL DE INFORMACIÓN Y DATOS PERSONALES POR INTERNET.	63
4.4 EL HABEAS DATA	65
4.5 CONVENIOS INTERNACIONALES	68

CAPÍTULO QUINTO

EL PROCEDIMIENTO PENAL MEXICANO Y LAS FIGURAS JURÍDICAS VINCULADAS EN LA COMISIÓN DE VIOLACIONES A LA INTIMIDAD MEDIANTE EL USO INDEBIDO DE EQUIPOS INFORMÁTICOS

5.1 GENERALIDADES DEL PROCEDIMIENTO PENAL.	70
5.2 BIEN JURÍDICO TUTELADO.	72
5.3 INSTRUMENTO MATERIAL DE LAS VIOLACIONES A LA INTIMIDAD.	73
5.4 NORMATIVIDAD Y PENALIDAD EXISTENTES RESPECTO A VIOLACIONES EN LA INTIMIDAD MEDIANTE EL USO INDEBIDO DE EQUIPOS INFORMÁTICOS.	73
5.5 EL DAÑO MORAL.	83
5.6 POLICÍA CIBERNÉTICA.	88

5.7 FUNCIÓN PERSECUTORIA DE LOS DELITOS INFORMÁTICOS.	90
5.8 LOS MENORES DE EDAD COMO PRINCIPALES TRANSGRESORES DE LA INTIMIDAD MEDIANTE EL USO INDEBIDO DE SISTEMAS Y EQUIPOS INFORMÁTICOS.	92
5.8.1 MEDIDAS DE CORRECCIÓN PARA LOS MENORES INFRACTORES	95
5.9 LA INTIMIDAD ANTE LOS AVANCES INFORMÁTICOS Y SU SITUACIÓN ACTUAL.	99
CONCLUSIONES	103
PROPUESTA	109
BIBLIOGRAFÍA	113

INTRODUCCIÓN

De la misma forma en que el hombre nace libre físicamente, tiene la libertad de dar a conocer de sí mismo, a la sociedad lo que su voluntad le sugiera, pero con los avances de la tecnología y la creciente demanda de información en nuestros días, esto parece ser imposible.

La revolución tecnológica ha redimensionado las relaciones del hombre con los demás hombres con su contexto o marco de convivencia.

En este trabajo se descubre la estrecha conexión entre la intimidad y la informática, toda vez que en la actualidad nuestra vida se ve envuelta en los avances tecnológicos y con ello el uso de las computadoras y la Internet, ya que en la mayoría de las actividades a realizar durante el día se ve involucrado un sistema o equipo informático, tal y como se analizara en el desarrollo del presente tema.

En el desarrollo de esta investigación he dedicado un espacio para el estudio de la intimidad, del como es que se ve afectada por el afán de cada de persona por conocer la vida de los demás y los alcances jurídicos que se aplican al verse conculcados los datos íntimos del titular de la información por medio del uso indebido de los sistemas y equipos informáticos.

Si bien, la información es un elemento indispensable para la toma de decisiones y que el hombre nace con la garantía de acceso a las noticias y demás acontecimientos, también lo es que hombre nace con la plena facultad de decidir con quien compartir sus ideas, sentimientos o hechos de su vida personal o simplemente reservarlos para sí mismo.

El presente trabajo nace con el propósito de reflejar y proponer soluciones a la vasta y compleja problemática que la evolución de las nuevas tecnologías de la informática constituye.

La intimidad se muestra como una figura poco aludida en la actual sociedad, y aún no reconocida por el Estado, se habla de los diversos medios tecnológicos que han invadido nuestra sociedad, como lo son los sistemas y equipos informáticos, que constituyen ya una nueva forma de comunicación, rápida y económica.

Las nuevas tecnologías de la información y de la comunicación permiten multiplicar por mil la velocidad de tratamiento de datos, desde su capacidad de almacenamiento hasta la transmisión de los mismos.

En la denominada era tecnológica, el avance informático ha sorprendido al ser humano y lo ha expuesto a nuevos y desconocidos peligros.

Hoy toda persona puede tener acceso a un ordenador personal que le permite realizar operaciones. Permitiendo así que la informática penetre en casi todos los ámbitos de la vida social.

Con la tecnología informática se abre una nueva etapa en la que es posible recabar, almacenar, organizar y difundir informaciones en el tiempo y en el espacio, con la máxima garantía de celeridad y exactitud.

Se habla de que el ciberespacio es un microcosmos digital en el que no existen fronteras, distancias ni autoridad centralizada.

La gran mayoría de la gente sabe por puro instinto, que nadie puede inmiscuirse en su vida privada, en su intimidad, nadie puede violar ese derecho, y quien lo haga tiene que ser sancionado por esa falta.

El tomar datos de algún archivo es siempre una violación a la intimidad, pero cuando se usan computadoras, la toma de datos tiene una mayor relevancia por la agregación que se puede hacer.

Mediante la utilización de técnicas informáticas y la transmisión de datos entre ordenadores, con su capacidad de proceso se puede ejercer un control social, sin que la persona llegue a percatarse de tal suceso.

El derecho a la intimidad reconocido constitucionalmente ha establecido la prohibición de suministrar información que afecte la intimidad personal y familiar por parte de los servicios informáticos, es decir plasma la inquietud del legislador respecto a los avances tecnológicos de los sistemas informáticos y su mal uso.

Por ello, al abordar el presente trabajo en estudio, se habla de que hoy en día, con los diversos servicios que ofrece Internet, hemos logrado crear espacios en los cuales podemos almacenar información que solo concierne al titular de la misma y que es su derecho mantener fuera del alcance público, como los son fotografías, videos, correos electrónicos, pensamientos, preferencias sexuales, que por su contenido se considera que deben ser reservadas. Se hace hincapié que con los avances de la tecnología estos datos se ven perturbados por sujetos que cuentan con conocimientos especializados en la intromisión a las bases de datos de compañías que ofrecen un resguardo de diversa información de usuarios, que no les ha sido autorizado conocer, sin embargo por sus habilidades en el uso de Internet y de los equipos informáticos invaden nuestra intimidad.

Cada vez que alguien utiliza el correo electrónico, navega por la red, intervienen en foros de conversación (*chats*), participa en grupos de noticia o hace uso de un servicio, está revelando datos acerca de su personalidad, economía, gustos, hábitos sociales, residencia, etc., los cuales pueden ser aprovechados maliciosamente por terceros en perjuicio del usuario.

Internet ha supuesto un factor de incremento de formas de criminalidad informática, al potenciar la difusión de sabotajes, virus y accesos indebidos a los sistemas por parte de un número imprevisible e incontrolable de *hackers*.

La informática actúa, en suma, como un elemento funcional activo para la comisión de actos delictivos y/o pasivo, en cuanto sistema operativo objeto de atentados criminales.

Las repercusiones de la informática en el Derecho están siendo cada vez más extensas e intensas. Dar cuenta de ellas resulta una tarea prácticamente inviable, entre otras cosas por el carácter abierto y dinámico que reviste esa proyección. Baste pensar que, que en el horizonte tecnológico del presente, muchos de los problemas y de las soluciones jurídicas tradicionales aparecen irremediabilmente caducos. Ello impele a diseñar nuevos instrumentos de análisis y marcos conceptuales prontos para adaptarse a las exigencias de una sociedad en transformación. La informática jurídica, el derecho informático y los sectores que las integran, constituyen una de las aportaciones con que cuenta la teoría del Derecho actual para responder a esos apremios.

La adaptación de un sistema normativo que debe crear los tipos para incriminar se ve complicado ante la aparición de estos nuevos modelos delictivos. La informática ha creado nuevas formas de delito a la vez que ha permitido perfeccionar las anteriores.

El derecho penal tradicional se ha visto desbordado recientemente por la aparición de numerosos delitos impensados en otra época.

En lo que corresponde a las consecuencias legales que se derivan de la revelación u obtención sin autorización de datos de carácter personal, cabe precisar que como dicha violación va acompañada tanto del agravio que se le causa al gobernado como el beneficio del infractor del derecho, necesariamente debe de haber un resarcimiento en los derechos del afectado.

Se habla de los elementos del delito en su aspecto positivos, así como se hace alusión a los delincuentes informáticos, en su forma de operar al momento de la comisión de conductas delictivas haciéndose valer de sistemas y equipos informáticos.

Dentro de este trabajo se sitúa a la policía cibernética como una figura coadyuvante del ministerio público, con el fin de combatir los delitos cometidos por el mal uso que se les da a los equipos informáticos.

La legislación vigente en México descuida muchos de los aspectos en relación a que autoridad es competente para conocer de conductas antisociales mediante el uso indebido de sistemas y equipos informáticos, toda vez que no toma en cuenta que dichas acciones delictuosas pueden ser cometidas por sujetos internacionales.

En mi tesis que tiene como fin primordial obtener el título de licenciada en derecho, he realizado el estudio de la situación actual del tema, en los capítulos de conclusiones y propuestas, formulo las modificaciones que, desde mi particular punto de vista, deben hacerse a la materia realizada.

“LA INTIMIDAD Y SU TRANSGRESIÓN MEDIANTE EL USO INDEBIDO DE EQUIPOS INFORMÁTICOS”

CAPÍTULO PRIMERO

GENERALIDADES DE LA INTIMIDAD, INFORMACIÓN Y DATOS PERSONALES

1.1 DIVERSAS ACEPCIONES DEL CONCEPTO DE INTIMIDAD.

El término íntimo viene de *intimus*, superlativo latino que significa "lo más interior". La intimidad corresponde al ámbito psicológico e **inconmensurable** del individuo, comprende su personalidad, sus valores morales y religiosos, sus tendencias sexuales y amorosas, sus orientaciones ideológicas. Lo íntimo está más fuera del alcance del interés público que lo privado. Se alude al carácter oculto o secreto de aquellas circunstancias internas esenciales que rodean la existencia del hombre. Es un derecho innato, surgido con el comienzo de la vida misma del individuo

La intimidad se refiere a una esfera tan interior del individuo que en principio sólo él puede revelar, es, asimismo, el derecho al secreto, a no ser conocidos en ciertos aspectos, por los demás, a que no sepan lo que somos y lo que hacemos; se encierra la proclamación explícita de estar dotado de iniciativa, dueño de sí mismo y responsable de sus actos, en uso de su libertad.

La intimidad es el poder concedido a la persona sobre el conjunto de actividades que forman parte de su círculo íntimo, personal y familiar, poder que le permite excluir a los extraños de entrometerse en él y darle una publicidad que no desee el interesado.

Por lo tanto, en mi particular acepción, la intimidad es todo aquello que queremos ocultar de nuestra vida, lo que nos singulariza como sujetos, lo que

constituye nuestra esencia, que a criterio propio y apegándonos a costumbres que hemos adoptado, hay ciertos acontecimientos que al ser expuestos en un ámbito público podrían llegar a ser criticados, discriminados y castigados, ya sea por el núcleo familiar o hasta por la misma sociedad. La intimidad faculta al individuo a practicar un control eficaz sobre sus propias experiencias y vivencias. Así, lo íntimo es lo más personal siendo, por tanto, todo lo íntimo secreto y reservado.

Con el vocablo “intimidad” se alude no sólo al carácter oculto o secreto de aquellas circunstancias que rodean la existencia del hombre sino que se refiere sobre todo a circunstancias internas, esenciales del individuo y que éste mantiene como núcleo de su personalidad. Así, lo íntimo no representa aquello que la persona quiere reservar, sino parte de su esencia individual que se encuentra en su interior y le es propia, como aspecto de su condición de ser humano, y sin la cual se vería despojada de su sustancialidad humana. Íntimo, pues, no se identifica con secreto o desconocido para terceros; va más allá, porque representa la propia esencia de cada individuo en cuanto ser humano, su propia individualidad.

1.2 CONCEPTOS AFINES CON LA INTIMIDAD.

A) SECRETO.

Por secreto se debe entender todo lo oculto, ignorado, escondido. Conocimiento que exclusivamente tiene alguien de una cosa.

El secreto tiene un componente relacional que no afecta a la intimidad, que nace y concluye con el sujeto; el secreto nace de la idea de compartir, de hacer cómplices a los demás de nuestras vivencias y sentimientos, mientras que la intimidad está próxima a la idea de reserva, de disfrute interior de la propia existencia.

No todo lo secreto será íntimo; aquello que es revelado en determinadas circunstancias o a determinadas personas aunque no se identifique con la interioridad del individuo, con su esencia persona, deberá ser ocultado por aquellos a quienes se

comunicó, es decir, tiene el deber jurídico además de moral, de no compartir la información recibida con terceros extraños.

B) CONFIDENCIALIDAD.

Representa una manifestación de la “confianza” que se ha depositado en un tercero, que será quien oculte la complicitad de la persona, lo que le ha sido revelado

Es aquello que se hace o dice en confianza, es la esperanza firme que se tiene en un persona o cosa, como ánimo o aliento de ser tratado con familiaridad y con la seguridad de que lo tratado o depositado, entre las personas en cuestión, será manejado de una manera extremadamente íntima y en secreto, no accesible al público en general. Es una característica importantísima de datos realizados entre personas, buscando sea privilegiado y personal, no accesible a los demás ni mucho menos del dominio público. Se deposita de una a otra persona algún tipo de información, de cosa o de sentimiento con la posibilidad inminente de ser particular y de buena fe.

La confidencialidad constituye un medio o instrumento de protección de la intimidad.

C) PRIVACIDAD.

El concepto de privacidad nace del deseo de proteger el conjunto de facetas de la personalidad del individuo que carecen de significación consideradas aisladamente pero que, coherentemente enlazadas, pueden arrojar un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado en tanto afecte a su honor, nombre o imagen. Es este aspecto el que debe ser defendido, y así lo recogen los instrumentos internacionales de protección de los derechos humanos.

Privado, se define como contrapuesto a público; representa lo apartado, lo retirado, exclusivo de la persona. Se identifica con comportamientos, actitudes o comunicaciones que no se exponen a los demás, si bien una decisión del sujeto los podría fácilmente transformar en públicos.

1.3 DIFERENCIAS ENTRE INTIMIDAD Y PRIVACIDAD.

Tres son los aspectos susceptibles de defensa que afectan al ámbito personal: lo secreto o conjunto de hechos que deben permanecer ignorados; lo íntimo o ámbito singular o familiar que debe quedar libre de intromisiones, y lo privado o ámbito puramente personal relacionado con el honor, nombre o imagen de un individuo.

Por tanto, no parece que privado e íntimo sean sinónimos; íntimo se aplica a las cosas profundas e interiores del alma humana y, por extensión, a lo cercano, mientras que privado se refiere a lo personal y lo particular, esto es, a aquello que se mantiene cerrado al acceso público. Nótese que ninguno de los usos anteriormente señalados del adjetivo privado admiten su sustitución por íntimo sin que se produzca un cambio de sentido: una reunión íntima es un encuentro muy cercano, donde existe gran proximidad afectiva, mientras que una reunión privada es un encuentro alejado del público, o bien una reunión para abordar cuestiones particulares; un mensaje íntimo implica cercanía estrecha y confesión de sentimientos profundos, mientras que un mensaje privado es aquel que se envía de particular a particular, sin utilizar un medio público o al margen del conocimiento público.

En nuestro entorno social y cultural utilizamos en muchas ocasiones en forma indistinta ambos conceptos, probablemente se debe a que ambos tienen el mismo objeto.

El concepto vida privada es muy amplio, genérico y engloba a todo aquello que no es o no queremos que sea de general conocimiento. Dentro de ello, existe un núcleo que protegemos con más celo, con mayor fuerza porque lo entendemos como esencial en la configuración de nuestra persona. A esto último le denominamos intimidad.

“Vida privada” hace referencia a una esfera de retiro y aislamiento, al ámbito donde los demás dejan en paz al sujeto, con tranquilidad para actuar y, donde no tienen derecho a inmiscuirse en tanto que la intimidad se refiere al interior del individuo, a un

“mundo propio”, fuera de los ojos de los demás, se trata de la esfera más sagrada de la persona.

Cada uno de nosotros elaboramos nuestra vida privada o nuestra intimidad con grado, rangos y caracteres diferentes.

Muy claramente nos lo ejemplifica la autora Cabezuelo Arenas, “Pertenece a mi vida privada el ámbito matrimonial, mis hijos, mis padres, pertenece a mi intimidad cómo figuro aquél ámbito, como lo llevo a efecto. Es conocida mi situación civil, si viven mis padres o tengo hijos (vida privada). Si es mi voluntad han de desconocerse mis relaciones sexuales, o los detalles de ésta (intimidad). La intimidad es la lejanía, la vida privada lo más próximo desde la perspectiva de los demás”.¹

En ambas rige la libertad, existe la conciencia social de restricción, de no injerencia, de ello deviene la protección legal.

El elemento consustancial tanto en la intimidad como en la vida privada hemos afirmado que es la voluntad, la libertad o la facultad de exclusión del propio sujeto, y es éste quien configura el grado, quien deslinda la intimidad de la vida privada.

1.4 QUE DEBEMOS ENTENDER POR DERECHO.

El Derecho nace por y para la persona, que se erige así en fundamento y objeto del ordenamiento jurídico, en tanto los bienes que son propios del individuo, que le definen como tal ante los demás, presentándose así en el ámbito jurídico como objeto de protección.

Es un principio tan viejo, como el common law, que el individuo debe gozar de total protección en su persona y en sus bienes.

¹CABEZUELO ARENAS, Ana Laura. “DERECHO A LA INTIMIDAD”. Editorial Tyrant Lo Blanch, Valencia, 1998. p. 462.

Se debe entender por **Common Law** o **Derecho consuetudinario**, como el término usado para referirse al grupo de normas y reglas de carácter jurídico no escritas, pero sancionadas por la costumbre o la jurisprudencia, que son fundamento ineludible del Derecho de los países anglosajones.

El Derecho es una forma de libertad social (distante) que condiciona la personalización de los individuos y el desarrollo de la sociedad.

Como un concepto personal y apegada a los términos comunes de los que habla la doctrina, tenemos que **derecho** es la protección que tiene la persona sobre sí misma, su vida, sus actos, su integridad física, su intimidad, que por naturaleza va implícita al ser humano en cualquier tiempo o espacio, misma que es reconocida por el Estado, y por lo tanto es imprescriptible e inalienable.

La finalidad del derecho debe ser tanto garantizar a aquellas personas cuyos asuntos no son causa de preocupación legítima para la comunidad, como proteger a toda persona, sea quien sea, sin distinguir posición social, de ver divulgados, contra su voluntad, asuntos que pudiese preferir mantener reservados. Lo que se censura y hay que evitar, siempre que sea posible, es la injustificada violación de la intimidad.

El derecho no crea la dignidad de la persona, pero sí asegura su eficacia, garantiza su respeto y posibilita su desarrollo.

1.5 BREVES ANTECEDENTES DEL DERECHO A LA INTIMIDAD.

Surge con la revolución burguesa, con lo que actualmente se define como derecho a la vida privada.

Al remontarnos en la Edad Antigua hallamos las primeras manifestaciones de la intimidad y su trascendencia respecto a la vida individual y social de la persona. Así, en Grecia a través de la reflexión se alcanzaba una plena vida interior, el hombre alcanzaba la sabiduría y el fundamento de su individualidad.

Todas las actividades humanas eran partícipes en la vida común, no se entendía una separación entre lo público y lo propio o personal, y hasta el aspecto más interior de la vida humana (natalidad, uniones conyugales, educación) quedaba a merced del estado y sus leyes.²

En Roma, la intimidad era entendida como la exigencia de cada individuo de un conocimiento de sí mismo, de alcanzar la esencia de la persona y acotar un espacio de dominio interior que nadie pudiera invadir. Tal como recuerda FARIÑAS MATÓN, los romanos admitían un “derecho de propiedad del yo”, cuya manifestación principal se traducía en el reconocimiento de un respeto a la persona del prójimo, en cuyo mundo interior sólo se penetraba si la intensa vinculación con su “propietario” lo hacía aconsejable.³

En la Edad Media, se profundiza la búsqueda de los bienes inmateriales, se abandona la concepción patrimonial de la intimidad. Se configura como el discernimiento personal que cada individuo tiene como ser humano único, diferente y extraordinario. A través del pensamiento cristiano, la intimidad se alza como valor supremo o sagrado de la existencia individual, así el hombre se constituye en sí mismo portador de valores propios y absolutos, que reserva en su esfera privada.

Así, la intimidad es un bien “sagrado” para el hombre, y que a nadie es lícito invadir, tanto la capacidad intelectual, como volitiva del ser humano, encontrándose en íntegra relación con la intimidad del individuo.

En la Edad Moderna, se despierta en el hombre un anhelo de afirmación de su intimidad, encontrando su naturaleza de ser intelectual, vinculado al respeto y reserva del mundo interior de la persona; el conocimiento de sí mismo, el disfrute íntimo de las experiencias, sentimientos o pensamientos; constituye un bien irrenunciable del ser

² RUIZ MIGUEL, Carlos. LA CONFIGURACIÓN CONSTITUCIONAL DEL DERECHO A LA INTIMIDAD. Madrid, Tecnos, 1995, Pág. 15

³ FARIÑAS MATÓN, Luís M^a. EL DERECHO A LA INTIMIDAD. Madrid, Trivium, 1983, Págs. 288 – 289.

humano, que le impulsa en sus relaciones sociales, y le proporciona dominio de su esfera de actuación y reflexión.

Convendrá en admitir que el impulso definitivo en el reconocimiento de la necesidad humana de desarrollo intelectual y sentimental interior se alcanza en la sociedad moderna que, dominada por el ansia de saber y conocer de los demás la mayor información posible, orienta la conducta de los individuos según la máxima: “la información es poder”; y ciertamente, esto es así, cuanto más se conozca de los demás mejor se podrá controlar y vigilar su comportamiento. No obstante, esta necesidad humana de aislamiento interior ya había sido sentida mucho tiempo antes. El hombre requiere para su plena madurez personal una manifestación interior de su vida individual, que le sea permitido interiorizar sus vivencias, pensamientos o sentimientos allí donde el acceso permanece cerrado a los demás.

1.5.1 DERECHO A LA INTIMIDAD.

La raíz de la existencia del derecho radica en la unidad finalista que caracteriza a la persona humana, en el ser dueña de sí misma (*sui iuris*), autónoma (libre) y digna ante sí, y ante otros (exigente).

La intimidad es un derecho innato, surgido con el conocimiento de la vida misma del individuo.

Siendo la intimidad un atributo del hombre, una consecuencia de la naturaleza humana, y viviendo aquel en sociedad, parece lógico que deba de existir una protección normativa, que alcance a lo personal.

El derecho a la intimidad consiste en un conjunto de facultades del individuo para desenvolverse sin lesionar derechos ajenos, y un poder de exclusión del conocimiento ajeno de su vida íntima. Por ello, el derecho a la intimidad se sitúa en el marco de los derechos humanos que suelen calificarse de “individuales”.

El derecho a la intimidad es un derecho fundamental de la persona humana, autónomo, basado en los valores constitucionales como la dignidad, el respeto mutuo, el libre desarrollo de la personalidad y la igualdad entre los seres humanos y en los principios y fuentes normativas internacionales y universales, como fundamento del orden político y la convivencia pacífica de los ciudadanos en un estado social de Derecho.

Garantiza una calidad en las relaciones con los demás, que tan solo se conozca aquello que cada persona revela, sin que ello suponga la pérdida de control sobre la propia información.

BAJO FERNÁNDEZ, dice que el derecho a la intimidad representa un valor especial e irrenunciable en la dimensión vital del hombre y estima que “todos los derechos humanos naturales, congénitos al hombre, o mejor, inherentes a su propia esencia, son de igual valor, a partir del “derecho a la vida” que, por razones obvias, es derecho básico o radical”.⁴

El common law garantiza a cada persona el derecho a decidir hasta que punto pueden ser comunicados a otros sus pensamientos, sentimientos y emociones. Bajo nuestro sistema político, nunca se puede forzar a alguien a expresarlos (salvo cuando se comparece como testigo); e incluso, cuando ha elegido expresarlos, retiene por regla general, el poder de fijar los límites de la publicidad que se les podrá dar. La existencia de este derecho no depende del medio concreto de expresión utilizado. No importa que sea de palabra o por señas, mediante la pintura, la escultura o la música. La existencia de este derecho no depende tampoco de la naturaleza o valor del pensamiento o de la emoción, ni de la calidad de los medios empleados en su expresión.

Es el autor de la información, quien tiene derecho a decidir si lo que es suyo debe salir a la luz pública.

⁴ BAJO FERNÁNDEZ, M. “PROTECCIÓN DEL HONOR Y DE LA INTIMIDAD” en “Comentarios a la Legislación Penal”, dirigidos por M. COBO DEL ROSAL. Tomo I. DERECHO PENAL Y CONSTITUCIÓN. Madrid, 1982. paginas 101 y 110.

El derecho a la intimidad se configura como un ámbito reservado *ad intra*, donde opera la voluntariedad del individuo respecto de aquello que debe trascender y a la vez es el derecho a controlar lo que *ad extra* puede ser conocido del ciudadano.

En síntesis, el derecho a la intimidad es la facultad que le reconoce el Estado al hombre de mantener reservada la información que considere no comunicable. Entonces, el hombre decide cuales son los datos que debe limitar a su saber y el Derecho es el que se encarga mediante sus leyes de evitar la intromisión de terceros a dicha información.

El derecho a la intimidad tutela la zona espiritual, reservada de la persona que permanece en su interior, referida a la conciencia de sí mismo como ser humano libre en su ámbito moral e intelectual.

Este derecho protege la parte más íntima de una persona, esto es, esa esfera personal que define qué es y qué no es privado. Dicho de otra forma, hablar de intimidad es hablar de sentimientos, de creencias (políticas, religiosas), pensamientos o de una información, o la relativa a la vida sexual, cuya difusión puede producir ciertas reservas al individuo. Se trata en definitiva de aquellos datos que bajo ninguna circunstancia proporcionarían un individuo de manera libre y consciente. Partiendo de este punto, nacen derechos como la inviolabilidad de su intimidad o el derecho a la propia imagen; ambos muy relacionados con la parte más privada de la psique del individuo.

Debido a la naturaleza de los medios con los que se invade la intimidad, el daño infligido guarda, a simple vista, un parecido con los agravios contemplados por la ley de la difamación y libelo, mientras que una reparación legal de este daño debería considerar únicamente los sentimientos heridos, como causa sustantiva de la acción. Por otra parte nuestro derecho no reconoce ningún principio bajo el que pueda otorgarse una compensación por mera ofensa a los sentimientos.

Pudiera afirmarse que la definición que con mayor acierto refleja la adecuación de los derechos de la personalidad a los nuevos avances tecnológicos o informáticos es aquella que los describe como el derecho del individuo a decidir por sí en qué medida o en qué circunstancias desea compartir con terceras personas, sus pensamientos, sentimientos y expresiones personales.

Es un derecho, cuyos pilares básicos se han visto profundamente transformados como consecuencia de los avances que la ciencia y la tecnología han introducido en las relaciones humanas.

Tener derecho a la intimidad es una forma de decir que los demás tienen deber de respetarla y que, en caso de lesión, se pueda exigir castigo al culpable.

El derecho a la intimidad debe ser considerado elemento principal en la construcción del derecho a la autodeterminación informativa.

Se aspira al reconocimiento a cada individuo de una cierta capacidad de decisión respecto al registro y utilización de los datos relativos a su persona, derecho que en modo alguno tiene carácter absoluto.

El derecho a la intimidad se define a través de lo que es propio y exclusivo de la persona, es el derecho que concierne a cada persona a ser ella, será quien determine cuándo y hasta qué límite desea entrar en contacto con la sociedad que lo rodea.

1.6 CONCEPTO DE INFORMACIÓN PÚBLICA E INFORMACIÓN PRIVADA.

En sentido general, la **información** es un conjunto organizado de datos **procesados**, que constituyen un mensaje sobre un determinado ente o fenómeno. De esta manera, si por ejemplo organizamos datos sobre un país, tales como: número de habitantes, densidad de población, nombre del presidente, etc. y escribimos por ejemplo, el capítulo de un libro, podemos decir que ese capítulo, constituye información sobre ese país. Cuando tenemos que resolver un determinado problema o tenemos que

tomar una decisión, empleamos diversas fuentes de información (como podría ser el capítulo mencionado de este libro imaginario); construimos lo que en general se denomina conocimiento o información organizada que permite la resolución de problemas o la toma de decisiones.

La información es la noticia o dato de una cosa. En el mundo actual se ha transformado en una necesidad de carácter ineludible en la toma de decisiones.

En la actualidad, la globalización permite el acceso a enormes volúmenes de información depositados en soportes cada vez más complejos, con increíbles posibilidades de almacenamiento y conexión con otras fuentes. Nos referimos a las bases de datos, las redes de transmisión de datos, la red de Internet...etc.

Cabe señalar que dentro de nuestro entorno en el cual nos desenvolvemos, manejamos dos tipos de información, como los son, la pública y privada, la primera de ellas es de la cual toda persona puede tener acceso, ya que el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, a la letra dice “ El derecho a la información será garantizado por el Estado”, lo cual nos permite conocer datos de relevancia social, como lo son asuntos del propio Estado, de instituciones gubernamentales, decisiones políticas, etc. La segunda es aquella sobre la cual el titular posee un derecho exclusivo de uso o conocimiento pero que en mayor o menor medida es conocida por un grupo de personas a su alrededor y por el Estado, respondiendo a fines de garantía de los derechos del ciudadano.

De acuerdo al tema que me ocupa, es esencial que haga hincapié en que debe de reconocerse otro tipo de información de la cual nos da una clara definición el autor ANDRÉS CÁMPOLI, “**información íntima**, es aquella sobre la cual el titular tiene la absoluta exclusividad de su conocimiento y divulgación, que se encuentra ligada a sus procesos internos de selección y no puede ser conocida ni aún en circunstancias especiales por persona alguna ni por el Estado”.⁵

⁵ ANDRÉS CÁMPOLI, Gabriel. “DELITOS INFORMÁTICOS EN LA LEGISLACIÓN MEXICANA”. Editorial Instituto Nacional de Ciencias Penales, 2ª Ed., 2007, Pág. 65.

1.6.1 DERECHO A LA INFORMACIÓN Y SU CONTROL.

El derecho a la información es una garantía individual de carácter social. Retomando lo expuesto en el punto anterior respecto de la información. La información es el intercambio de ideas, la comunicación de acontecimientos, pensamientos, sentimientos, etcétera. La comunicación de la información puede ser masiva o de “difusión” o puede ser comunicación interpersonal. El legislador se ocupó de adicionar esta garantía al lado de la de la libertad de expresión, por medio de las cuales el estado se compromete a proteger el derecho de unos a manifestar las ideas o comunicar los hechos y de que otros se enteren de toda esa información.

La información, para que pueda servir, debe estar organizada. Existen muchos modos de organización. Pero la diferencia entre la organización manual y la computarizada radica en la posibilidad que tiene esta última de recuperar esa información en cualquier momento, en cualquier orden y en cualquier combinación; con la seguridad de tener toda la información, de poder hacer un rápido chequeo de la misma y de poder reorganizarla tantas veces como uno quiera sin perder las anteriores. Todo ello de manera inmediata, de modo automático, y sin importar cuál sea la cantidad de información ni de las combinaciones.

El derecho a la información es una garantía constitucional, contenida en el artículo sexto de la Constitución Política de los Estados Unidos Mexicanos, que a la letra dice: “.. *Artículo 6°.- La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito o perturbe el orden público; el derecho a la información será garantizado por el Estado...*”

El derecho a la información comprende dos vertientes, a saber, el deber de informar y el derecho a ser informado.

a) El deber de informar. Esta vertiente comprende desde los actos la investigación, recopilación y demás actividades destinadas a la obtención de información hasta los de difusión de la información, es decir, es la parte garantizada por la constitución denominada libertad de expresión.

b) El derecho a ser informado. Es el derecho de los individuos a estar comunicados respecto de los sucesos públicos y en general de todo acontecimiento o idea que pueda afectar su vida personal o le pueda hacer cambiar su forma de pensar. Pues como lo dijimos, la información nos dota de poder y nos permite realizar con mayor eficacia nuestras relaciones sociales y laborales.

El derecho a la información emplea los más diversos espacios, instrumentos y tecnologías para la transmisión de hechos e ideas.

El derecho a la Información, actualmente se encuentra consignado en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, la cual tiene en cuenta aspectos tales como la veracidad de la información proporcionada, fijación de los plazos para la entrega de la información; vías administrativas, jurisdiccionales y judiciales para actuar frente a la denegatoria o entrega parcial de información; imposición de sanciones, régimen de excepciones, etc. O sea, que el derecho a la información, se encuentra estrechamente vinculado con el derecho a conocer la verdad, exige que las autoridades se abstengan de dar a la comunidad información manipulada e incompleta.

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, contempla limitaciones específicas del ejercicio del derecho a la información, tendientes a equilibrar el derecho del individuo frente a terceros y a la sociedad, puesto que el ejercicio de ese derecho no debe menoscabar la moral, los derechos de terceros, que implica el honor, la dignidad y el derecho a la intimidad de éste, en su familia y decoro; así como tampoco puede provocar algún delito o perturbar el orden público.

Definitivamente, el derecho a la intimidad se encuentra en conflicto con la cultura informacional, específicamente y por lo que atañe a la presente investigación, con la información automatizada, empero no con el derecho a estar informado, pues el derecho a la información no comprende los datos de una persona o empresa que no son susceptibles de publicar. La autonomía individual integrada por sentimientos, hábitos, costumbres, relaciones familiares, posición económica, creencias religiosas,

salud mental y física y todos los hechos y datos que integran el estilo de vida de una persona que la comunidad considera reservadas al individuo y cuyo conocimiento o divulgación significa un peligro para la intimidad.

Respecto de lo anterior la autora CAMPUZANO TOMÈ, hace mención del Principio de proporcionalidad, se persigue con ello conseguir el equilibrio entre el efectivo ejercicio del derecho a la libertad de expresión con el derecho a la intimidad del sujeto de los datos.⁶

Lo anterior nos pone de manifiesto que no por el hecho de que al ser humano se le reconozca el derecho de ser informado de los acontecimientos que atañen a la actual sociedad, éste tendrá la facultad de inmiscuirse en la información íntima de otra persona, ya que ese aspecto no es considerado que sea del conocimiento del público por contener datos de relevancia personal y privada, por lo tanto debe existir una limitante en el conocimiento de determinada información y existir un equilibrio entre el derecho y los abusos del mismo.

1.7 DATOS PERSONALES.

Es la información de una persona física, identificada o identificable, que tiene relación con su origen étnico o racial, su vida afectiva y familiar, sus características físicas, morales o emocionales, su domicilio y número telefónico, su patrimonio, ideología y opiniones políticas, sus creencias o convicciones religiosas o filosóficas, su estado de salud físico o mental, sus preferencias sexuales, u otras análogas que afecten su intimidad.

A) DATOS PERSONALES ÍNTIMOS.

En definitiva, son los relacionados al orden privado de los individuos que los hacen merecedores de una protección más profundizada y específica que los demás

⁶ CAMPUZANO TOMÈ, Herminia. VIDA PRIVADA Y DATOS PERSONALES. SU PROTECCIÓN JURÍDICA FRENTE A LA SOCIEDAD DE LA INFORMACIÓN. Editorial TECNOS. Madrid 200. Pág. 179.

tipos de datos generales debido a que se revelan exclusivamente de forma particular e individual, y rara vez son objeto de tratamiento público.

B) DATOS PERSONALES PÚBLICOS.

A modo ejemplificativo serían el nombre y apellido, domicilio, estado civil, filiación, número de teléfono, la credencial de elector, CURP, grado de estudios.

CAPÍTULO SEGUNDO

NOCIONES GENERALES DE LA INFORMÁTICA. Y SUS VARIANTES EN RELACIÓN CON LA INTIMIDAD

2.1 BREVE ANÁLISIS DE EQUIPOS INFORMÁTICOS.

A las computadoras se les denomina equipos informáticos y a su vez se le conoce por el término ordenadores.

Entonces, tenemos que computadora es una máquina electrónica a la que se le introduce una serie de datos y de órdenes (comandos) para que los manipule y procese con la ayuda de la memoria interna; tras realizar las operaciones indicadas, los devuelve en forma de resultados finales o como nuevos datos que permiten realizar operaciones posteriores.

La Computadora es un dispositivo electrónico capaz de almacenar información, procesar datos y entregarle al usuario los resultados de la información procesada. Gracias a los avances de las tecnologías de redes e Internet las computadoras en la actualidad también pueden ser utilizadas como herramientas de telecomunicaciones.

A continuación se detallan las características básicas de las computadoras:

- a) las computadoras funcionan mediante impulsos electrónicos, lo cual les permite trabajar internamente a una velocidad muy cercana a la velocidad de la luz, es decir, casi 300 000 kilómetros por segundo.
- b) las computadoras tienen la capacidad de seguir instrucciones, una a una, las cuales en conjunto satisfacen la solución de problemas administrativos, cálculos laboriosos o simulaciones físicas, lo cual, aunado a la prodigiosa velocidad con que operan, permiten obtener resultados en tiempos imposibles de alcanzar por otros medios.

- c) las computadoras tienen la facultad de tomar decisiones en función de los datos que procesan, lo cual significa que pueden resolver problemas diversos y encontrar soluciones sin importar prácticamente las variantes de los datos que se le proporcionen.
- d) Las computadoras están dotadas para trabajar con márgenes de precisión inigualables por ningún otro mecanismo.
- e) las computadoras pueden almacenar cientos de millones de datos en un espacio de sólo algunos metros cuadrados.

Para su funcionamiento, la computadora requiere de un sistema informático y éste a su vez se compone de dos subsistemas: *Hardware* y *Software*.

Para entender el complejo mundo de una computadora -también llamada en algunos lugares ordenador o PC (por Computadora Personal)-, hay que tener en cuenta dos partes fundamentales que la conforman: el *hardware* y el *software*. El primero hace referencia a todos los elementos físicos que la componen (CPU, *Mouse*, monitor, teclado, etc.). El segundo, el software, tiene que ver con los programas que permiten su funcionamiento (por ejemplo, el sistema operativo *Windows*).

Asimismo, dentro del hardware podemos diferenciar entre componentes internos y periféricos externos de entrada/salida. En cuanto a los componentes internos, básicamente se encuentra la placa madre (dispositivo madre que interconecta todos los elementos que integran la computadora entre sí), el procesador o CPU (el “cerebro” de la PC) y los dispositivos de almacenamiento, como la memoria RAM, que guarda la información que se utiliza en el momento y el disco duro, que es el que posee la capacidad de almacenamiento masiva en donde se guardan los programas, archivos, etc.

En cuanto a los periféricos, los hay de entrada y salida. Los de entrada son el *mouse*, teclado, *webcam*, *scanner*, entre otros. Y los de salida, la impresora, el monitor, las bocinas, etc.

Finalmente, también hablamos del software, en donde se encuentra por un lado el sistema operativo, que es el que permite administrar las funciones de la computadora y que se ejecuten los programas. Y las aplicaciones del usuario, que son aquellos programas que instala el usuario y que son ejecutados por el sistema operativo en general, como por ejemplo los antivirus o los editores de texto.

Las computadoras son actualmente los dispositivos más populares y utilizados a los efectos de realizar operaciones tan diversas como desarrollar contenido, comunicarse con otras personas, buscar información, utilizar aplicaciones diversas, y cientos de otras posibilidades.

Técnicamente, un ordenador es una máquina programable conformada por un conjunto de circuitos y componentes integrados (entre ellos el más relevante sería el microprocesador o cerebro de la máquina) que pueden ejecutar secuencias, rutinas y operaciones con rapidez, orden y sistematización en función de una serie de aplicaciones prácticas para el usuario programadas previamente.

Las aplicaciones más frecuentemente utilizadas en todo tipo de ordenadores son el uso de procesadores de texto y otras similares como hojas de cálculo y bases de datos, navegadores *web* para acceder a Internet, programas de correo electrónico, reproductores de archivos multimedia y aplicaciones que funcionan a través de la *web* como las redes sociales.

Todos los ordenadores de uso general requieren los siguientes componentes de hardware:

- Memoria: Permite almacenar datos y programas al ordenador, por lo menos temporalmente.
- Dispositivo de almacenamiento masivo (*mass storage device*): Permite que el ordenador conserve cantidades grandes de datos permanentemente. Los discos duros son un ejemplo de dispositivo de almacenamiento masivo.
- Dispositivos de entrada (*input devices*): Generalmente teclado y ratón, el dispositivo de entrada es el conducto a través de el cual los datos y las instrucciones se introducen en un ordenador.

- Dispositivos de salida (output devices): La pantalla de visualización, la impresora, o cualquier otro dispositivo que te deja ver el resultado de lo que ha hecho el ordenador.
- La unidad de proceso central (CPU): Es el cerebro del ordenador, es el componente que realmente ejecuta las instrucciones.

En síntesis, los equipos informáticos son lo que conocemos actualmente como computadoras, las cuales las utilizamos para una diversidad de actividades, que va desde escribir un simple texto, hasta hacer uso de la misma para lograr comunicarnos con personas de otros países, es más, la vida social se desenvuelve ya mediante los servicios informáticos, toda vez que mediante el uso de la Internet nos permite realizar movimientos bancarios, almacenamiento de información a través de cuentas de correo electrónico, convirtiéndose ésta en uno de los servicios mas utilizados por los cibernautas.

2.1.1 CONCEPTO DE INFORMÁTICA.

La palabra **informática** es un neologismo derivado de los vocablos información y automatización, sugerido por Phillippe Dreyfus en el año de 1962. En sentido general, la informática se define como un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información.⁷

Podemos decir entonces, que Informática es, el Conjunto de disciplinas y técnicas desarrolladas para el tratamiento automático de la información, considerada como soporte de los conocimientos de la sociedad humana, mediante el uso de computadoras. O bien, la Ciencia del tratamiento automático y racional de la información considerada como soporte de los conocimientos y las comunicaciones.

Conceptualmente, se puede entender como aquella disciplina encargada del estudio de métodos, procesos, técnicas, desarrollos y su utilización en ordenadores (computadores), con el fin de almacenar, procesar y transmitir información y datos en

⁷ TÉLLEZ VALDÉS, Julio. DERECHO INFORMÁTICO. Tercera Edición. Editorial MC GRAW HILL, México 2004, Pág. 514.

formato digital, por lo tanto la electrónica juega un papel muy importante en la informática ya que mediante esta ciencia se puede entender a plenitud el entorno de hardware y software.

La informática, si bien en la actualidad se relaciona con los ordenadores, es también un medio particular de pensar y afrontar los problemas de la información que se vincula con la cibernética (ciencia de la comunicación y control entre el hombre y la maquina).

2.2 CARACTERÍSTICAS FUNDAMENTALES DEL DERECHO INFORMÁTICO.

Actualmente tenemos al derecho informático como una nueva rama del conocimiento jurídico, es propiamente una disciplina que se encuentra en continuo desarrollo.

Constituye una ciencia y rama autónoma del derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en dos aspectos: a) Regulación del medio informático en su expansión y desarrollo y b) Aplicación idónea de los instrumentos informáticos

El derecho informático es una rama de las ciencias jurídicas que considera a la informática como instrumento (informática jurídica) y objeto de estudio (derecho de la informática).

Derecho Informático se define como un conjunto de principios y normas que regulan los efectos jurídicos. Es una rama del derecho especializado en el tema de la informática, sus usos, sus aplicaciones y sus implicaciones legales. El Derecho Informático es la aplicación del derecho a la informática permitiendo que se adopten o creen soluciones jurídicas a los problemas que surgen en torno al fenómeno informático. Esta nueva disciplina jurídica tiene método e instituciones propias que surgen de un fenómeno que tiene implicancias globales y que por tanto permite tener

bases doctrinales y principios similares con las peculiaridades propias de cada ordenamiento jurídico.

2.3 LA INTERNET Y SU IMPORTANCIA EN LAS DIFERENTES ÁREAS DE NUESTRA VIDA.

Internet es un conjunto de redes, redes de ordenadores y equipos físicamente unidos mediante cables que conectan puntos de todo el mundo. Estos cables se presentan en muchas formas: desde cables de red local (varias máquinas conectadas en una oficina o campus) a cables telefónicos convencionales, digitales y canales de fibra óptica que forman las "carreteras" principales. Esta gigantesca Red se difumina en ocasiones porque los datos pueden transmitirse vía satélite, o a través de servicios como la telefonía celular, o porque a veces no se sabe muy bien a dónde está conectada.

En realidad, uno de los servicios más utilizados, el servicio **WWW**, o *Word Wide Web* es tan solo eso, un servicio más de Internet, pero no es el único. Otros servicios que ofrece Internet son:

- Correo electrónico (SMTP)
- Transmisión de archivos (FTP y P2P)
- Conversaciones en línea (IRC)
- Mensajería instantánea (a través de texto, voz y/o imagen)
- la transmisión de contenido y comunicación multimedia

El acceso a los diferentes ordenadores y equipos que están conectados a Internet puede ser público o estar limitado. Una red de cajeros automáticos o terminales de banco, por ejemplo, pueden estar integrados en Internet pero no ser de acceso público.

En cuanto a organización, Internet no tiene en realidad una cabeza central, ni un único organismo que la regule o a quien pedirle cuentas si funciona mal. Gran parte de la infraestructura es pública, de los gobiernos mundiales, organismos y universidades.

Muchos grupos de trabajo colaboran para que funcione correctamente y continúe evolucionando. Otra gran parte de Internet es privada, y la gestionan empresas de servicios de Internet (que dan acceso) o simplemente publican contenidos.

Internet se ha convertido en poco tiempo en la herramienta tecnológica más revolucionaria y poderosa de todas, influyendo en prácticamente todos los niveles de la actividad humana.

Algunas de las razones de su importancia e impacto son:

- El acceso global y económico a un mundo de información, entretenimiento, conocimiento y de recursos digitales de todo tipo.
- La democratización de la información.
- Abaratamiento y agilización de las comunicaciones.
- Desarrollo, transformación y potenciamiento de negocios y campos laborales muy diversos.
- Estímulo y fomento de la comunicación y la creatividad en formas interactivas y participativas.
- Ha transformado (y sigue haciéndolo) el estilo de vida de millones de personas en todo el mundo.

VENTAJAS:

- Permanencia en contacto con amigos, parientes y colegas alrededor del mundo, a una fracción del costo de una llamada telefónica o correo aéreo.
- Conversaciones con personas sobre cualquier tema en varios idiomas diferentes.
- Exploración en millones de bibliotecas y bases de datos de información globalmente.
- Acceso a millones de documentos, diarios, reservas y programas.

- Servicio de Noticias de cualquier tipo, desde noticias deportivas hasta información meteorológica.
- Juegos en vivo y en tiempo real; permite jugar con docenas de personas de inmediato.
- Probablemente la característica más llamativa de Internet es que puede tener acceso a cualquier parte del mundo por el precio de una llamada local, es decir, la distancia de la misma no es proporcional al costo de la comunicación establecida, esto es debido a que cada tramo de red se gestiona sus propios gastos y no son repercutidos directamente al usuario.

Conectarse a la Red hoy toma, en un sentido, algo de aventura. Se necesita la predisposición para aprender y una capacidad de tomar un hábito profundo cada vez superior en poco tiempo. Visitar la Red, hoy día, es como viajar al extranjero.

Es muy común a estas alturas oír hablar de Internet en cualquier momento, a cualquier hora, en cualquier lugar.

Internet lejos de ser un medio o herramienta para gente especializada en programas o sistemas de cómputo, ha abierto sus puertas a todo el mundo y a toda la gente aun cuando no todos puedan contar con una computadora personal de su propiedad.

El correo electrónico, los *chats*, e incluso las video conferencias de computadora a computadora han dado una gran apertura al individuo para relacionarse con el mundo exterior de una manera real, en tiempo real.

Además, el usuario que ya dispone de un mínimo de conocimientos sobre navegación en Internet, fácilmente puede remitirse a la información que proporcionan algunas agencias gubernamentales.

La principal diferencia entre Internet y cualquier otra red informática reside en que esta no pertenece a ningún país, ni organismo oficial, ni a una empresa determinada, es decir, se trata de una red libre ya que cualquier persona puede acceder

a ella desde cualquier punto del planeta, de la misma forma que no existe ningún tipo de restricción para toda la información que circula por la misma.

2.3.1 LA INTERNET COMO UNA VÍA PARA EL MAL USO DE LA INFORMACIÓN PERSONAL.

Desafortunadamente, existe la posibilidad de un mal uso de los datos personales que han sido proporcionados a Internet, ya que cualquier persona que tenga instrucción técnica en sistemas de red, podría acceder a los archivos en donde se almacena esta información. Los operadores de empresas, que ofrecen los servicios de Internet únicamente se comprometen a través de simples declaraciones que resultan de buena fe, y que no salvaguardan absolutamente nada, ya que solo es por cumplir con una formalidad.

Al darle un mal uso a la información personal, puede dañarse la imagen de ésta y así la opinión de los demás para sí. Al acontecer dicha situación, cabe la posibilidad de que esto afecte su situación económica y cause daños incalculables. La opinión que se causa en los demás, aunque se niegue, es muy importante, ya que de ésto dependen muchos factores de importancia para el desenvolvimiento en sociedad.⁸

El ataque a los datos, puede ser el robo, interceptación o la modificación, borrando, destruyendo o alterando. Se pueden dar fraudes, o incluso realizar actos, de cualquier índole, ostentando ser otra persona, ya que al tener acceso a información a bases de datos personales, se puede escoger bajo que nombre se puede conducir a alguien a realizar o cometer delitos en la red.

Hay muchos programas, especialmente los de mensajería instantánea, con funciones de inicio de sesión automático que guardan el nombre de usuario y contraseña.

Con frecuencia, el usuario no sabe con certeza si el sitio que visita es confiable, desconoce cuál puede ser el destino y uso de la información que proporciona, así como

⁸ VILLANUEVA, Ernesto, "Derecho a la información", Editorial Porrúa, México 2006, Pág. 301 a 312

las repercusiones que pueda tener en la seguridad y privacidad de su persona y su familia. Estos dos aspectos resultan fundamentales en las decisiones que toman los usuarios respecto a un sitio Web.

Mientras la computadora esté encendida, estará conectada a Internet y personas maliciosas podrán tener mayor posibilidad de atacarla.

2.4 SERVICIOS INFORMÁTICOS MÁS USADOS QUE CONLLEVAN UN INTERCAMBIO DE DATOS PERSONALES E ÍNTIMOS.

Para la mayor comprensión sobre este punto, empezaremos por entender que son los servicios informáticos tal como lo señala Davara Rodríguez, “Son todos aquellos que sirven de apoyo y complemento a la actividad informática en una relación de afinidad directa con ella”.⁹

A) CORREO ELECTRÓNICO.

Servicio postal electrónico, por llamarlo de alguna manera. Es el acceso que tenemos las personas para poder estar comunicados unos con otros, enviar archivos de información, imágenes, sonidos incluso videos. Permite mantener a los individuos en la posibilidad de estar al tanto de situaciones que acontezcan en otro lugar, hasta podría decirse remoto. En términos técnicos es el espacio cibernético que las compañías, o empresas dedicadas a proporcionar el servicio brindan a las personas para recibir y enviar mensajes. Esta correspondencia de la que se menciona es principalmente enviada a otra persona para que también tenga esa reservación de espacio electrónico, y viceversa para poder recibir este tipo de mensajes es necesario contar con una dirección de correo electrónico; ésta se diferencia de otras direcciones principalmente por el carácter @, es cuando sabemos que estamos frente a una dirección de correo electrónico y que será recibida por la persona titular del servicio.

Un correo electrónico responde a un modelo tipo carta escrita, que contiene remitente, destinatario, asunto, mensaje, y que permite a su vez adjuntar archivos como

⁹ DAVARA RODRÍGUEZ, Miguel Ángel, Derecho Informático, Aranzadi, en <http://www.colex-data.es>.

documentos de texto o imágenes. Para enviar un *email* sólo hace falta una computadora (u otro dispositivo) con conexión a Internet y un software como puede ser *Outlook Express* o *Gmail* para enviar y recibir los correos. El usuario debe contar con una dirección de correo electrónico y un proveedor de correo, que puede ser de pago o gratuito y que puede utilizarse como software o directamente en la *Web*.

Además de ser más fácil y rápido, el servicio de correo electrónico cuenta con múltiples posibilidades, como la alternativa de enviar el mensaje a destinatarios con copia oculta, filtrar determinado tipo de mensajes o destinatarios, o hacer envíos a muchos destinatarios a la vez. Esto hace que comunicarse a distancia en todo el mundo sea mucho más rápido, fácil y barato.

Uno de los grandes problemas que enfrenta esta tecnología es la cantidad de *spam* o “correo basura” que es enviado y recibido por día. Esto significa que un usuario promedio probablemente recibirá muchísimo correo indeseado a diario.

A través de la red pueden transmitirse mensajes de correo electrónico. Cada usuario tiene una o varias direcciones de correo electrónico y un espacio reservado en el servidor de su red local como buzón. Diversos programas informáticos permiten enviar mensajes electrónicos de buzón a buzón. Estos mensajes pueden contener texto o cualquier otro tipo de información como imágenes, sonido o videos. Las empresas y los particulares utilizan cada vez más el correo electrónico para comunicarse, por la rapidez de transmisión y el ahorro económico que representa el uso de la tecnología.

El correo electrónico es una maravilla que ha quedado al alcance de todas las personas que deseen adquirir uno. Los correos electrónicos no cuestan absolutamente nada, solo es necesario contar con un ordenador que esté conectado a un servidor que lo introduzca en la red. De este modo, si alguien tiene deseo de adquirir un correo únicamente debe de ingresar a la página del prestador de servicio de su preferencia y proporcionar sus datos personales y escoger una denominación para que se le pueda proporcionar una dirección electrónica. Al momento de solicitar el servicio es necesario aceptar una serie de cláusulas que dicta el prestador de servicios.

Este medio de comunicación es ya muy común en la mayoría de las empresas por decir todas, y usado por la mayoría de las personas.

VENTAJAS:

- Rapidez.- el envío y la recepción de mensajes es muy rápida casi instantánea, por lo que no debemos esperar días a que información importante llegue, ni siquiera tenemos que adelantar nuestras cartas de Navidad, Año Nuevo o cumpleaños para que éstas lleguen a tiempo. Esto sucede independientemente del lugar donde se encuentre el destinatario.
- Eficacia.- podemos escribir y enviar el mensaje desde un mismo lugar, sin tener que buscar un correo, estampillas ni nada parecido.
- Facilidad.- Las pantallas de los *softwares* para correo electrónico son extremadamente sencillas y existen diversos programas cuya utilidad es únicamente el envío y recepción de mensajes.
- Utilidad.- Para aquellas personas cuya recepción de mensajes es muy alta, se pueden crear filtros que automáticamente ordenan los mensajes dependiendo de algunas variables, como fecha, remitente, asunto, prioridad, etc. Lo cual permite revisar el correo en orden de importancia, así como tirar toda la propaganda sin siquiera abrirla.

DESVENTAJAS:

- Falta de Privacidad.- debido a que los mensajes vienen abiertos, una vez que se tienen en la computadora, cualquiera puede verlos, leerlos e incluso contestarlos.
- Tamaño.- Algunos administradores de correos electrónicos tienen definido un tamaño específico para los usuarios, de tal manera que no pueden recibir mensajes muy grandes o bien no pueden recibir más información si su buzón ya está lleno.
- Seguridad.- Si los mensajes se mandan sin utilizar algún tipo de encriptación, cualquier persona (*hacker*) puede ver la información de ese correo. Este punto es muy importante, ya que los correos mientras se encuentran en tráfico, pueden ser vistos por cualquier persona que esté buscando cierta información.

Por otra parte, están todos aquellos virus y gusanos que se envían por correo y que llegan a infectar gran número de computadoras en cuestión de minutos.

Correos electrónicos internacionales. Entendiendo por estos correos, aquellos que recibimos sin saber ni siquiera lo que significa el asunto del mensaje, - viene en inglés, francés, etc.-. Desgraciadamente, ante este tipo de correos electrónicos, los recursos contenidos en la normativa estatal de que disponemos no nos amparan en demasía.

Correos electrónicos nacionales. Frente a este tipo de correos que nos inundan, constantemente, la bandeja de entrada de nuestro programa de correo electrónico, cabe apuntar que todos los usuarios estamos amparados por la normatividad del país en que residimos.

En realidad, lo que tenemos aquí es un medio bastante beneficioso, pero que puede llegar a ser perjudicial, si no cuidamos lo que enviamos, como lo enviamos, lo que recibimos y por supuesto lo que abrimos.

Podemos concluir que: Si estamos manejando información sensible, debemos tener medidas precautorias como: contar con encriptación, manejo de llaves públicas y privadas, mandar archivos compactados con clave o cualquier otra medida de seguridad que permita utilizar el correo electrónico de manera segura.

B) MESSENGER.

Es uno de los clientes de mensajería instantánea más usados por Internet, con el que podemos comunicarnos con nuestros amigos de todo el mundo a tiempo real, de múltiples maneras: escribiendo, con *emoticonos*, dibujando, hablando, en video.

MSN Messenger es un programa de comunicaciones que permite:

- Ver si tus amigos están conectados en un momento determinado.
- Enviarles mensajes instantáneos.
- Intercambiar con ellos imágenes y otros archivos.
- Mantener una comunicación simultánea con varias personas a la vez.

- Hablar de viva voz, utilizando un micrófono.
- Mantener comunicaciones con video, utilizando una cámara Web.
- Invitar a otra persona a participar en un juego.

C) HI5.

Al momento de crear o modificar una cuenta de *hi5*, el usuario puede configurar su propia cuenta, llenando los espacios de su información con la del usuario propio para que así toda la red de amigos pueda informarse.

Existen 2 bloques para datos. Uno de ellos cuenta con la información personal del usuario. Por ejemplo: estado civil, edad, religión, idiomas, ciudad natal, buscando. Mientras que el otro bloque de datos es para información personal relacionada con los gustos personales del usuario. Tales como: Acerca de mi, Música favorita, Películas favoritas, Libros favoritos, Programa de TV favoritos, frase.

Todos los usuarios que acceden a una cuenta podrán ver toda la información que se haya registrado. Cabe expresar que el usuario dueño del perfil, puede restringir el acceso al mismo, dejando libre entrada a "amistades" en su "red de amigos".

CARACTERÍSTICAS:

Amigos

La cantidad de amigos que una cuenta de *hi5* puede tener es ilimitada. Por lo general, en esta red la palabra *amigo* no significa otra cosa más que una cuenta asociada a otra, en ocasiones los amigos no se conocen entre sí, pero pueda que se dé el caso de conocerse virtualmente. Además, de poder elegir hasta 15 amigos, como *principales*. Pero se debe tomar en cuenta que el *hi5* no protege al usuario del tipo de amigos que lo contacten, propiciando así que algunos hagan mal uso de éste.

Comentarios

Otro elemento casi esencial del *hi5*. Los comentarios pueden ser de varios tipos:

- En perfil: Los comentarios de perfil (al principio se llamaban "testimonios") aparecen publicados en la página principal de la cuenta del propietario, todos los que visiten su perfil podrán verlos.

Los comentarios en el perfil son por lo general mensajes que describen qué tan buen amigo es. Y como cualquier otro comentario de *hi5*, también pueden ser acompañados con colores, imágenes o videos.

- En fotos: Los comentarios dejados en las fotos suelen hablar del contenido de la foto y van dirigidas al propietario de la foto, todos los usuarios que vean dicha foto podrán ver también todos los comentarios aprobados ahí.

A veces, vienen acompañadas de adornos, tales como: colores, imágenes o hasta videos. Otra característica es poder etiquetar a los amigos que aparecen en cada foto y a uno mismo. Si el amigo etiquetado tiene una cuenta en *hi5*, la etiqueta enlaza a su perfil.

- En el diario: Si el propietario de una cuenta escribe una entrada en su diario, los visitantes pueden dejar sus comentarios en cada entrada, de manera similar a los comentarios en *blogs*.
- *Fives*: Los *fives* son una especie de emoticons permanentes o medallones virtuales con los cuales se puede dedicar como gratificación, recuerdo, diversión o conmemoración a algo.

Ejemplos de *fives*:

- *Cute*: Para dar a alguien atractivo
- *Brother*: Para dar a alguien que consideras tu hermano
- *Birthday*: Para conmemorar su fecha de cumpleaños.
- *Best friend*: Para dar a tu mejor amigo, o uno de tus mejores amigos.

Los *fives* solían entregarse con la compañía un mensaje indicando el porqué de la entrega, sin embargo la nueva versión de *hi5* quitó esta característica.

Visitas.- Este atractivo a diferencia de otros *blogs*, permite ver quien te visitó durante el día y muestra las visitas que has tenido a lo largo de la activación de tu cuenta. Sin embargo, esta característica se puede modificar en privacidad y así las personas no se dan cuenta de si usted la visitó o no.

Like

Nueva aplicación de una empresa de servicios de música en línea: *Like* y *Qloud*. Se pueden añadir videos, artistas y canciones favoritas.

Artículos

Entre éstos se pueden elegir *slideshows* de fotos con música, videos de *YouTube*, fotos con efectos especiales, horóscopos, palabras con *glitter*, juegos y cuentas regresivas.

Aplicaciones

En esta sección, existe una amplia gama de aplicaciones: se puede compartir bebidas con tus amigos favoritos, hacer guiños en las fotos de perfil, añadir *tests*, *supercomentarios*, "*superfives*", *poker*, *grafittis* y demás.

Para importar los contactos, el usuario de la cuenta de *hi5* debe dar el nombre de usuario y la contraseña de su cuenta de *e-mail*. Hasta el día de hoy importa contactos de e-mail por medio de un canal sin cifrado. Esta práctica no es recomendable; ya que cualquiera con un programa de sniffing puede conocer la clave.

D) FACEBOK.

Facebook es un sitio *Web* gratuito de redes sociales creado por *Mark Zuckerberg*. Originalmente era un sitio para estudiantes de la Universidad de Harvard, pero actualmente está abierto a cualquier persona que tenga una cuenta de correo electrónico. Los usuarios pueden participar en una o más redes sociales, en relación con su situación académica, su lugar de trabajo o región geográfica.

Ha recibido mucha atención en la *blogosfera* y en los medios de comunicación al convertirse en una plataforma sobre la que terceros pueden desarrollar aplicaciones y hacer negocio a partir de la red social.

Servicios que ofrece

- Amigos: es una forma de localizar amigos con quienes se perdió el contacto o agregar otros nuevos con quienes intercambiar fotos o mensajes, el servicio de *facebook* te ayuda a buscarlos y también te sugiere otros.
- Grupos y Páginas: es una de las utilidades de mayor desarrollo reciente. Se trata de reunir personas con intereses comunes. En los grupos se pueden añadir fotos, vídeos, mensajes. En cuanto a las páginas, éstas también se crean con fines específicos, solo que no hay foros de discusión y están encaminadas hacia marcas o personajes específicos, más no hacia ningún tipo de convocatoria.

Además, los grupos también tienen su normativa, entre la cual se incluye la prohibición de grupos con temáticas discriminatorias o que inciten al odio y falten al respeto y la honra de las personas. Si bien ésto no se cumple en muchas ocasiones, existe la opción de denunciar y reportar a los grupos que vayan contra esta regla, por lo cual *Facebook* incluye un *link* en cada grupo el cual se dirige hacia un cuadro de reclamos y quejas.

- Muro: el muro (*wall*) es un espacio en cada perfil de usuario que permite que los amigos escriban mensajes para que el usuario los vea. Sólo es visible para usuarios registrados, muro te permite ingresar imágenes y poner cualquier tipo de logo tipos en tu publicación. Una mejora llamada supermuro permite incrustar animaciones flash.
- Fotos: Según *Facebook*, hay:
 - 5 mil millones de fotos de usuario.
 - 160 *terabytes* de almacenaje.

- Regalos: los regalos o *gift* son pequeños íconos con un mensaje. Los regalos dados a un usuario aparecen en la pared con el mensaje del donante, a menos que el donante decida dar el regalo en privado, en cuyo caso el nombre y el mensaje del donante no se exhibe a otros usuarios.

Una opción "anónima" está también disponible, por la que cualquier persona con el acceso del perfil puede ver el regalo, pero solamente el destinatario verá el mensaje.

Algunos regalos son gratuitos y el resto cuestan un dólar, (es necesario un número de tarjeta de crédito o cuenta *Paypa*).

- Juegos: la mayoría de aplicaciones encontradas en *facebook* se relacionan con juegos de rol, trivias (p. ej. geografía), y pruebas de habilidades (digitación, memoria). Entre los más célebres se encuentran los juegos de *Playfish* y los juegos de Zynga Games.

F) MySpace.

MySpace (MySpace.com) es un sitio *Web* de interacción social formado por perfiles personales de usuarios que incluye redes de amigos, grupos, *blogs*, fotos, videos y música, además de una red interna de mensajería que permite comunicarse a unos usuarios con otros y un buscador interno.

2.5 INTIMIDAD INFORMÁTICA.

La informática entendida como medio, constituye indefectiblemente poder, dado que elimina las barreras del espacio y del tiempo y se constituye en un elemento muy útil para el acopio y uso de todo tipo de información.

La informática, unida a las comunicaciones, ofrece un potencial ilimitado de acceso inmediato a la información. Ésta se ha convertido en nuestro recurso más valioso. Nuestra forma de comunicación – ya sea entre particulares, ya frente a la administración-, de utilización del ocio, de adquisición de nuevos conocimientos, y, en general, nuestra forma de vida, está cambiando. Consecuentemente las instituciones

sociales, las reglas de conducta, los medios de enseñanza y nuestro estilo de vida deben adaptarse a estos cambios con el fin de obtener el máximo beneficio posible de la que ya con carácter general se viene denominando <<sociedad de la información>>.

Por tanto, entendemos a la intimidad informática como aquél contenido del derecho a la intimidad que establece la garantía de control y no injerencia sobre los datos relativos a la persona susceptible de tratamiento informático. Ello requiere el conocimiento por parte del individuo de la existencia y características de los bancos de datos que poseen datos a él relativos. De esta forma la extensión del derecho a la intimidad, en un ámbito concreto como la informática, lo que está haciendo es dar solución no a una nueva amenaza, sino a una forma o medio de llevarla a efecto.

El uso de los modernos medios electrónicos, estén en manos de quien estén, contraen el riesgo de injerencia en la intimidad, tiene implícita la posibilidad de lesionar derechos de la personalidad

El derecho a la intimidad informática debe ser considerado como el derecho que tiene todo gobernado de reservar para sí, datos de carácter personal, cuyo acceso solo es permisible a aquellas personas autorizadas por el titular de los mismos, salvo los casos de interés público, así como el derecho que tiene toda persona de acceder a cualquier clase de banco, almacén, contenedor, administrador o archivo de datos que contenga datos personales con el fin de actualizarlos, modificarlos, rectificarlos o retirarlos previos tramites de ley.

Es así entonces, que la intimidad informática, se conforma por aquella información de índole personal, misma que constituye la esencia del titular de la misma, dichos datos se encuentra contenidos en sistemas y equipos informáticos, por eso es que se le ha denominado intimidad informática.

2.6 INFORMÁTICA JURÍDICA.

La informática jurídica es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación.

El derecho de la informática se define como el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática. Es decir, es un conjunto de leyes en cuanto que, si bien escasos, existen varios ordenamientos jurídicos nacionales e internacionales con alusión específica al fenómeno informático.

La herramienta básica de la informática jurídica es:

- El procesador de textos o procesador de palabras, *Word processor* o *Word text*, es un programa o conjunto de programas que se utilizan para escribir y transformar textos en lenguaje natural, los que además pueden presentarse en el momento de su impresión en distintos tipos de letra, con distinta diagramación y pueden ser archivados para ser usados con posterioridad. La idea básica es que uno puede escribir un borrador e irle dando forma como desee, para luego obtener un texto final totalmente acabado y sin errores. La posibilidad de escribir y efectuar la transformación que hemos mencionado, consiste en que se puede escribir e intercambiar o sobreimprimir letras o palabras; borrar todo el texto, o parte de él, ya sea palabras o letras; reacomodar el texto; traer un texto de otro archivo e incorporarlo, etc.

Cada procesador tiene sus ventajas, a medida que se hace más complejo su manejo, requiere más instrucción, pero permiten realizar mayores tareas.

El uso de un procesador nos permitirá pasar a otros, conociendo en gran parte el potencial que tiene el mismo y reconociendo funciones comunes.

La informática jurídica tiene por objeto la aplicación de la tecnología de la información al derecho. Es una disciplina bifronte en la que se entrecruzan una metodología tecnológica con su objeto jurídico que, a su vez, condiciona las propias posibilidades o modalidades de tal aplicación. La informática jurídica estudia el tratamiento automatizado de las fuentes de conocimiento jurídico, a través de:

- a) La informática jurídica documental.- tiene por objeto la automatización de los sistemas de información relativos a las fuentes de conocimiento jurídico: legislación jurisprudencia y doctrina.
- b) Informática jurídica de gestión.- se trata de la realización a través de soportes informáticos o telemáticos de opresiones destinadas a recibir y transmitir comunicaciones de cualquier tipo, de leer y escribir textos; de formar, organizar y actualizar archivos y registros; exigir y recibir pagos; estipular condiciones y controlar su cumplimiento.
- c) Informática jurídica decisional. Se halla integrada por los procedimientos dirigidos a la sustitución o reproducción de las actividades del jurista; a proporcionarle decisiones y dictámenes, es decir, a ofrecerle soluciones de problemas y no mera documentación sobre problemas.

Estos sistemas pueden prestar un importante servicio al abogado al informarle sobre la normativa aplicable sobre determinados supuestos, así como sobre las consecuencias jurídicas derivadas de aplicar dicha normativa a situaciones específicas.

2.7 RIESGOS INFORMÁTICOS.

Es un concepto nuevo en la terminología jurídica sin existir por tanto una definición específica. El riesgo se refiere a la incertidumbre o probabilidad de que ocurra o se realice una eventualidad, la cual puede estar prevista; en este sentido, podemos decir que el riesgo es la contingencia de un daño. En función de lo anterior, podemos aseverar que los riesgos informáticos se refieren a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos, como los equipos informáticos, periféricos, instalaciones, proyectos, programas de cómputo, archivos, información, datos confidenciales.

Cada usuario debe ser advertido de sus responsabilidades en materia de seguridad respecto a sus colegas, equipos y trabajo.

CAPÍTULO TRES

GENERALIDADES DEL DERECHO PENAL APLICADOS AL ESTUDIO DE LA PROTECCIÓN A LA INTIMIDAD

3.1 EL DERECHO EN GENERAL.

La esencia del Derecho en general consiste en lo permanente e invariable de los principios que lo rigen y fundamentan; de modo que la naturaleza de esos principios constituye propiamente la materia de la ciencia jurídica. En el ámbito penal, esa esencia se configura por el análisis y conocimiento de los principios básicos de naturaleza penal.¹⁰

Dentro de ellos se encuentra la propia norma que origina a la ley penal, la que en combinación con otras disposiciones jurídicas del orden civil, administrativo, constitucional, etc., crea o da lugar al estado de Derecho, mediante el cual las sociedades y los individuos pueden convivir.

El Derecho tiene como finalidad encauzar la conducta humana; manifiéstese como un conjunto de normas que rigen la conducta externa de los hombres en sociedad, las cuales pueden imponerse a sus destinatarios mediante el empleo de la fuerza de que dispone el Estado.

3.1.1 DERECHO PENAL.

El Derecho Penal constituye una parte integrante del derecho público, en el que se establecen las relaciones entre el Estado y los particulares, frente a la necesidad de salvaguardar el orden público; concretamente, el delito implica una relación de derecho entre el delincuente y el poder público, cuya misión es perseguirle y castigarle.

¹⁰ LÓPEZ BETANCOURT, Eduardo. INTRODUCCIÓN AL DERECHO PENAL, Editorial PORRÚA, México 2004, Pág. 415.

La expresión Derecho Penal, como certeramente afirma MAGGIORE, se aplica para designar tanto al conjunto de normas penales (ordenamiento jurídico penal), cuanto a la ciencia del Derecho Penal, como una rama del conocimiento humano compuesta de un acervo de nociones jurídicas de naturaleza intelectual.¹¹

RAÚL CARRANCA Y TRUJILLO, señala que, “es el conjunto de leyes mediante las cuales el Estado define los delitos, determina las penas imponibles a los delincuentes y regula la aplicación concreta de las mismas a los caos de incriminación”.¹²

JIMÉNEZ DE ASÚA, al hablar de las características del Derecho Penal manifiesta que éste es un Derecho Público, normativo, valorativo y finalista que tiene la norma y el bien jurídico como polos de su eje y cuya naturaleza es eminentemente sancionadora”.¹³

Es importante mencionar que la finalidad del Estado, al imponer normas, es primordialmente preventiva, más que sancionadora, es decir, al Estado le interesa más que castigar, prevenir el hecho delictivo, mediante la amenaza de ser sancionado en casos de que el autor se coloque en el presupuesto de la norma penal, infringiendo la ley impuesta por el estado.

El Derecho Penal es el reflejo de las normas morales y éticas que hacen posible la vida en sociedad, razón por la cual podemos afirmar que el derecho penal es el reflejo normativo instituido para la protección de aquellos bienes jurídicos que esa sociedad o grupo considera valiosos¹⁴.

Luego entonces el Derecho Penal encuentra en la ley su única forma de expresión y manifestación, lo cual, expuesto en otras palabras significa que la ley es la exclusiva fuente generadora del Derecho Penal, por ello atinadamente JIMÉNEZ DE

¹¹ MAGGIORE. DERECHO PENAL I. Editorial, TEMIS, Bogotá, 1954, Pág. 3

¹² CARRANCA Y TRUJILLO, Raúl. DERECHO PENAL MEXICANO. PARTE GENERAL, TOMO I, 5ª, ED., Editorial, Antigua Librería Robredo, México, 1958, Pág. 17.

¹³ JIMÉNEZ DE ASÚA, Luís. PRINCIPIOS DEL DERECHO PENAL. LA LEY Y EL DELITO, 3ª Edición, Editorial SUDAMERICANA, Buenos Aires, 1990.

¹⁴ ANDRÉS CÁMPOLI, Gabriel. DELITOS INFORMÁTICOS EN LA LEGISLACIÓN MEXICANA, Editorial Instituto Nacional de Ciencias Penales, México 2007. Pág. 28.

ASÚA, sostiene que la Ley Penal”en su sentido formal y más solemne, es la manifestación de la voluntad colectiva expresada mediante los órganos constitucionales, en la que se definen los delitos y se establecen las sanciones.¹⁵

El Derecho Penal forma parte del Derecho Positivo Mexicano; es Derecho vigente. Es de carácter público, porque las sanciones impuestas por el Estado, son en razón de un interés público; el delito crea una relación jurídica entre el sujeto activo del delito y el Estado, en cuanto aquella facultad exclusiva del Estado de determinar los delitos, las penas y las medidas de seguridad.

3.2 ELEMENTOS DEL DELITO.

Para mejor comprensión de este punto, iniciare por indicar la definición de delito, el cual deriva del verbo *delinquere*, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley.

Todo delito nace, como toda acción humana, en la mente del autor. La deliberación puede ser más o menos breve –e incluso faltar- lo que explica que, de concurrir, la (premeditación) constituya una circunstancia de agravación. Pero la resolución, más o menos lúcida, es presupuesto de todo hecho doloso, aunque en la omisión pueda adoptar forma pasiva. Ahora bien: en sí misma la fase interna no puede ser objeto de castigo por el Derecho, sino sólo en cuanto se traduzca en una fase externa, en ciertas condiciones.

Los elementos del delito según AMUCHATEGUI REQUENA, Son los aspectos positivos, a cada uno de los cuales corresponde uno negativo, que llega a ser la negación de aquel; significa que anula o deja sin existencia al positivo y, por tanto, al delito.¹⁶

¹⁵ JIMÉNEZ DE ASÚA, Luís. PRINCIPIOS DEL DERECHO PENAL. LA LEY Y EL DELITO, 3ª Edición, Editorial SUDAMERICANA, Buenos Aires, 1990.

¹⁶ AMUCHATEGUI REQUENA, Irma Griselda. DERECHO PENAL (CURSOS PRIMERO Y SEGUNDO). Editorial HARLA, México, 1993. Pág. 418.

ELEMENTOS POSITIVOS

Conducta

Tipicidad

Antijuridicidad

Culpabilidad

Imputabilidad

Punibilidad

ELEMENTOS NEGATIVOS

Ausencia de conducta

Atipicidad

Causas de justificación

Inculpabilidad

Inimputabilidad

Excusas absolutorias

En este apartado solo cabe abordar los elementos positivos, ya que en el delito de violaciones a la intimidad, existe toda la intención del individuo de delinquir, toda vez que cuenta con los conocimientos esenciales de la informática, permitiéndole acceder a datos que ningún otro sujeto puede obtener, no obstante el tema a desarrollar requiere especificar algunos elementos negativos del delito para una mayor amplitud y comprensión.

Actualmente existe la noción de “profesión del crimen”; se trata de desarrollar el comportamiento como una profesión, incluso el sujeto trata de perfeccionarse y llega a especializarse, como lo es en la comisión de algunos delitos patrimoniales, delitos en materia internacional, delitos de cuello blanco, etc. Para su ejercicio, se requiere una capacidad intelectual superior a la común, además de toda una organización.

Por el tipo de delitos de que se trata, se deben excluir específicamente del campo de estudio a los demás inimputables, ya que por el grado de especialización técnica que requieren estos actos, resultaría poco menos que imposible que un demente o débil mental pudiese resultar involucrado en este tipo de actividades.

Sin embargo cabe hacer hincapié en que los menores de edad son considerados por el Derecho Penal como sujetos inimputables, considerados como carentes de aptitud psicológica para la delictuosidad, pero en mi particular punto de vista considero que los individuos a que hago alusión si pueden cometer conductas antisociales y pueden llegar a comprender el grado de afectación al infringir la ley, tal y como lo indicare en el punto respectivo del siguiente capítulo.

3.2.1 CONDUCTA Y ACCIÓN.

Entendemos por conducta, el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito.

En la actualidad es unánime el pensamiento en el sentido de que sólo las personas físicas pueden delinquir, más está en pie que hoy se cometen delitos mediante las computadoras como instrumento, convirtiéndose en un individuo ante la vista e interpretación de los demás, por el hecho de tomar una personalidad mediante una red, comúnmente denominada Internet, en el cual se hace conocer ante su víctima como un sujeto, hasta en ocasiones se asigna nombre para delinquir, pero es así que en términos reales, dicha herramienta es manipulada por un ser humano, ya que la computadora no puede efectuar sus funciones sin la ayuda o intervención del hombre.

La acción consiste en actuar o hacer; es un hecho positivo, el cual implica que el agente lleve a cabo uno o varios movimientos corporales, y comete la infracción a la ley por sí mismo o por medio de instrumentos, animales, mecanismos e incluso mediante personas.

Según CUELLO CALÓN, la acción, en sentido estricto, es el movimiento corporal voluntario encaminado a la producción de un resultado consistente en la modificación del mundo exterior o en el peligro de que se produzca.¹⁷

¹⁷ CUELLO CALÓN .DERECHO PENAL. TOMO I, 8ª Edición, Barcelona 1947

3.2.1.1 AUSENCIA DE CONDUCTA

Es pues, la ausencia de conducta uno de los aspectos negativos, o mejor dicho, impositivos de la formación de la figura delictiva, por ser la actuación humana, positiva o negativa, la base indispensable del delito como todo problema jurídico.¹⁸

Cualquier causa capaz de eliminar la conducta, que es el elemento básico del delito, impedirá la integración de éste.

3.2.2 TIPLICIDAD.

Es la adecuación de la conducta al tipo penal o sea, el encuadramiento de un comportamiento real a la hipótesis legal.

Dentro de esta figura encontramos el dolo y la culpa:

- Dolo. Cuando el sujeto comete el delito con la intención de realizarlo. Se tiene la voluntad y el dolo de infringir la ley.
- Culpa. El delito se comete sin la intención de cometerlo; ocurre debido a negligencia, falta de cuidado, imprevisión, imprudencia, etc.

La tipicidad es el encuadramiento de una conducta con la descripción hecha en la ley; la coincidencia del comportamiento con el descrito por el legislador.

Su función es predominantemente descriptiva.

- TIPO: Descripción de la acción prohibida.

¹⁸ CASTELLANOS, Fernando. LINEAMIENTOS ELEMENTALES DE DERECHO PENAL. Editorial PORRÚA, México, 2009, Pág. 363.

La tipicidad es la razón de ser de la antijuridicidad; el legislador crea las figuras penales por considerar antijurídicos los comportamientos en ellas descritos.

Adecuación de la acción (u omisión) al tipo.

La acción humana se caracteriza por tener siempre una finalidad, voluntad dirigida a un fin.

3.2.2.1 ATIPICIDAD

Es la ausencia de adecuación de la conducta al tipo. Si la conducta no es típica, jamás podrá ser delictuosa.

Las causas de atipicidad pueden reducirse a las siguientes:

- a) Ausencia de la calidad o del número exigido por la ley en cuanto a los sujetos activos y pasivo;
- b) Si faltan el objeto material o el objeto jurídico;
- c) Cuando no se dan las referencias temporales o espaciales requeridas en el tipo;
- d) Al no realizarse el hecho por los medios comisivos específicamente señalados en la ley;
- e) Si faltan los elementos subjetivos del injusto legalmente exigidos;
- f) Por no darse, en su caso, la antijuridicidad especial.

Lo que ocurre muy comúnmente en los delitos informáticos y más en las violaciones a la intimidad es que, estas conductas delictivas no pueden ser castigadas porque no se adecuan a los ordenamientos legales establecidos, por lo tanto quedan impunes.

3.2.3 ANTIJURIDICIDAD.

Supone que la conducta que se ha realizado está prohibida por el ordenamiento jurídico; en otras palabras, que dicho comportamiento es contrario a Derecho.

La antijuridicidad radica en la violación del valor o bien protegido a que se contrae el tipo penal respectivo.

No se vulnera la ley, se infringe la norma.

El acto será formalmente antijurídico cuando implique transgresión a una norma establecida por el Estado (oposición a la ley) y materialmente antijurídico en cuanto signifique contradicción a los intereses colectivos.

3.2.3.1 CAUSAS DE JUSTIFICACIÓN

a) Legítima defensa.- Para CUELLO CALÒN, es legítima defensa necesaria para rechazar una agresión actual o inminente e injusta, mediante un acto que lesione bienes jurídicos del agresor.¹⁹

b) Estado de necesidad.- es una situación de peligro para un bien jurídico, que sólo puede salvarse mediante la violación de otro bien jurídico.

c) Cumplimiento de un deber, ejercicio de un derecho, impedimento legítimo y consentimiento del interesado.

3.2.4 CULPABILIDAD.

Es la relación directa que existe entre la voluntad y el conocimiento del hecho con la conducta realizada. Reproche penal; grados: dolo y culpa.

Es la relación directa que existe entre la voluntad y el conocimiento del hecho con la conducta realizada.

¹⁹ CUELLO CALÓN. DERECHO PENAL, I, 8ª Edición , BARCELONA 1947, Pág. 341

- Dolo.- consiste en causar intencionalmente el resultado típico, con conocimiento y conciencia de la antijuridicidad del hecho.
- Culpabilidad.- ocurre cuando se causa un resultado típico sin intención de producirlo, pero se ocasiona solo por imprudencia o falta de cuidado o de precaución, debiendo ser previsible y evitable. La doctrina le llama delito culposo, imprudencial o no intencional.

3.2.4.1 INCULPABILIDAD

Es la ausencia de culpabilidad, ésta opera al hallarse ausentes los elementos esenciales de la culpabilidad: conocimiento y voluntad.

3.2.5 IMPUTABILIDAD.

La imputabilidad implica salud mental, aptitud psíquica de actuar en el ámbito penal, precisamente al cometer el delito. Por otra parte dice la autora AMUCHATEGUI REQUENA, El sujeto primero tiene que ser imputable para luego ser culpable; así, no puede haber culpabilidad si previamente no se es imputable.²⁰

Debemos considerar la imputabilidad como la aptitud legal para ser sujeto de aplicación de las disposiciones penales y, en consecuencia, como capacidad jurídica de entender y querer en el campo del derecho.

3.2.5.1 INIMPUTABILIDAD

Las causas de inimputabilidad son, pues, todas aquellas capaces de anular o neutralizar, ya sea el desarrollo o la salud de la mente, en cuyo caso el sujeto carece de aptitud psicológica para la delictuosidad.

²⁰ AMUCHATEGUI REQUENA, Irma Griselda. DERECHO PENAL (CURSOS PRIMERO Y SEGUNDO). Editorial HARLA, México, 1993. Pág. 418.

3.2.6 PUNIBILIDAD.

Es la amenaza de una pena que contempla la ley para aplicarse cuando se viole la norma. Así como la imputabilidad es un presupuesto de la culpabilidad, la punibilidad es una consecuencia de esta última.

3.3 BREVE ESTUDIO DOGMÁTICO DEL DELITO DE VIOLACIONES A LA INTIMIDAD.

Si bien es cierto en la actual legislación mexicana aún no se contempla este delito en forma específica, sin embargo he realizado un breve análisis de la estructura dogmática de las violaciones a la intimidad para una mejor comprensión del tema, haciendo la descripción siguiente:

NATURALEZA JURÍDICA

La naturaleza jurídica del delito de violaciones a la intimidad en su aspecto informático consiste en amparar, como bien jurídicamente tutelado por la norma la información íntima, ya que son datos sensibles y cualquier conocimiento o divulgación no autorizada produce necesariamente un daño, al menos moral, en el sujeto pasivo.

CLASIFICACIÓN DEL DELITO

- a) en función de su gravedad

La intromisión y divulgación de datos que corresponden al ámbito psicológico e inconmensurable del individuo es un delito, por que viola el pacto social hecho por los hombres para vivir en sociedad, dañando el bien jurídico protegido, la información

íntima y además, será perseguido por el representante social: ministerio público y juzgado por el poder judicial, quien impondrá en su caso la sanción que menciona las leyes penales.

b) según la conducta del agente

De acción. Este delito para su realización requiere movimientos corporales, materiales y el uso de conocimientos en informática, en ocasiones solo se necesita una noción en el manejo de computadoras e Internet.

c) por el resultado

Inmaterial: es inminentemente inmaterial, ya que en su efectuación ocasionará un resultado interior, el cual será un daño moral en la víctima.

d) por el daño que causa

De lesión: considero al ilícito de revelación de datos sensibles que constituyen la esencia del individuo, de lesión, por que daña el bien jurídico tutelado, amparado por la norma, el cual es la información íntima de las personas.

e) por su duración

1. Instantáneo.- según los casos previstos en los artículos 210, 211 y 211 Bis del Código Penal Federal, son delitos instantáneos, a virtud de que se consuman en un solo movimiento y en ese momento se perfeccionan. Por ejemplo cuando el agente accede a información íntima de una persona, mientras que el titular se encuentra fuera de su área personal o de trabajo según sea el lugar en el que haga uso de su información, asimismo el sujeto activo aprovecha ese momento para divulgar o utilizar tales datos.

2.- permanente.- podría aparecer de manera permanente, es decir, prolongándose su efecto negativo a través del tiempo, en los casos en que el agente o sujeto activo descargue la información de la base de datos del equipo informático del titular, para utilizarla en el momento que desee negándose a entregar los datos sustraídos; hasta que no la entregue cesa la conducta delictiva.

f) por el elemento interno

Doloso.- se presenta en forma dolosa, a virtud de que se precisa de la plena voluntad del agente para cometer el delito de revelación de secretos e información íntima. La naturaleza de este delito es dolosa, de tal suerte, sería sumamente difícil que se presentara culposamente, de acuerdo a nuestra legislación es inaceptable, porque se requiere la plena intención de que con perjuicio de alguien, el agente disponga para sí o para otro de cualquier información de la cual no se tenga autorización de su conocimiento.

g) por su estructura

Simple.- el delito de revelación de secretos e información íntima, es simple por que causa una sola lesión jurídica a la intimidad de la persona.

h) por el número de actos

Unisubsistente.- porque es suficiente un sólo acto para cometer este.

i) por el número de sujetos

Unisubjetivo.- el delito de revelación de secretos y acceso ilícito a sistemas y equipos de informática, como lo establece el tipo penal, se colma con la participación de una sola persona.

j) por su forma de persecución

De querrela.- por que para su persecución se requiere la petición de la parte ofendida.

k) en función de su materia. Federal y común

El delito de revelación de secretos e información íntima es federal porque se encuentra contenido en un ordenamiento de tipo federal: código penal federal.

l) clasificación legal

El delito que estoy analizando se encuentra contenido en el Título Noveno Revelación de Secretos y Acceso ilícito a sistemas y Equipos de Informática, capítulo I Revelación de Secretos, artículos 210, 211 y 211 Bis del Código Penal Federal.

3.4 LA TENTATIVA.

Una definición que nos da al respecto Jiménez de Asúa es que la tentativa “es la ejecución incompleta de un delito”.²¹

La tentativa es un grado en la vida del delito y de hecho se convierte en un delito imperfecto.

La tentativa aparece cuando el sujeto ha realizado todos los actos encaminados para la consumación del delito, y éste no se presenta por causas ajenas a la voluntad de dicho sujeto.

Tiene un inicio, un comienzo en la ejecución, donde se utilizan actos idóneos; pero en el transcurso de los actos necesarios o al final de los mismos, el resultado deseado no llega a presentarse.

El fundamento objetivo de la tentativa se encuentra en la decisión del sujeto de actuar dolosamente para afectar el orden público.

²¹ JIMÉNEZ DE ASÚA, Luís, LA LEY Y EL DELITO, Editorial. HERMES, México, 1986, p. 474.

MAGGIORE define la tentativa como “un delito iniciado y no cumplido por interrupción de la acción o por la irrealización del resultado”.²² Además, establece con base en esta definición que los elementos de la tentativa son tres:

- I) La intención dirigida a cometer un delito;
- II) Un acto idóneo, y
- III) Una acción no realizada o un resultado no verificado.

La tentativa acabada se entiende como aquella ejecución completa de la conducta realizada por el activo encaminada hacia un resultado delictivo, pero éste no aconteció por causas ajenas a la voluntad.

La tentativa inacabada consiste en la omisión del agente de uno o varios actos tendientes a la verificación del delito.

Los tipos penales cuya composición admiten la figura de la tentativa, son punibles cuando de acuerdo con su desarrollo ejecutivo causal se persigue una determinada finalidad, que no obstante al verse suspendida por motivos externos a la voluntad del autor, se deteriora o pone en riesgo el bien jurídico protegido, causando una perturbación grave del orden social.

Podemos afirmar que la tentativa es la ejecución de un delito que se suspende en cualquier punto de desarrollo objetivo, antes de alcanzar su consumación, por causas ajenas a la voluntad del autor.

Respecto a la tentativa en los delitos informáticos en general, podría no tener cavidad, sin embargo considero que se debe hacer referencia, ya que hay millones de personas en el ciberespacio que tienen la plena la voluntad de cometer una conducta ilícita a través de Internet y que propiamente lo hacen, pero en ocasiones fallan sus conocimientos en informática ocasionando que no puedan concluir con la conducta ilícita que tenían en mente, poniendo en peligro la integridad física, mental, psicológica o patrimonial de las personas que son atacadas

²² MAGGIORE, Guiseppe, DERECHO PENAL, VOL. II, Editorial. TEMIS, bogota, 1989,p.77

3.5 LA CONSUMACIÓN.

La consumación del delito no es otra cosa que la acción o la omisión plena y totalmente realizada y penalmente castigada y “todos los grados del delito se distinguen del delito consumado por la falta de realización del resultado externo descrito por la ley”

El delito consumado requiere una sucesión de pasos graduales, que son relevantes para el derecho penal, que es cuando se logra completar la acción descrita en el tipo, con todos sus efectos. En consecuencia, la ejecución del delito puede recorrer distintos grados, es decir, desarrollarse por medio de distintos pasos que al completar el fin determinado por su autor, alcanza plenitud típica.

Según el tiempo que tarde su consumación, el delito puede ser:

- “I. Instantáneo, cuando la consumación se agota en el mismo momento en que se han realizado todos sus elementos constitutivos;
- II. Permanente o continuo, cuando la consumación se prolonga en el tiempo, y
- III. Continuado, cuando con unidad de propósito delictivo, pluralidad de conductas y unidad de sujeto pasivo, se viola el mismo precepto legal.”

Ahora bien, una vez que he descrito lo básico del derecho penal y lo que es propiamente el delito consumado, ya puedo hacer referencia al contenido de la conducta ilícita que constituye la intromisión de sujetos conocidos como delincuentes informáticos a la intimidad de una persona que hace uso de la Internet mediante equipos informáticos, tal y como describiré en los capítulos siguientes.

CAPÍTULO CUARTO

LOS DELINCUENTES INFORMÁTICOS Y SU TRASCENDENCIA EN EL ÁMBITO INTERNACIONAL

4.1 CONCEPTO DE DELITO Y DELINCUENTE.

En la antigüedad se pensaba que el delito nacía de los defectos físicos y mentales y que era el producto de los rasgos hereditarios. Pero no hay que preocuparse, puesto que tales afirmaciones hoy en día no son tomadas como positivas sino más bien son rechazadas. Se ha llegado hoy a la conclusión de que el delito se aprende y no se hereda.

Delito, es el acto u omisión constitutivo de una infracción de la ley penal.

Delincuente, es la persona física que lleva a cabo la conducta delictiva, autor de uno o varios delitos.

4.2 LOS DELINCUENTES INFORMÁTICOS.

Se les denomina sujetos activos a quienes tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicas donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Es la persona o grupo de personas que en forma asociada realizan actividades ilegales haciendo uso de las computadoras y en agravio de terceros, en forma local o a través de Internet.

A) EL HACKER.

El *Hacker* es una persona con amplios conocimientos en tecnología, bien puede ser informática, electrónica o comunicaciones, mantiene permanentemente actualizado

y conoce a fondo todo lo relacionado con programación y sistemas complejos; es un investigador nato que se inclina ante todo por conocer lo relacionado con cadenas de datos encriptados y las posibilidades de acceder a cualquier tipo de "información segura".

Su formación y las habilidades que poseen les dan una experticia mayor que les permite acceder a sistemas de información seguros, sin ser descubiertos, y también les da la posibilidad de difundir sus conocimientos para que las demás personas se enteren de cómo es que realmente funciona la tecnología y conozcan las debilidades de sus propios sistemas de información.

Este grupo está conformado por adolescentes y adultos, en su mayoría estudiantes de informática, con una característica común: Las ansias de conocimientos.

Individuo que sin derecho penetra un sistema informático sólo por gusto o para probar sus habilidades. Usualmente no tiene fines delictivos graves este tipo de intrusión.

B) EL CRACKER.

Derivado del *hacking*. Persona que sin derecho penetra un sistema informático con el fin de robar o destruir información valiosa, realizar transacciones ilícitas, o impedir el buen funcionamiento de redes informáticas o computadoras. Alguien que viola la seguridad en un sistema. Este término fue acuñado por los *hackers* para defenderse del mal uso periodístico del término "*hacker*". El término "*cracker*" refleja la gran repulsión a los actos de robo y vandalismo perpetrados por los círculos de criminales conocidos como *crackers*.

Obviamente que antes que llegar a ser un *cracker* se debe ser un buen hacker. Asimismo se debe mencionar que no todos los hackers se convierten en crackers.

Un *cracker* es un hábil conocedor de programación de Software y Hardware; diseña y fabrica programas de guerra y hardware para reventar software y

comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos.

C) OTROS.

EL PHREAKER

El *phreaker* es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello.

Se caracterizan por poseer bastos conocimientos en el área de telefonía terrestre y móvil, incluso más que los propios técnicos de las compañías telefónicas; recientemente con el auge de los celulares, han tenido que ingresar también al mundo de la informática y del procesamiento de datos.

Su actividad está centrada en romper las seguridades de las centrales telefónicas, desactivando los contadores con el fin de realizar llamadas sin ningún costo.

Actualmente las tarjetas prepago son su campo de acción predilecto, suelen operar desde cabinas telefónicas o móviles y a través de ellas pueden captar los números de abonado en el aire y así crear clones de tarjetas telefónicas a distancia.

EL LAMMER

A este grupo pertenecen aquellas personas deseosas de alcanzar el nivel de un hacker pero su poca formación y sus conocimientos les impiden realizar este sueño. Su trabajo se reduce a ejecutar programas creados por otros, a bajar, en forma indiscriminada, cualquier tipo de programa publicado en la red.

Es el más numeroso que existe en la red; sus más frecuentes ataques se caracterizan por bombardear permanentemente el correo electrónico para colapsar los sistemas; emplear de forma habitual programas *sniffers* para controlar la red, interceptar contraseñas y correos electrónicos, y después enviar mensajes con direcciones falsas, en muchas ocasiones, amenazando el sistema, lo que en realidad no es cierto, su alcance no va mucho más allá de poseer el control completo del disco duro, aun cuando el ordenador esté apagado.

También emplean los *Back Oriffice*, *Netbus* o virus con el fin de fastidiar, sin dimensionar las consecuencias de sus actos, su única preocupación es su satisfacción personal.

EL COPYHACKER

Son una nueva generación de falsificadores dedicados al *crackeo* de *Hardware*, específicamente en el sector de tarjetas inteligentes. Su estrategia radica en establecer amistad con los verdaderos *Hackers*, para copiarles los métodos de ruptura y después venderlos a los "bucaneros" personajes que serán descritos más adelante.

Los *Copyhackers* se interesan por poseer conocimientos de tecnología, son aficionados a las revistas técnicas y a leer todo lo que hay en la red, su principal motivación es el dinero.

BUCANEROS.

Son los comerciantes de la red más no existen en ella; aunque no poseen ningún tipo de formación en el área de los sistemas, si poseen un amplio conocimiento en área de los negocios.

Su objetivo está centrado en comercializar o revender los productos que los *Copyhackers* les proporcionan, bajo un nuevo nombre comercial, con el ánimo de lucrarse en corto tiempo y con el más mínimo esfuerzo.

NEWBIE

Es el típico "cacharrero" de la red, sin proponérselo tropieza con una página de *Hacking* y descubre que en ella existen áreas de descarga de buenos programas de *Hackeo*, baja todo lo que puede y empieza a trabajar con ellos.

Es un aprendiz paciente e inofensivo, en su trasegar por la red, se puede topar con sistemas de fácil acceso y también con programas con un grado de dificultad mayor, para lo cual tiene que recurrir nuevamente a la red en busca de instrucciones que le permitan lograr su objetivo.

SCRIPT KIDDIE

Denominados también "*Skid kiddie*", son simples usuarios de Internet, sin conocimientos sobre *Hack* o *Crack* aunque aficionados a estos temas no los comprenden realmente, simplemente son internautas que se limitan a recopilar información de la red y a buscar programas que luego ejecutan sin los más mínimos conocimientos, infectando en algunos casos de virus a sus propios equipos.

4.3 LA IMPORTANCIA DE UNA REGULACIÓN JURÍDICA RESPECTO AL FLUJO INTERNACIONAL DE INFORMACIÓN Y DATOS PERSONALES POR INTERNET.

El flujo de datos transfronterizos es la circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y recuperación.

Este problema se refiere a la eventual limitación o favorecimientos de la circulación de datos a través de las fronteras nacionales dependiendo de los beneficios o afectaciones que ello pueda traer aparejado a los diferentes países.

En cuanto a los orígenes del problema, éste se desprende de la amalgama surgida entre la informática y las telecomunicaciones, de ahí el vocablo *teleinformática* o *telemática*, esta última es la fusión entre la informática y las telecomunicaciones para emitir y recibir información de todo tipo.

La información es un bien inmaterial pero constitutivo de un producto autónomo que por su mismo contenido económico requiere de tutela jurídica debido a los derechos y obligaciones que engendra, ya sea a nivel de una relación de posesión entre autor y objeto o a nivel de transferencia entre aquel que la emite y aquel que la recibe, pertenece originalmente al autor, es decir, aquel que la pone a disponibilidad de los diferentes fines de que pueda ser objeto y que por esto mismo permite concebir una relación de posesión entre autor e información a manera de un verdadero derecho real.

Las computadoras, al permitir un manejo rápido y eficiente de grandes volúmenes de información, facilitan la concentración automática de datos referidos a las personas, constituyéndose así en un verdadero factor de poder.

En Internet cambia para el Derecho la noción de tiempo y de espacio, porque es posible realizar enlaces inmediatos a tiempo real sin importar el lugar del mundo donde se encuentren las personas.

La información o redes pueden ser motivo de ilícitos, ya sea como medios o como objetivos, por lo que una consideración internacional en términos penales limitaría dichas acciones, ya no en forma correctiva sino también preventiva.

De un modo u otro todos presentan esta paradoja de un espacio no territorial, no geográfico, que por su sola existencia genera interrogantes y problemas al mundo legal conocido, fuertemente atado a lo geográfico por las soberanías.

Esta red, por medio de proveedores de servicios de Internet, conecta a los usuarios entre sí, y aún cuando no existe un gobierno ni autoridad central como los conocemos, existen agencias internacionales de gobierno de Internet que establecen estándares y habilitan el sistema para que funcione (Internet Society, ICANN, WIPO y otros), pero el acatamiento de sus disposiciones es voluntario y depende de la posición que se adopte frente a los principios de autogobierno de Internet.

Las fronteras no existen en Internet y los Estados tienen serias dificultades para delimitar sus jurisdicciones. Algunos intentan regular esto de manera unilateral, sin contar con la anuencia de los demás Estados, sobre cualquier asunto que sucede en su territorio.

Es que Internet avanza de manera muy rápida y cuando se aprueba una ley, la tecnología ya ha cambiado.

Este derecho unificado de Internet generado a partir de la decisión de las Cortes tendría la característica de ser un derecho de sujeto específico y no de lugar específico, como el derecho tradicional local o geográfico.

El envío de informaciones a otro país, en el estado actual de Derecho, les permite escapar a la reglamentación a que eventualmente pudieran estar sometidas en el país de origen. De aquí se pueden derivar atentados graves a las garantías de los ciudadanos o aún a la seguridad de los Estados, lo cual amerita sin duda una solución jurídica.

4.4 EL HABEAS DATA.

Antes de hablar del Habeas Data hablemos un poco de la figura en la que se basa esta institución, a saber, El Habeas corpus.

Es una figura jurídica que encuentra su origen en el Derecho Inglés; el *habeas corpus* tiene como finalidad la libertad personal de los individuos. Esta institución se

debe a la reacción de los sujetos pasivos de abusos a su libertad por parte de personas que no eran autoridad judicial, es decir, por parte de la corona y otros. Los monarcas eran arbitrarios y ordenaban privación de la libertad y ésta se llevaba a cabo sin orden judicial alguno.

El *habeas corpus* ha tenido un gran desarrollo en países como Inglaterra y Estados Unidos, aunque consta en un cuerpo legal muy antiguo (1679 en Inglaterra), tiene su fundamento en la jurisprudencia y costumbre de estos países y tiene una gran fuerza jurídica por el sistema de Derecho anglosajón, un Derecho consuetudinario.

En pocas palabras podemos definir al *habeas corpus* como una institución jurídica destinada a proteger la libertad personal de las personas. De la misma manera que nacemos con la libertad física, tenemos la libertad de disponer libremente sobre la información que nos pertenece, como los sentimientos, las ideas y en general todo lo que nuestra imaginación y cultura nos permite crear.

El *habeas data* puede ser concebido como un derecho que nos protege de las personas que se dedican a acceder a registros o bancos de datos y de esta forma conocer los datos personales que han sido almacenados y darles diferentes utilidades, comerciales, políticos y personales principalmente.

El *habeas data* garantiza la vida privada de una persona, que nadie viole las áreas de actividad de una persona no destinadas a ser difundidas, sin su consentimiento. También ampara la intimidad ante las autoridades, las que solo podrán acceder a la información privada cuando ésta ponga en peligro la seguridad de la nación o exista el peligro de un bien jurídico superior si determinada información no es revelada.

Al realizar un estudio acerca de esta figura, no intentamos solo justificar y fomentar el estudio del derecho a la intimidad, sino queremos informar acerca del manejo de la información por parte de personas públicas y privadas sin previa autorización de los titulares de tales datos. La manipulación de nuestros datos, sin permiso, se ha vuelto una práctica normal en la sociedad, pensamos que ésto se debe a la omisión de cuidar nuestra intimidad o lo que es lo mismo, no hemos puesto

barreras limitativas a las personas que se encargan de manejar datos que nos pertenecen.

El principal factor de creación del *habeas data* consideramos que ha sido el cambio radical que ha impuesto en nuestras vidas la Informática y demás herramientas tecnológicas de punta. Cabe hacer la aclaración de que el *habeas data* no sólo protege la intimidad del hombre, sino también la verdad e identidad de los datos del individuo que han sido registrados.

El rol de *habeas data* es evitar que los datos que libremente se facilitan para que sean incluidos en un fichero sean trasladados sin consentimiento del titular a otros bancos de datos. Puesto que la información personal no por el hecho de que la información de la intimidad personal tenga un valor económico deja de tener fundamentalmente valores personales éticos. La formación personal es parte de la intimidad individual, para decidir dentro de cierto límite, cuándo y qué información puede ser objeto de procesamiento automatizado. La protección del derecho a la intimidad contra el uso de un tratamiento automatizado de datos no se plantea exclusivamente como consecuencia de problemas individuales sino que también expresan conflictos que incluyen a toda la comunidad, tanto nacional como internacional. La idea de la persona titular de datos, el afectado es quien tiene el interés como parte de un grupo, en controlar el tratamiento automatizado de datos.

De lo anteriormente expuesto resulta que el *habeas data* protege un "*complejo de derechos personalísimos*", que incluyen la privacidad y la identidad, relacionados a su vez con la imagen y con los conceptos de verdad e igualdad; sin embargo, el sentido que quiero darle al *habeas data* en la presente investigación, es que su propósito se dirige a proteger los datos íntimos de una persona, con el fin de evitar lesiones morales que atentan contra la integridad humana de las personas.

El *habeas data* constituye un cause procesal para salvaguardar la libertad de la persona en la esfera informática, que cumple una función paralela, en el seno de los derechos humanos de la tercera generación, a la que en los de la primera generación

correspondió al *habeas corpus* respecto a la libertad física o de movimientos de la persona.

Al cotejar el *habeas corpus* y el *habeas data*, se comprueba una inicial coincidencia en lo referente a su naturaleza jurídica. En ambos casos no se trata de derechos fundamentales, *stricto sensu*, sino de instrumentos o garantías procesales de defensa de los derechos a la libertad personal, en el caso del *habeas corpus*, y de la libertad informática en lo concerniente al *habeas data*. El *habeas corpus* y el *habeas data* representan, además, dos garantías procesales de aspectos diferentes de la libertad. Así, mientras el primero se circunscribe a la dimensión física y externa de la libertad, el segundo se extiende a proteger prioritariamente aspectos internos en la libertad: la identidad de la persona, su autodeterminación, su intimidad.

4.5 CONVENIOS INTERNACIONALES.

Un país, por libre y soberano que se autoproclame, no puede vivir fuera del contexto y de la interrelación jurídica universal. El crimen internacional y los delitos llamados *ius gentium*, bastan para llamar la atención hacia un objeto de conocimiento dentro de un proceso. Es en atención a esto que surge la cooperación judicial internacional regulada, en gran medida a través de las convenciones o tratados internacionales, sean éstos bilaterales o multilaterales.

Ahora bien respecto al tema que me ocupa el Derecho Internacional está inmensamente vinculado con el Derecho Mexicano, ya que con los avances tecnológicos que han invadido la actual sociedad, las legisladores se han visto en la necesidad de regular nuevas conductas delictivas que son cometidas por el uso indebido de equipos informáticos, que no sólo trascienden en el ámbito nacional, sino también en el internacional, lo anterior conlleva una cooperación con otros Estados y países, toda vez que el Internet es una red muy amplia que no mide fronteras, por lo tanto al aplicar las normas sancionadoras referentes a delitos informáticos, se ve en un

gran dilema, ya que los sujetos que cometen este tipo de delitos pueden tener su ubicación en otro país que no es en el que se llevo a efecto la acción ilícita.

Actualmente se tiene conocimiento del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, mismo que fue adoptado por el comité de ministerios del consejo de Europa en septiembre de 1980 y quedó abierto a la firma de los estados miembros a partir del 28 de enero de 1981.

En nuestros días, son carentes los tratados internacionales que hacen hincapié a la cooperación jurídica en caso de delitos informáticos que involucran la intervención de otros Estados ya sea nacionales e internacionales, motivo por el cual en el presente trabajo hago de manifiesto la importancia en la creación de nuevos convenios internacionales, que fijen como un objetivo primordial la cooperación entre Estados, con el fin de que se apliquen normas compatibles y así lograr combatir este tipo de delitos.

CAPÍTULO QUINTO

EL PROCEDIMIENTO PENAL MEXICANO Y LAS FIGURAS JURÍDICAS VINCULADAS EN LA COMISIÓN DE VIOLACIONES A LA INTIMIDAD MEDIANTE EL USO INDEBIDO DE EQUIPOS INFORMÁTICOS

5.1 GENERALIDADES DEL PROCEDIMIENTO PENAL.

Una vez que, en los capítulos anteriores han quedado ya especificados los elementos que constituyen un delito, puedo iniciar con el análisis del procedimiento penal, mismo que se encuentra definido como “el conjunto de actividades reglamentadas por preceptos previamente establecidos, que tienen por objeto determinar qué hechos pueden ser calificados como delito para, en su caso, aplicar la sanción correspondiente”.²³

Todo procedimiento penal inicia cuando el sujeto pasivo o la víctima, acude ante el Ministerio Público o autoridad investigadora para hacer del conocimiento de ésta, una agresión, ya sea, física, patrimonial o psicológica, a dicha manifestación se le denomina denuncia, tal y como lo describe el autor DE PINA VARA, en su definición que hace de la palabra denuncia, siendo ésta, el acto mediante el cual se pone en conocimiento de la autoridad la comisión de algún delito o infracción penal.²⁴

Una vez que se tiene conocimiento de un hecho que puede ser delictuoso, lo primero que procede es que la autoridad investigadora averigüe y reúna los elementos que son necesarios para poder acudir al órgano jurisdiccional en solicitud de aplicación de la ley al asunto en concreto. El órgano jurisdiccional a quien le han sido consignados los hechos, busca si en el caso de su atención, puede haber elementos que justifiquen el proceso, es decir, si puede comprobarse la existencia de un delito y si hay datos que hagan probable la responsabilidad de un sujeto. Sin estos efectos, el órgano

²³ RIVERA SILVA, Manuel. EL PROCEDIMIENTO PENAL. Editorial PORRÚA, México, 2007, Pág. 397.

²⁴ DE PINA VARA, Rafael. DICCIONARIO DE DERECHO. Editorial PORRÚA, México, 2004, Pág. 223.

jurisdiccional no tiene por que continuar ocupándose del asunto, ya que no hay base para que realice actividades y sin dicha base sería ocioso el desarrollo de sus funciones. Si el órgano jurisdiccional encuentra que hay base para el proceso, inicia éste y después de que las partes aportan los medios probatorios que estimen pertinentes para la ilustración del órgano jurisdiccional, y fijan su parecer tomando en consideración dichas pruebas, se aplica el derecho.

Primer periodo. De preparación de la acción procesal. Este primer periodo se inicia con la averiguación previa y termina con la consignación. En otros términos: principia con el acto en el que la autoridad investigadora tiene conocimiento de un hecho estimado como delictuoso y termina con el acto en que la autoridad investigadora tiene conocimiento de un hecho estimado como delictuoso y termina con el acto en que el ministerio público solicita la intervención del órgano encargado de aplicar la ley. El fin de este periodo reside en la reunión de los datos que son necesarios para que el ministerio público pueda excitar al órgano jurisdiccional a que cumpla con su función. El contenido de la preparación de la acción procesal, es llenado por un conjunto de actividades realizadas por y ante un órgano especial que es el ministerio público y la policía judicial y debidamente reglamentadas en capítulo propio.

Segundo periodo. De preparación del proceso. Este periodo principia con el asunto de radicación y termina con el auto de formal prisión. Se inicia con la primera actividad que ejecuta el órgano jurisdiccional una vez que tiene conocimiento de la consignación y termina con la resolución que sirve de base al proceso. La finalidad perseguida en este periodo es reunir los datos que van a servir de base al proceso, o sea, comprobar la comisión de un delito y la posible responsabilidad de un delincuente. Sin la comprobación de la comisión de un delito sería inútil seguir un proceso y sin acreditar, cuando menos, datos de los que se puede inferir la responsabilidad de un sujeto, sería también ineficaz la iniciación del proceso. Para que se siga un proceso el legislador exige se tenga base para ello y la finalidad del periodo que estudiamos, es precisamente construir esa base. El contenido de este periodo está integrado por un conjunto de actividades legalmente reguladas y dirigidas por el órgano jurisdiccional.

Tercer periodo. El proceso: los autores lo dividen en las siguientes partes, instrucción, discusión, fallo y cumplimiento de lo juzgado. Atentos a la posición que hemos adoptado, respecto de los límites del procedimiento, desde luego podemos manifestar que el cumplimiento de lo juzgado queda fuera, tanto del proceso, como del procedimiento, razón por la cual para nada lo tratamos.

5.2 BIEN JURÍDICO TUTELADO.

Es todo valor ideal del orden social jurídicamente protegido, en cuyo mantenimiento tiene interés la comunidad, y que se puede atribuir como a su titular, tanto particular, como a la colectividad.

Según COBO DEL ROSAL, el bien jurídico se puede definir como todo valor de la vida humana protegido por el derecho”.²⁵

El bien jurídico lo conceptuamos como el derecho intrínseco que la norma protege. No es otra cosa que la pretensión del legislador de darle protección a ciertos valores del ser humano, y que se convierte en intereses no sólo personales, sino sociales y del Estado.²⁶

Se puede afirmar que el bien jurídico es la tutela que la norma penal brinda a los valores tangibles e intangibles del hombre, desde los más significativos (vida, libertad, patrimonio entre otros), hasta los más irrelevantes (honor, fidelidad, entre otros). En el caso que me ocupa, la intimidad es un bien intangible que merece ser reconocido por las leyes penales, ya que es propiamente un derecho que nos corresponde, el cual consiste en apartar del conocimiento publico los datos más sensibles de nuestra persona, que constituye la esencia de cada sujeto, mismo se ha visto atentado por la

²⁵ COBO DEL ROSAL, Manuel. DERECHO PENAL. PARTE GENERAL, Tercera Edición. Editorial PORRÚA, México, 1979.

²⁶ ZAMORA JIMÉNEZ, Arturo. CUERPO DEL DELITO Y TIPO PENAL. Editorial ANGEL EDITOR, México 2000. Pág. 191.

más alta tecnología, que son los sistemas y equipos informáticos, quedando al descubierto de millones de personas.

El bien jurídico que se protege en cuanto hace al derecho a la intimidad se puede definir como el modo de ser de la persona, sustraído al conocimiento ajeno porque el sujeto no desea su divulgación y conocimiento por terceros, dada la perturbación que ello provocaría en su moral y en la vida social que desarrolle. (La intimidad personal y familiar de cada individuo).

5.3 INSTRUMENTO MATERIAL DE LAS VIOLACIONES A LA INTIMIDAD.

En la actualidad el nuevo instrumento en la comisión de delitos, son las computadoras, también conocidas como ordenadores, dichas herramienta se ha convertido en un medio comisivo de los denominados delitos cibernéticos.

Una computadora es un equipo electrónico incapaz de operar por sí solo. Debe ser dirigida por el hombre para que funcione.

Asimismo cabe hacer mención que los delincuentes informáticos no solo se valen de los ordenadores, sino también de sistemas informáticos, provistos por Internet, concluyendo que el software es algo inmaterial, por que se trata de una creación intelectual. Pero esta creación intelectual no tiene sentido si no se incorpora a elementos materiales en los cuales produce sus efectos.

5.4 NORMATIVIDAD Y PENALIDAD EXISTENTES RESPECTO A VIOLACIONES EN LA INTIMIDAD MEDIANTE EL USO INDEBIDO DE EQUIPOS INFORMÁTICOS.

Primeramente entendamos qué es una pena, ésta es el castigo que el Estado impone con fundamento en la ley, al sujeto responsable de un delito.

Entendamos que la fijación de las sanciones, que se hacen análogamente al señalamiento de los delitos, de una manera abstracta y general, no logra por sí sola ninguna finalidad práctica, pues para ello es necesario que la amenaza se traduzca en realidad. Se logra que los que no han cometido delitos por temor a la sanción no los realicen (prevención general) y que los infractores, por haber sufrido la sanción, temerosos de una nueva aplicación, no vuelvan a cometer delitos (prevención especial).

Respecto a las violaciones a la intimidad mediante el uso indebido de sistemas o equipos informáticos, aún no son consideradas como delito en el término formal de la palabra. Por lo tanto la aplicación de una sanción tiende a ser confusa al momento de adecuarla a la normatividad existente referente a los delitos informáticos.

Para la aplicación de una sanción penal hay que considerar que en el ciberespacio es lo mismo una persona física que una moral, ya que en todos los casos, ambas son incorpóreas a fin de unir los espacios físicos en la red.

Por otra parte no puedo ignorar que existe hoy la posibilidad de evadir la acción de la justicia por la (a veces) imposibilidad de determinar al autor material del acto criminògeno.

A estas fechas, la mayoría de los *hackers* son menores de edad, quienes intentan abrirse paso y ganarse una reputación ingresando y violando, tal o cual sistema protegido. El problema radica justamente en el hecho de su minoridad, ya que la mayoría de los sistemas penales se encuentran impedidos de aplicar pena alguna.

La mayoría de las conductas desviadas se produce en etapas que promedian los 15 o 16 años en que los sujetos activos son menores de edad.

En la mayoría de los sistemas actuales, resulta que a esas edades los sujetos activos pueden resultar no punibles según el régimen penal inoperante de menores.

Actualmente no hay una legislación que reglamente las violaciones a la intimidad mediante el uso indebido de sistemas y equipos informáticos, sin embargo, existe normatividades que van encaminadas a la protección de datos personales, siendo éstas las siguientes:

LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL (CAPÍTULO IV)

Capítulo IV

Protección de datos personales

Artículo 20. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;

II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;

IV. Procurar que los datos personales sean exactos y actualizados;

V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y

VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Artículo 21. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

Artículo 22. No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:

I. (Se deroga).

Fracción derogada DOF 11-05-2004

II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;

IV. Cuando exista una orden judicial;

V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y

VI. En los demás casos que establezcan las leyes.

Artículo 23. Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales.

Artículo 24. Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.

La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27.

Artículo 25. Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones.

Artículo 26. Contra la negativa de entregar o corregir datos personales, procederá la interposición del recurso a que se refiere el Artículo 50. También procederá en el caso de falta de respuesta en los plazos a que se refieren los artículos 24 y 25.

LEY FEDERAL DEL DERECHO DE AUTOR (PROTECCIÓN DE LOS PROGRAMAS DE COMPUTACIÓN).

Capítulo IV

De los Programas de Computación y las Bases de Datos

Artículo 101.- Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

Artículo 102.- Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

Artículo 103.- Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.

Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

Artículo 104.- Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

Artículo 105.- El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

I. Sea indispensable para la utilización del programa, o

II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

Artículo 106.- El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;

II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;

III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y

IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

Artículo 107.- Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

Artículo 108.- Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

Artículo 109.- El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Artículo 110.- El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;

II. Su traducción, adaptación, reordenación y cualquier otra modificación;

III. La distribución del original o copias de la base de datos;

IV. La comunicación al público, y

V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111.- Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

Artículo 112.- Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

Artículo 113.- Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.

Artículo 114.- La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

CÓDIGO PENAL FEDERAL

LIBRO SEGUNDO

TÍTULO NOVENO. REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

CAPÍTULO I. REVELACIÓN DE SECRETOS

Artículo 210. Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que

pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

Artículo 211. La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial

Artículo 211 bis. A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Artículo 211 bis 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el distrito federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 3. Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad mas de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

5.5 EL DAÑO MORAL.

En la comisión de conductas delictivas que dañan o transgreden la intimidad de una persona, principalmente el castigo que se les asigna a los sujetos activos es la privación de la libertad, sin embargo, considero, que al individuo que ha sido lesionado en su intimidad, se le ve afectado en su integridad emocional y psicológica, toda vez

que se han perturbado sus datos sensibles, poniendo al descubierto sus deseos más íntimos ante millones de personas, motivo por el cual hago hincapié al daño moral.

Daño: (del latín *damnum*) efecto de dañar; perjuicio, detrimiento, menoscabo. Es toda lesión a un interés.

El daño resarcible, es ofensa o lesión de un derecho o de un bien jurídico cualquiera.

Cuando existe una lesión sobre bienes de naturaleza extrapatrimonial o inmaterial, al daño causado se le llama moral; es decir, cuando los derechos de la personalidad son conculcados, estamos ante un agravio moral. Cuando el campo de protección del derecho se proyecta sobre bienes que no pueden ser tasables en dinero, como son el honor, sentimientos, afectos, creencias, etc., el daño causado a éstos se denomina moral.

Es cierto que tratándose de bienes patrimoniales, el problema se resuelve con la misma rapidez que el planteamiento de la controversia. Su naturaleza así nos lo permite determinar: si yo dañé el reloj, entonces o bien arreglo el reloj dañado – reparación natural- o entrego uno de la misma especie y calidad- reparación por equivalencia -, y asunto concluido. Pero si lesiono en el honor a una persona causándole un dolor moral, dicho agravio quedará para siempre; nunca existirá en la reparación moral la situación de que las cosas vuelvan al estado en que se encontraban o que el daño desaparezca. Es por eso que la reparación moral sólo cumple una satisfacción equivalente; nuestro derecho así lo admite.

El daño moral no admite una evaluación pecuniaria en atención a los bienes lesionados, por lo que la entrega de la suma de dinero no indica que se valore o ponga precio a bienes de naturaleza inmaterial como son el honor, los sentimientos la reputación, etc. Es por esto que la reparación moral tiene como fin último la función satisfactoria que pueda considerarse equivalente al sufrimiento experimentado.

La reparación moral es:

- *Equivalente*: se da cuando las cosas no pueden volver al estado en que se encontraban antes del daño, pero se tratará de ubicar al agraviado en una situación parecida a la que vivía. La compensación opera normalmente entregando una suma de dinero, que es el medio más idóneo. Esta reparación por equivalencia es monetaria, única y exclusivamente. No puede existir la reparación como en ciertos casos de daño patrimonial, donde se entrega un objeto similar al dañado, ya que además de ser esto imposible, tratándose de bienes inmateriales.
- *Satisfactoria*: en razón de que la reparación moral no admite con respecto de los bienes que tutela una evaluación en dinero, ni perfecta ni aproximada, por ser de naturaleza extrapatrimonial.

SUJETOS QUE INTEGRAN LA RELACIÓN JURÍDICA QUE NACE DEL DAÑO MORAL

- Agraviado o sujeto pasivo. Es toda persona que soporta el daño cierto y actual sobre un bien de naturaleza extrapatrimonial y por lo cual tendrá la acción de reparación moral en contra del sujeto activo de la misma.
- Sujeto activo o agente dañoso. Es aquel a quien se le imputa que por un hecho u omisión ilícitos afecta a una persona en sus derechos de la personalidad, lesionando uno o varios bienes que tutela el daño moral, el cual será responsable moralmente ante el ofendido del daño causado.

La demostración de la existencia del daño moral es objetiva y resulta de la violación de alguno de los bienes que tutela el derecho sobre agravio extrapatrimonial, realizados por una conducta ilícita.

Al daño originado por todo acto atentatorio de los derechos de la personalidad, doctrinariamente se le llama daño moral, y por clasificación en cuanto al objeto, no puede considerarse daño moral aquel que se proyecta sobre bienes de naturaleza material. El daño en su concepción teórica, no puede existir éste considerado como daño puro, porque no existe daño si no existe un sujeto agraviado. Es decir, si no hay sujeto dañado, no puede existir el daño por sí mismo para efectos de la reparación, ya que para fines teóricos y procesales no se integra la relación jurídica de responsabilidad civil, entre la existencia del daño y el sujeto agraviado. Este criterio es aplicable íntegramente al daño moral. Se denomina daño moral directo aquél que lesiona o afecta bienes de naturaleza extrapatrimonial o inmateriales, y el daño moral indirecto se da cuando la afectación de un bien de naturaleza extrapatrimonial se causa un menoscabo de naturaleza material, o cuando de la afectación de un bien de naturaleza patrimonial se lesionan bienes del patrimonio inmaterial o moral de la persona.

El agravio moral es fuente de obligaciones, porque su reparación, en último análisis, desemboca en el derecho al cobro de daños y perjuicios. El patrimonio moral de una persona se puede definir como: “el conjunto de bienes de naturaleza extrapatrimonial, los cuales, por su naturaleza inmaterial, no son susceptibles de valoración directa en dinero y su afectación provoca la reparación civil por equivalente y con un fin satisfactorio.

El derecho a la reparación moral es un derecho personalísimo, ya que no puede transmitirse a terceros por acto entre vivos y tal derecho se extingue con la muerte de su titular. Esta singularidad sufre una excepción, cuando la acción de reparación, por disposición de la ley, pasa a los herederos del agravio, siempre que éste haya intentado la acción en vida. Si no se cumple esta condición, dicha transmisión no opera.

Pero no debe confundirse lo personalísimo de este derecho con el derecho que se tiene para demandar ante un tribunal el pago de una reparación moral (legitimación procesal). Es personalísimo el derecho a la reparación moral. Esto significa que el derecho para demandar por daño moral se extingue con la muerte del titular, y la acción

de reparación no puede transmitirse a terceros mientras viva el sujeto agraviado, si el titular del derecho a ser reparado muere, también muere tal derecho.

Otro aspecto importante es que la acción para reclamar la reparación moral prescribe en el lapso de dos años, contados a partir del día en que se causó el daño o en que terminó de causarse, y la prueba del daño moral es de carácter objetivo, ya que tiene las siguientes características:

- a. Debe probarse la relación de causalidad, que vincula al sujeto activo o agente dañados, con el sujeto pasivo o agraviado.
- b. Se debe acreditar la existencia del hecho u omisión ilícitas que causaron un daño moral, lesionando uno o varios de los bienes que tutela esta figura, y
- c. El daño moral desde el aspecto subjetivo, no requiere ser demostrado.

El órgano jurisdiccional tiene facultad discrecional para determinar el monto de dinero que se entregará al sujeto pasivo por concepto de reparación moral. Esta facultad discrecional deberá apreciar lo siguiente: los bienes lesionados, el tipo y grado de responsabilidad, la realidad del ataque, la conducta ilícita y los aspectos económicos del sujeto activo y del sujeto pasivo.

Requisitos previos

- a. el juez deberá hacer un análisis de los derechos lesionados; es decir, si el agravio moral conculcó la honra de una persona solamente o también su reputación, sentimientos, decoro, etc., según el caso concreto.
- b. El grado de responsabilidad se relaciona directamente con el vínculo jurídico que existe entre el sujeto activo y el agraviado, ya sea de responsabilidad directa o indirecta.
- c. La situación económica de la víctima y del responsable. El juez debe analizar este punto descartando la idea de que, si el sujeto activo es muy rico, la reparación deberá ser generosa o que si el agraviado carece de recursos

económicos se le entregará una gran suma de dinero por concepto de indemnización, y de la misma forma a *contrario sensu*.

- d. Circunstancias genéricas del caso. El juez, una vez que haya analizado y considerado los incisos anteriores, deberá, si así lo acredita la controversia, evaluar todo elemento extraño a lo mencionado, y que sea de una importancia tal que incluya directamente en el aumento o disminución del monto de la reparación. Incluso aquí es donde puede valorar circunstancias que destruyan la ilicitud de la conducta o irrealidad del ataque, o aclaren la magnitud o extensión del daño, recordando que todos los medios de prueba permitidos por nuestra ley procesal pueden ser utilizados para acreditar que existe o no agravio moral, o bien, que el monto de la reparación debe ser significativo, reducido o simbólico.

Su regulación jurídica del daño moral o más bien denominado reparación del daño, se encuentra inmerso en el Código Penal para el Distrito Federal, en el Título Tercero, Capítulo Quinto, Artículos 42 a 49.

En el código penal federal se encuentra regulado en el Título Segundo, Capítulo Quinto, Artículos 30 a 39

5.6 POLICÍA CIBERNÉTICA.

La llamada Policía Cibernética es una de las más recientes "adquisiciones" de la Secretaría de Seguridad Pública Federal. Y aunque sus funciones primarias son la detección de pedófilos y grupos criminales dedicados a la prostitución infantil, su base de datos es también una valiosa herramienta para detectar a 'hackers' que de alguna manera comprometen la información de personas, instituciones públicas y privadas.

La Policía Cibernética opera a través de lo que llaman 'patrullajes *antihacker* por el ciberespacio' a través de computadoras. Esto sirve también para atrapar a los delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red, sin que necesariamente se dediquen a la pornografía infantil.

Tiene como objetivo el garantizar la seguridad y la capacidad reactiva conjunta para combatir ilícitos provocados por la acción humana en la Red *Internet* mediante el uso de sistemas de cómputo.

INTEGRANTES:

- Entidades del Poder Ejecutivo Federal, integrantes del gabinete de Seguridad Nacional.
- El Poder Legislativo Federal a través de las comisiones de Comercio, Seguridad, Equidad y Género, Población Vulnerable y Derechos Humanos de la Cámara de Diputados y de Senadores.
- Gobiernos Estatales: Distrito Federal, Jalisco, Baja California y Coahuila.
- Universidades y Centros de Educación Superior.
- Empresas privadas vinculadas con seguridad en sistemas de cómputo, asociaciones nacionales e internacionales.
- Organizaciones civiles comprometidas con la seguridad en Internet y de e-commerce.
- Proveedores de servicios de Internet en México

ACTIVIDADES.- Es un cuerpo colegiado que concentra la información necesaria para la identificación, monitoreo, rastreo y localización de todas aquéllas manifestaciones delictivas tanto en el territorio nacional como fuera de él.

En la actualidad, la Policía Cibernética así como también DC México trabaja conjuntamente con los siguientes organismos:

- *US Customs Cybersmuggling Center (C 3)*
- *Servicio Secreto de los EUA*
- *National Center for Missing & Exploited Children.*
- *Brigada Tecnológica de España.*
- *International Association of Law Enforcement Intelligence Analysts.*

- *High Technology Crime Investigation Association*
- *APEC Counter-Terrorism Action plan*

Cabe señalar que si bien entre sus funciones está la de combatir la pornografía infantil vía Internet, la Policía Cibernética también busca prevenir otros delitos que se cometen en y a través de una computadora, principalmente aquéllos que atentan contra las instituciones y la población vulnerable.

Con ello se busca hacer de Internet en México un lugar seguro para el intercambio de información, además de analizar y atacar los diferentes tipos de delitos cibernéticos que se presentan en el ciberespacio, así como su *modus operandi*.

La policía cibernética es la encargada de vigilar las páginas *Web* existentes que pudieran vulnerar los artículos correspondientes del Código Penal Federal.

El fin específico de la policía cibernética es coadyuvar con el ministerio público en la investigación de delitos que se cometan por medio de sistemas o equipos informáticos.

5. 7 FUNCIÓN PERSECUTORIA DE LOS DELITOS INFORMÁTICOS.

La función persecutoria, consiste en perseguir los delitos o lo que es lo mismo, en buscar y reunir los elementos necesarios y hacer las gestiones pertinentes para procurar que a los autores de ellos se les apliquen las consecuencias establecidas en la ley.

La función persecutoria impone dos clases de actividades, a saber:

- a) Actividad investigadora, entraña una labor de auténtica averiguación; de búsqueda de las pruebas que acreditan la existencia de los delitos y la responsabilidad de quienes en ellos participan. Durante esta actividad, el órgano que la realiza trata de proveerse las pruebas necesarias para

comprobar la existencia de los delitos y poder estar en aptitud de comparecer ante los tribunales y pedir la aplicación de la ley.

- b) Ejercicio de la acción penal. Agotada la averiguación y cerciorado el órgano encargado de ella (Ministerio Público) de la existencia de una conducta típica y de la imputación que de la misma se puede hacer, se prepara el momento culminante de la preparación del ejercicio de la acción penal.

El ejercicio no sólo comprende la consignación, pues también abarca las actuaciones posteriores como son: aportación de pruebas, órdenes de comparecencia, aseguramientos precautorios, formulación de conclusiones, de agravios y alegatos.

En palabras del autor RIVERA SILVA, asevera que el órgano persecutor al momento de dictar el ejercicio de la acción penal excita a los tribunales a la aplicación de la ley al caso concreto.²⁷

El artículo 21 constitucional establece que” la investigación y la persecución de los delitos incumbe al Ministerio Público y a las policías, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función.

El Ministerio Público actúa en cuanto tiene noticias de la comisión de un acto reputado como delictuoso e inicia el ejercicio de la acción penal cuando de la investigación que ha practicado, infiere la existencia de un “delito real” y la posible responsabilidad de alguien.

En este capítulo me he referido en gran parte a las atribuciones y facultades del ministerio público, por que considero que esta figura jurídica es la primera en conocer de un acto que se considera delictuoso, siendo la primera autoridad a la que se debe de

²⁷ RIVERA SILVA, Manuel. El Procedimiento Penal. Editorial PORRÚA, México, 2007, Pág. 397.

acudir ante la perturbación de nuestra persona mediante el uso indebido de sistemas o equipos informáticos. Con las reformas constitucionales publicadas en el Diario Oficial de la Federación el 18 de junio de 2008, el ejercicio de la acción penal privada se realizará directamente por la víctima u ofendido ante la autoridad judicial.

Para una denuncia o el levantamiento de una averiguación previa se sugiere realizar la acusación de manera formal ante la **Agencia del Ministerio Público** más cercano al domicilio de la víctima, en contra quien resulte responsable; asimismo se sugiere anexar copias de correos y todo aquel documento cuyo contenido exponga algún hecho relacionado con la denuncia. Todo esto con la finalidad de que se le pueda brindar una mejor atención. Esto con respecto a cuando se aclare que se ha realizado un delito.²⁸

Esto es en razón de que por mandato constitucional la investigación de los delitos corresponde al **Ministerio Público y a las policías**, las cuales actuarán bajo conducción y mando de aquel en el ejercicio de esta función.

La agencia del ministerio más cercana al domicilio de la víctima será el que conocerá del asunto referente a delitos informáticos y deberá atender la denuncia del ofendido sea el órgano competente o no, una vez que se hace del conocimiento de la autoridad un hecho que se considera delictivo, éste ordenará su envío para la investigación y se reúnan pruebas a la policía cibernética, para que se acrediten los elementos del delito y se pueda consignar a los tribunales y le den seguimiento al delito para su respectiva sanción.

5.8 LOS MENORES DE EDAD COMO PRINCIPALES TRANSGRESORES DE LA INTIMIDAD MEDIANTE EL USO INDEBIDO DE SISTEMAS Y EQUIPOS INFORMÁTICOS.

Comúnmente se afirma que en nuestro medio los menores de 18 años son inimputables y, por lo mismo, cuando realizan comportamientos típicos del Derecho

²⁸ policia_cibernetica@ssp.gob.mx

Penal no se configuran los delitos respectivos; sin embargo desde el punto de vista lógico y doctrinario, nada se opone a que una persona de 17 años, por ejemplo, posea un adecuado desarrollo mental y no sufra enfermedad alguna que altere sus facultades; en este caso, al existir la salud y el desarrollo mentales, sin duda el sujeto es plenamente capaz. Ciertamente el artículo 4º de la ley para el tratamiento de menores infractores, para el distrito federal en materia común y para toda la república en materia federal, fija como limite los 18 años, por considerar a los menores de esa edad una materia dúctil, susceptible de corrección.²⁹

Con el amplio nivel de la tecnología que existe hoy en día, nuestra vida se ha visto invadida por un sin número de actividades a realizar mediante el uso de una computadora y el Internet, el uso de la red se ha cotizado de una manera increíble, ahora la mayoría de las personas pueden tener acceso a un ordenador, ya sea por adquisición propia, o mediante los servicios que brindan los cyber café o comúnmente denominados cyber Internet, en los cuales se pueden rentar las computadoras y utilizar el Internet; este avance tecnológico ha dado pie a que se impartan clases de informática a nivel primaria, secundaria y bachillerato, así como también existen licenciaturas para ingenieros en sistemas de computación, etc.

El amplio conocimiento que se puede adquirir en estos tiempos es inimaginable, los menores de edad son quienes hacen uso del Internet a cada momento, por los amplios servicios que ofrecen las diversas empresas, mismos que en ocasiones no son muy específicos en el momento de contratarlos, los jóvenes en su afán de conocer amigos de otras ciudades se ven inmersos en paginas de Internet que en la mayoría de los casos no son seguras, los link más usados por los menores son *el Messenger*, *hi5*, *facebock* y otros, estos servicios conllevan el intercambio de información y a su vez permiten visualizar datos personales que talvez para los usuarios no son relevantes, pero para otros tantos si, ya que a los denominados delincuentes informáticos les permite crear los perfiles de sus victimas.

²⁹ CASTELLANOS, Fernando. LINEAMIENTOS ELEMENTALES DE DERECHO PENAL. Editorial PORRÚA, México, 2009, Pág. 363.

Muchos menores de edad han alcanzado una mentalidad más amplia, en mi particular punto de vista ya no se les debería considerar o juzgar como sujetos inimputables, porque en estos tiempos los jóvenes de entre 12 y 18 ya son aptos de tomar decisiones por si mismos, y con la ayuda del Internet y la educación que se imparte en las escuelas les ayuda a abrir más su mente, orillándolos a cometer conductas delictivas.

El Internet es una red de gran amplitud, que permite navegar en espacios que jamás podríamos haber imaginado, hoy en día es un medio muy usado para delinquir, ya que es difícil rastrear a los sujetos que se encuentran al frente de una computadora, en la mayoría de ocasiones al estar en comunicación con otra persona por Internet no sabemos con exactitud si es un hombre o una mujer, toda vez que este medio se presta para cambiar de identidad cuantas veces lo deseemos.

A los jóvenes entre 12 y 18 años se les hace fácil quebrantar las reglas, ya que tiene la idea de que por ser menores de edad no se les va castigar si cometen alguna conducta delictiva, el Internet es una herramienta para que los adolescentes y otros tantos adultos cometan delitos informáticos, ya que el medio se los permite, muchos de nosotros utilizamos servicios que ofrece el Internet, sin siquiera enterarnos que tan seguro puede ser el usarlos y damos datos sin informarnos antes de que tan grave puede ser que estos sean manejados en el ciberespacio.

Los menores de edad en la mayoría de los casos sabe que al inmiscuirse en la vida privada de otra persona o el obtener datos íntimos de la misma, ya esta entrando en un ámbito que sabe y entiende que lo es permitido o autorizado conocer, pero que sin embargo por la curiosidad o por el afán de diversión transgrede los sentimientos de otros sujetos para sentirse superior o hacerse reconocer ante sus amigos, ello implica que muchos jóvenes se vena involucrados en delitos informáticos, porque piensan que jamás podrán ser rastreados por las autoridades.

Es por eso que en el presente trabajo he dedicado un apartado para los menores de edad, ya que considero que son quienes actualmente cometen más conductas delictivas mediante el uso del Internet, ya que son quienes constantemente usan dicho servicio y tienen la curiosidad de conocer el ámbito privado e íntimo de los demás, uno de los servicios en el cual se delinque más es, en la intromisión a cuentas de correo electrónico, mediante el cual los sujetos sustraen datos de índole personal permitiéndoles hacer un uso indebido de ellos, ya sea difamando a los propietarios de las cuentas de correo o propagando la información obtenida de los mensajes que son depositados en dicho servicio. Lo anterior implica un delito y por lo tanto a los menores de edad que son sorprendidos en la comisión de este tipo de conductas antisociales se les debe sancionar, tal y como lo expongo en el punto siguiente.

5.8.1 MEDIDAS DE CORRECCIÓN PARA LOS MENORES INFRACTORES

Actualmente las conductas delictivas cometidas por menores de edad se ven sancionadas mediante la ley de justicia para adolescentes para el distrito federal, así también esta la del estado de México, pero en el presente trabajo solo haré hincapié a la del Distrito Federal, esta tiene aplicación supletoria en El Código Penal para el Distrito Federal, el Código de Procedimientos Penales para el Distrito Federal.

Para el mejor desempeño de sus funciones, los órganos y autoridades especializadas en justicia para adolescentes podrán celebrar convenios con organismos, instituciones públicas o privadas y entidades federativas para que participen y colaboren en la consecución de los fines establecidos en la presente Ley, (artículo 13)

Los adolescentes serán responsables por la comisión de las conductas tipificadas como delitos, en los casos y términos que se establecen en esta Ley.

La responsabilidad de los adolescentes se fincará sobre la base del respeto irrestricto al principio de culpabilidad por el acto y no admitirá bajo ninguna circunstancia

consideraciones acerca de la personalidad, peligrosidad, ni de cualquier otra que se funde en circunstancias personales del autor de la conducta tipificada como delito.

Para resolver sobre la probable responsabilidad del adolescente, la autoridad deberá constatar que no exista acreditada a favor de aquél alguna causa de exclusión y que obren datos suficientes para acreditar su probable culpabilidad

Cuando se trate de conductas tipificadas como delitos culposos, el agente del Ministerio Público entregará de inmediato al adolescente a sus padres, representantes legales o encargados, quienes quedarán obligados a presentar al adolescente ante la autoridad competente cuando para ello sean requeridos, para tal efecto deberán presentar las garantías necesarias, como lo prevé esta Ley.

El agente Ministerio Público estará obligado a solicitar la reparación del daño y el Juez no podrá absolver al adolescente de dicha reparación si ha emitido resolución que lo considera plenamente responsable, (artículo. 15).

El Juez al recibir las actuaciones por parte del agente del Ministerio Público que contengan la acción de remisión con adolescente detenido, radicará de inmediato el asunto, calificará en su caso de legal la detención y tomará la declaración inicial dentro del término de veinticuatro horas contadas a partir de que el Juez realizó la radicación; pronunciará dentro de las cuarenta y ocho horas siguientes resolución inicial, que determine la situación jurídica del adolescente sin perjuicio de que este plazo se amplíe por setenta y dos horas más, únicamente si así lo solicitara el adolescente o su defensor con la finalidad de aportar pruebas a su favor.

En este último caso, la ampliación del plazo se hará de inmediato del conocimiento del funcionario que tenga a su disposición al adolescente para los efectos de su custodia.

En caso de acción de remisión sin detenido, el Juez en un término de dos días deberá radicar la investigación remitida librando orden de comparencia, cuando se trata de conducta tipificada como delito no grave, o de detención para conductas tipificadas

como delito graves, y sólo hasta que el adolescente es puesto a disposición del Juez comenzarán a correr los términos a que se refiere el primer párrafo de este artículo, (artículo 27).

ARTÍCULO 28.

Cuando se ejercite la acción de remisión con detenido, el juez radicará de inmediato el asunto y calificará la legalidad de la detención. Celebrará audiencia en la que tomará la declaración inicial del adolescente, analizará la pertinencia de las medidas cautelares si el Ministerio Público o la defensa lo solicitare.

Si la detención resultare improcedente, la audiencia se suspenderá y se decretará la inmediata libertad del adolescente y se devolverán las actuaciones al Ministerio Público. Cuando las actuaciones sean devueltas al Ministerio Público, contará con treinta días para integrar el expediente de la averiguación previa para remitirlo nuevamente al Juez. En caso de que el Ministerio Público no presentará en el plazo señalado las actuaciones correspondientes, el Juez deberá dictar sobreseimiento respecto al proceso de que se trate.

Para efectos de la celebración de la audiencia, el Juez notificará de manera personal a las partes, aclarando el momento en que se realizó la radicación y observando en todo momento el término para practicar la declaración inicial del adolescente. En el mismo auto hará del conocimiento del adolescente y su defensor el derecho que tienen a ofrecer pruebas, mismas que se desahogarán en la audiencia, únicamente las que hayan sido admitidas por el Juez.

Si la audiencia se suspende a petición del adolescente o su defensor, el Juez, a solicitud del representante del Ministerio Público, podrá imponer alguna de las medidas cautelares de las previstas en esta Ley hasta que la audiencia se reanude.

A esta audiencia deberán concurrir el agente del Ministerio Público, el adolescente probable responsable, su defensor y, en su caso, podrán asistir, padres,

tutores o quienes ejerzan la patria potestad o la custodia del adolescente. La ausencia de éstos últimos no suspenderá la audiencia.

Para la celebración de la audiencia, si el adolescente no se encontrara detenido, a solicitud del Ministerio Público, el Juez podrá dictar:

I. Orden de detención, ejecutada por la fuerza pública, cuando la conducta que se investiga sea grave, merezca medida de internamiento y exista una presunción razonable, por apreciación de las circunstancias del caso particular, de que el adolescente podría no someterse al proceso u obstaculizarlo, o se estime que el adolescente puede cometer una conducta tipificada como delito doloso contra la propia víctima, alguno de los testigos que depongan en su contra, servidores públicos que intervengan en el proceso o contra algún tercero.

II. Orden de presentación, en todos los demás casos.

Las medidas reguladas por esta Ley tienen como finalidad la reintegración social y familiar del adolescente y brindarle una experiencia de legalidad, así como valorar los beneficios de la convivencia armónica, del civismo y del respeto de las normas y de los derechos de los demás y serán impuestas por la autoridad judicial; se instrumentarán en lo posible, con la participación de la familia, de la comunidad y, en su caso, con el apoyo de los especialistas, atendiendo en todo momento a la protección integral y al interés superior del adolescente.(artículo 56)

Todas las medidas reguladas por esta Ley, están limitadas en su duración y no podrán, bajo ninguna circunstancia, superar el máximo previsto para cada una de ellas. Ello no excluye la posibilidad de determinar el cumplimiento de la medida antes de tiempo, ni adecuarla en beneficio del sujeto de la misma, en los términos previstos por esta Ley.

La decisión sobre la medida que corresponde ser impuesta debe tener relación directa con los daños causados, así como la intencionalidad de ocasionarlos, (artículo 57).

Una vez dictada la sentencia, la reparación del daño derivado de la realización de una conducta tipificada como delito puede solicitarse por la víctima u ofendido o sus representantes legales ante el Juez que imponga la medida, (artículo 90)

De lo anterior podemos observar que si hay aplicación de sanciones a los menores de edad, pero para que se puedan ser castigados, primeramente debe existir un ordenamiento específico en el cual la conducta antisocial cometida por dicho sujeto sea debidamente encuadrada. Motivo por el cual es indispensable que se lleven a cabo reformas en el código penal respecto del tema que me ocupa, tal como lo señalo en el capítulo respectivo de propuestas.

Uno de los problemas más evidentes es el ámbito de aplicaciones de la ley penal, es que las conductas que se realizan mediante el uso indebido de sistemas y equipos informáticos, en la mayoría de los casos se cometen en diversas ciudades del mundo, motivo por el cual no existe una compatibilidad de penas, y por tanto no hay una exacta aplicación de sanciones a los infractores.

5.9 LA INTIMIDAD ANTE LOS AVANCES INFORMÁTICOS Y SU SITUACIÓN ACTUAL.

En la denominada **sociedad de la información** se ha invadido la intimidad de la persona, hasta tal punto que en la actualidad el individuo reclama la adopción de instrumentos jurídicos de respuesta a las sucesivas y frecuentes intromisiones que debe padecer en su intimidad. En una sociedad caracterizada por el ansia de poder y en la que el poder se consigue con información, es fácil comprender el requerimiento del individuo en orden a la regulación de instrumentos jurídicos eficaces ya adecuados para la protección de la intimidad personal y familiar.

Ahora el individuo aspira a reservar para sí la información que le concierne, que revela sus hábitos y comportamientos, sin necesidad de que la misma sea íntima o permanezca a su núcleo esencial de personalidad. Por tanto se trataría de reconocer al individuo capacidad para decidir y determinar qué información personal se podrá difundir, cuál permanece como núcleo esencial de su estricta intimidad, y por tanto, excluida del conocimiento de los demás.

La información constituye en la actualidad un instrumento de poder y en ocasiones mercancía valiosa de cambio; de lo que se trata es de impedir los abusos y asegurar a los sujetos una cierta esfera privada, libre de incursiones de terceros a no ser que preste su consentimiento, o bien se lleven a cabo por causas excepcionales y justas previstas por la ley.

En la situación tecnológica propia de la sociedad actual todos los ciudadanos, desde su nacimiento, se hallan expuestos a violaciones de su intimidad perpetradas por determinados abusos de la informática y la telemática. La injerencia del ordenador en las diversas esferas y en el tejido de relaciones que conforman la vida cotidiana se hace cada vez más extendida, más difusa, más implacable.³⁰

Siendo esto así, la mayoría de los usuarios no es consciente de la cantidad de información privada que de forma inadvertida e involuntaria está revelando a terceros al hacer uso de Internet. Cada vez que se visita un sitio *web*, se suministra de forma rutinaria una información que puede ser archivada por el administrador o proveedor de sitio; a éste no le resulta difícil averiguar la dirección de Internet de la máquina desde la que se está operando, la dirección de correo electrónico del usuario, qué páginas lee y cuántas no le interesan, cuántas ha visitado, así como el sistema operativo y el navegador utilizado. Con ello se expone a ser víctima de graves atentados contra su vida privada, dando también lugar a que terceros – por ejemplo, empresas de servicios o de publicidad – se aprovechen de esta información y de estos datos para fines comerciales.

³⁰ REBOLLO DELGADO, Lucrecio. El Derecho Fundamental a la Intimidad. Editorial DYKINSON, Madrid España, 2000, Pág. 299.

Las modernas técnicas de procesamiento y tratamiento de datos personales permiten en la actualidad la posibilidad de acumular la información sin límites, tanto en lo que se refiere al tiempo, como al espacio.

La facilidad de intercambiar informaciones a distancia puede generar importantes peligros para la protección de los datos personales. El carácter internacional e ilimitado de esas conductas hacen más difícil su descubrimiento, prevención y castigo, ya que incluso en los casos en que puedan ser detectadas pueden plantearse conflictos sobre la jurisdicción sancionadora competente.

Este hecho ya marca una notable diferencia con el mundo real, la cual se ve monumentalmente agrandada si se toma en cuenta que por ejemplo, en la red no existe el sexo, ya que al menos detrás de un monitor bien puede ser hombre, bien puede ser mujer y quien esté del otro lado difícilmente notará la diferencia.

Esta ventaja del entorno otorga un cierto grado de sensación de impunidad debido al anonimato, lo cual anima aún más a las conductas desviadas.

Hoy en día, se reconoce al individuo una tutela legal para conocer y acceder a las informaciones almacenadas en ficheros de datos que les conciernen, así como la facultad de controlar por el interesado la calidad de los datos inexactos o indebidamente automatizados y consentir su transmisión que define el contenido que integra la libertad informática.

El verdadero desafío, dicho todo lo anterior, consiste en aplicar las reglas vigentes de la criminología actual a las conductas desarrolladas por los individuos que podríamos considerar desviados dentro de esta subcultura informatizada sobre todo si estos comportamientos pueden trasuntar en desvalores para la sociedad en general.

Si no se prevén los alcances de las nuevas tecnologías en referencia a la ubicación de los autores y la posibilidad o no de su comparecencia en un juicio ante los

tribunales competentes para la aplicación de sanciones con referencia al caso concreto, dará origen a que una gran suma de víctimas(sobre todo en los delitos informáticos) sientan que pierden el tiempo y la verdad es que en la mayoría de los casos, debido a la novedad de los delitos, a la falta de una correcta legislación y a los escasos conocimientos de la materia de los encargados del *ius puniendi*,; en la realidad, casi siempre las víctimas pierden el tiempo puesto que rara vez se condena a algún responsable del delito, porque o no se puede hacer la subsunción penal correcta o no existen pruebas.

No es realmente grave que se pueda disponer de infinidad de datos de las personas en soportes reducidos, lo verdaderamente significativo es la utilización que se haga de dicha información, cómo se relacione o a quién se transmita y con qué finalidades. Datos relativos a las personas aparentemente inconexos, irrelevantes o inútiles se transforman en informaciones trascendentes y reveladoras de los comportamientos y personalidades cuando se relacionan o entrelazan adecuadamente.

Actualmente se trata de garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada con respecto al tratamiento automatizado de datos que pueden afectarle, conciliando los valores fundamentales del respeto a las libertades y de la libre circulación de información entre los pueblos.

CONCLUSIONES

PRIMERA.- Someramente, se han sentado las bases de la definición de la intimidad, conceptuándola como la esfera interior del individuo sobre el conjunto de actividades que forman parte de un círculo íntimo, personal y familiar que constituyen datos sensibles, mismos que quedan excluidos del conocimiento del público.

SEGUNDA.- La intimidad pertenece al ámbito más interno de la naturaleza humana y que se corresponde con la esfera más profunda de la persona. La privacidad se define como la libertad del individuo ante el contacto con la sociedad y frente a la observación de los demás, esto es, el derecho a la privacidad reconoce la capacidad de la persona para decidir voluntariamente un apartamiento o retirada de la vida en sociedad.

TERCERA.- El ser humano es social por naturaleza pero, pese a ello, no deja de sentir la necesidad de realizar una vida interior, ajena a las relaciones que mantiene con otros individuos y que le permite identificarse como ser humano.

CUARTA.- El derecho nace para regular relaciones sociales, esto es, el legislador está interesado en que la convivencia o los asuntos que conciernan a la comunidad se rijan por unos principios determinados.

QUINTA.- La dignidad es una parte esencial de los atributos de la persona, independientemente de que el derecho lo reconozca o no.

SEXTA.- El derecho a la intimidad se define a través de lo que es propio y exclusivo de la persona, es el derecho que concierne a cada persona a ser ella, será quien determine cuándo y hasta qué límite desea entrar en contacto con la sociedad que lo rodea.

SÉPTIMA.- La intimidad no consiste únicamente en el ocultamiento o la reserva de aspectos de la vida íntima o privada de las personas, sino en el reconocimiento de un conjunto de facultades que permitan a la persona decidir respecto a su vida y sus relaciones, disponiendo de mecanismos de defensa que aseguren la libertad del individuo y su control sobre la información que se ha revelado respecto a su persona.

OCTAVA.- La facultad de intercambiar ideas y experiencias, mediante el lenguaje, es un atributo definitorio del género humano. Sin comunicación no puede existir conocimiento entre los hombres, tampoco relaciones mutuas basadas en la cooperación; en suma, sin ella no es posible la sociedad o comunidad.

NOVENA.- Toda información personal, merece protección frente al poder informático, no es lo verdaderamente significativo la naturaleza íntima o no de los datos que se conocen o tratan, sino que sea susceptible de afectar al individuo; se pretende evitar la intromisión, la simple invasión en la vida ajena, el ataque a la misma es susceptible de causar un daño irreparable a la persona.

DÉCIMA.- La información constituye en la actualidad un instrumento de poder y en ocasiones mercancía valiosa de cambio; de lo que se trata es de impedir los abusos y asegurar a los sujetos una cierta esfera privada, libre de incursiones de terceros a no ser que preste su consentimiento, o bien se lleven a cabo por causas excepcionales y justas previstas por la ley.

DECIMOPRIMERA.- Con el desarrollo de las tecnologías informáticas tanto el ámbito íntimo, como el menos próximo a la persona puede verse afectado y su conocimiento, divulgación o inadecuado tratamiento informatizado puede perjudicar a la persona; frente a la utilización y tratamiento informático de la información no cabe clasificar la información en íntima y no íntima, porque los datos relativos a la persona, hasta los más insignificantes o inocuos, si son adecuadamente relacionados pueden representar un peligro para la integridad moral y para la identidad personal.

DECIMOSEGUNDA.- La seguridad, que se traduce en el establecimiento de medidas que garanticen los datos personales frente a los riesgos de destrucción, pérdida, modificación o accesos indebidos; y la responsabilidad que se traduce en la necesidad de identificar al titular del fichero a fin de que pueda responder de sus obligaciones sobre la protección de datos personales.

DECIMOTERCERA.- Se reconoce al individuo una tutela legal para conocer y acceder a las informaciones almacenadas en ficheros de datos que les conciernen, así como la facultad de controlar por el interesado la calidad de los datos inexactos o indebidamente automatizados y consentir su transmisión que define el contenido que integra la libertad informática.

DECIMOCUARTA.- Actualmente existen diferentes jóvenes intrusos capaces de acceder a los sistemas informáticos indebidamente gracias a sus conocimientos de las nuevas tecnologías. Para ellos el acceso ilícito a las redes informáticas representa un reto intelectual con propósito lúdico y para algunos otros con afán de lucro económico.

DECIMOQUINTA.- En nuestros días, son más reducidos los espacios vitales aislados del conocimiento ajeno a consecuencia del Internet.

DECIMOSEXTA.- Las nuevas tecnologías de la información y de la comunicación permiten multiplicar por mil la velocidad de tratamiento de la información, la capacidad de almacenamiento y la capacidad de transmisión de los datos.

DECIMOSÉPTIMA.- La característica fundamental de las redes digitales, y en concreto de Internet, es la gran cantidad de información y datos que circulan por ellas, así como la facilidad con la que los usuarios pueden acceder a los mismos.

DECIMOCTAVA.- Los sistemas *on-line*, permiten la posibilidad de establecer interrelación a distancia con objeto de precisar la pregunta mediante un diálogo entre el usuario y la máquina.

DECIMONOVENA.- La cibernética, es la ciencia que estudia los sistemas de control y comunicación de las máquinas, de modo que la cibernética jurídica sería la ciencia que estudia los sistemas de control y comunicación de las máquinas en el campo del derecho.

VIGÉSIMA.- La informática jurídica es el conjunto de aplicaciones de la informática en el ámbito del derecho.

VIGÉSIMO PRIMERA.- El derecho informático o derecho de la informática es una materia inequívocamente jurídica; conformada por el sector normativo de los sistemas jurídicos contemporáneos integrado por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, la informática y la telemática.

VIGÉSIMO SEGUNDA.-La difusión de la informática en todos los ámbitos de la vida social ha determinado que se le utilice como instrumento para la comisión de actividades que lesionan bienes jurídicos y entrañan el consiguiente peligro social, o que sea la propia informática el objeto de atentados criminales. Estas facetas compendian la noción genérica de delito informático, es decir, aquel conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectan al funcionamiento de los sistemas informáticos.

VIGÉSIMO TERCERA.- Los derechos a la confidencialidad de la información y la intimidad de nuestros datos personales sólo podrán ser violados si se prueba que es claramente razonable y justificado hacerlo en el contexto de una sociedad libre y democrática. Esto es, que constituye una medida necesaria para la seguridad nacional, para el bienestar económico del país, para la defensa del orden y de la prevención de las infracciones penales, para la protección de la salud o para la protección de los derechos y libertades de terceros.

VIGÉSIMO CUARTA.- La amenaza más evidente, de la que cualquier usuario de Internet es consciente, consiste en los ataques a la confidencialidad, autenticidad e

integridad del correo electrónico. La mayor preocupación se centra en encontrar medios de criptografía que permitan al usuario hacer correr datos personales por la red sin ser identificados.

VIGÉSIMO QUINTA.- Al consagrar la libertad de expresión. Ello permite recibir y dar información, lo que indudablemente, ante la aparición de la informática y la interconexión de redes, o el acceso a ficheros determinados, da lugar a que se conozcan y expongan los datos de una persona de manera que puedan afectar tanto su derecho a la defensa en juicio, como su intimidad, por exposición de datos sensibles (como los políticos, sexuales y especialmente de enfermedades como el caso del SIDA), puedan crear problemas que no sólo afecten la esfera personal, sino que produzcan discriminación desde el punto de vista racial o religioso, no planteados ostensiblemente en la exclusión que se haga.

VIGÉSIMO SEXTA.- Con la aparición de las redes digitales la información se ha tornado en una valiosa mercancía de cambio. El desarrollo de los útiles y herramientas de navegación por Internet permite realizar un tratamiento *invisible* de esta información mediante la creación de ficheros ocultos. Ello supone que el usuario de Internet, cada vez que enciende el ordenador e inicia una sesión de navegación, va dejando almacenados en tales ficheros, denominados *cookies*, un gran número de datos personales, suficientes para que terceros puedan elaborar un perfil preciso y detallado sobre una persona. Todo ello sin su conocimiento y, por tanto, haciendo quebrar uno de los principios fundamentales sobre los que se asientan la mayor parte de leyes de protección de datos: el de la prestación del consentimiento. No resulta difícil admitir que ello puede constituir una grave amenaza para la vida privada.

VIGÉSIMO SÉPTIMA.- Regulación jurídica de Internet, implica favorecer o restringir la circulación de datos a través de las fronteras nacionales.

VIGÉSIMO OCTAVA.- El objetivo del derecho penal, hoy en día es sancionar la comisión de verdaderos actos ilícitos en los que se tengan a las computadoras como instrumentos para realizarlos.

VIGÉSIMO NOVENA.- La agencia del ministerio más cercana al domicilio de la víctima será quien conocerá del asunto referente a delitos informáticos y deberá atender la denuncia del ofendido sea el órgano competente o no, una vez que se hace del conocimiento de la autoridad un hecho que se considera delictivo, éste ordenará su envío para la investigación y se reúnan pruebas a la policía cibernética, para que se acrediten los elementos del delito y se pueda consignar a los tribunales y le den seguimiento al delito para su respectiva sanción.

PROPUESTAS

PRIMERA.- Elevar la información sobre intimidad, más propiamente en el aspecto penal, ya que es un tema poco reconocido en la actualidad, tanto por los particulares como por las autoridades judiciales.

SEGUNDA.- Con la aparición de las redes digitales la información se ha tornado en una valiosa mercancía de cambio que hoy en día afecta propiamente a la intimidad de las personas, por lo tanto es necesario que los penalistas sitúen su atención a este tipo de violaciones, ya que es un tema que a simple vista es ignorado por los legisladores.

TERCERA.- Crear un sistema de reeducación de los jóvenes a fin de evitar ese tipo de conductas y aplicar los conocimientos adquiridos para la realización de esos actos en el desarrollo de sistemas de seguridad de mayor eficacia que impidan futuras intromisiones, ya que los gobiernos son con los que con mayor frecuencia reciben ataques informáticos.

CUARTA.- introducir al derecho y a la legislación penal mexicana un apartado que permita proteger a las personas frente a los avances tecnológicos.

QUINTA.- Que las compañías que brindan servicios de Internet respeten la vida privada de los usuarios y que faciliten los instrumentos necesarios para ajustarse a la normativa sobre protección de datos.

SEXTA.- Desarrollar y aplicar medidas legales para que los vendedores de software y hardware proporcionen a los usuarios información sobre los datos que pretenden recopilar, almacenar o transmitir, y que sistemas de seguridad proporcionan.

SÉPTIMA.- la creación y formulación jurídica adecuada de tratados internacionales que permitan la cooperación internacional, ya que los delitos que constituyen las violaciones

a la intimidad pueden involucrar más de un sistema jurídico, por la posibilidad que presentan de ser cometidos aún a distancia.

OCTAVA.- Establecer más herramientas de Derecho suficientes para evitar las conductas que puedan vulnerar los bienes jurídicos que se intentan proteger por considerarlos importantes para el desarrollo de la sociedad.

NOVENA.- proveer a la policía cibernética de mejores equipos informáticos para el rastreo de delincuentes cibernéticos.

DÉCIMA.- Implantar cursos de capacitación para los integrantes de la policía cibernética con el fin de identificar a todos los transgresores en forma fehaciente durante sus actividades en la red y así combatir este tipo de delitos.

DECIMOPRIMERA.- Que los salarios de la policía cibernética sean más remuneradores, con el fin de que los miembros de la misma desempeñen mejor sus actividades y así evitar algún tipo de corrupción.

DECIMOSEGUNDA.- Integrar a los servicios periciales de las autoridades investigadoras, policías y órganos jurisdiccionales.

DECIMOTERCERA.- Obligar a los servidores públicos de las agencias investigadoras a que tomen cursos sobre delitos informáticos y como brindar atención a las personas que son víctimas de este tipo de conductas antisociales.

DECIMOCUARTA.- Que se asignen oficinas de orientación e información sobre medidas de seguridad al momento de navegar en Internet.

DECIMOQUINTA.- Elaborar campañas preventivas para hacer frente a la situación de la comisión de delitos informáticos, a través de comerciales televisivos, anuncios en las principales páginas de Internet, así como carteles en lugares públicos que permitan informar a la sociedad sobre el riesgo que se enfrenta ante los avances tecnológicos.

DECIMOSEXTA.- Esclarecer más el término del daño moral, por parte de los legisladores, a manera que los delincuentes informáticos reparen el daño en forma económica y al mismo tiempo brindar brigadas de información a la sociedad, ya que indirectamente también le causan un daño.

DECIMOSÉPTIMA.- Crear una institución social que a la vez sea reconocida por el Estado, en la cual se reclute a todos los delincuentes informáticos sentenciados, y como pena alternativa brinden sus conocimientos, con el fin de que sean utilizados correctamente por la policía cibernética y así tener mejores herramientas de combate ante las conductas delictivas que perturban la intimidad de los usuarios de Internet.

DECIMOCTAVA.- Que se implante en el sistema de educación a nivel secundaria y bachillerato, clases sobre los tipos de delitos que pueden ser cometidos por medio de las computadoras y el uso del Internet y que sanciones se aplican a los mismos, lo anterior con el fin de que se creé conciencia en los jóvenes y a su vez un temor sobre penalidades en caso de incurrir en este tipo de conductas delictivas.

DECIMONOVENA.- Movilizar a los políticos y otros aliados relevantes, las comunidades nacionales e internacionales, comprendidas las organizaciones intergubernamentales y no gubernamentales, para coadyuvar con los países internacionales, con el objetivo preciso de que entre éstos y México exista una cooperación en el combate y eliminación total de los diversos delitos informáticos, evitando que los delincuentes sigan delinquiendo libremente sin obtener una sanción respectiva.

VIGÉSIMA.- Formular nuevas medidas de apremio que sancionen las conductas ilícitas cometidas por adolescentes menores de edad mediante el uso indebido de equipos informáticos y la Internet, ya que actualmente estos individuos son los que más delinquen respecto a esta temática.

VIGÉSIMO PRIMERA.- Que se adicione en el código penal federal, respecto al Título Noveno Capítulo II, Acceso ilícito a sistemas y equipos de informática, un nuevo artículo el cual versará de la siguiente forma:

“Artículo 211 bis 8.- Al que sin autorización, obtenga, modifique, revele y utilice datos sensibles, entendiendo por éstos, aquellos que de forma más directa afectan a la intimidad personal, contenida en sistemas o equipos de informática, se le impondrán de de uno a cuatro años de prisión y de doscientos a seiscientos días de multa”.

“Artículo 211 bis 8 A.- La sanción señalada en el artículo anterior se aumentará en una tercera parte de la que corresponde y de 30 a doscientas jornadas de trabajo a favor de la comunidad cuando el autor ejerza violencia física, moral o psicológica a la víctima”.

VIGÉSIMO SEGUNDA.- Que se creen normas compatibles con otros países, con el firme objetivo de que entre uno y otro no hay ventaja o desventaja al momento de aplicar las sanciones respectivas.

VIGÉSIMO TERCERA.- Crear un Código penal federal que abarque la jurisdicción nacional, que no se tenga que estar aplicando un código por cada entidad federativa, según donde se haya cometido el delito, como un ejemplo real tenemos la Ley Federal del Trabajo, que es un solo ordenamiento legal aplicable para toda la república mexicana.

BIBLIOGRAFÍA

AMUCHATEGUI REQUENA, Irma Griselda. DERECHO PENAL (CURSOS PRIMERO Y SEGUNDO). Editorial HARLA, México, 1993. Pág. 418.

ANDRÉS CÁMPOLI, Gabriel. DELITOS INFORMÁTICOS EN LA LEGISLACIÓN MEXICANA. Editorial Instituto de Ciencias Penales, México 2007, Pág. 175.

CABEZUELO ARENAS, Ana Laura. DERECHO A LA INTIMIDAD. Editorial. TIRANT LO BLANCH, Valencia, 1998 Pág. 462.

CAMPUZANO TOMÈ, Herminia. VIDA PRIVADA Y DATOS PERSONALES. Editorial TECNOS, Madrid 2000, Pág. 179.

CARRANCA Y TRUJILLO, Raúl. DERECHO PENAL MEXICANO. PARTE GENERAL, TOMO I, 5ª, ED., Editorial, Antigua Librería Robredo, México, 1958.

CASTELLANOS, Fernando. LINEAMIENTOS ELEMENTALES DE DERECHO PENAL. Editorial PORRÚA, México, 2009, Pág. 363.

CUELLO CALÓN, Eugenio, DERECHO PENAL. TOMO I, 8ª Edición, Barcelona 1947

FARIÑAS MATÓN, Luís Mª. EL DERECHO A LA INTIMIDAD. Madrid, Trivium, 1983.

HERNÁNDEZ RICARDO Y DEL POZO LUZ MARÍA. INFORMÁTICA EN DERECHO. Editorial TRILLAS. Primera Edición 1992, Pág. 190.

HERRÁN ORTIZ, Ana Isabel. LA VIOLACIÓN DE LA INTIMIDAD EN LA PROTECCIÓN DE DATOS PERSONALES. Editorial DYKINSON, S.L, Madrid España, 1998, pag. 395.

JIMÉNEZ DE ASÚA, Luís. PRINCIPIOS DEL DERECHO PENAL. LA LEY Y EL DELITO, 3ª Edición, Editorial SUDAMERICANA, Buenos Aires, 1990.

LÓPEZ BETANCOURT, Eduardo. INTRODUCCIÓN AL DERECHO PENAL. Editorial PORRÚA, México 2003, Pág. 303.

LÓPEZ BETANCOURT, Eduardo. DELITOS EN PARTICULAR. TOMO UNO. Editorial PORRÚA, México 2004, Pág. 415.

M. FALCÓN, Enrique. ¿QUÉ ES LA INFORMÁTICA JURÍDICA?. Editorial ADELEDO-PERROT, Buenos Aires, 1992. Pág. 197.

MAGGIORE, Giuseppe, DERECHO PENAL I. Editorial, TEMIS, Bogotá, 1952.

MAGGIORE, Giuseppe, DERECHO PENAL, VOL. II, Editorial. TEMIS, Bogotá, 1989.

OCHOA OLVERA, Salvador. LA DEMANDA POR DAÑO MORAL. Editorial MUNDONUEVO, México 1991. Pág. 171.

PÉREZ LUÑO, Antonio Enrique. MANUAL DE INFORMÁTICA Y DERECHO. Editorial ARIEL, S.A, Barcelona, Edición Febrero 1996, Pág. 222.

REBOLLO DELGADO, Lucrecio. EI DERECHO FUNDAMENTAL A LA INTIMIDAD. Editorial DYKINSON, Madrid España, 2000, Pág. 299.

RIVERA SILVA, Manuel. EL PROCEDIMIENTO PENAL. Editorial PORRÚA, México, 2007, Pág. 397.

RUEDA DEL VALLE, Doraye. EL DERECHO A LA INTIMIDAD Y LA GRAFOLOGÍA. Editorial PORRÚA, México 2007, Pág. 146.

RUIZ MIGUEL, Carlos. LA CONFIGURACIÓN CONSTITUCIONAL DEL DERECHO A LA INTIMIDAD. Madrid, Tecnos, 1995.

SANTOS PASCUAL, Efrén. PROTECCIÓN DE DATOS PERSONALES. MANUAL PRACTICO PARA EMPRESAS. Editorial FUNDACIÓN CONFEMETAL, España, Madrid, 2005.

SILVA SILVA, Jorge Alberto. DERECHO PROCESAL PENAL. Colección Textos Jurídicos Universitarios, Editorial HARLA, México 1990, Pág. 826.

TÉLLEZ VALDÉS, Julio. DERECHO INFORMÁTICO. Editorial MC GRAW HILL, Tercera Edición, México 2004, Pág. 514.

VILLANUEVA, Ernesto, DERECHO A LA INFORMACIÓN, Editorial Porrúa, México 2006, Pág. 301 a 312

WARREN, Samuel y **BRANDEIS**, Lous. EL DERECHO A LA INTIMIDAD. Editorial. CIVITAS, S.A., Madrid, España, 1995, Pág. 73.

ZAMORA JIMÉNEZ, Arturo. CUERPO DEL DELITO Y TIPO PENAL. Editorial ÁNGEL EDITOR, México 2000. Pág. 191.

DICCIONARIOS

DE PINA VARA, Rafael. Diccionario de Derecho. Editorial PORRÚA, México 2004, Pág. 525.

SECO REYMUNDO, Manuel. DICCIONARIO DE DUDAS Y DIFICULTADES DE LA LENGUA ESPAÑOLA. Editorial, ESPASA CALPE, Madrid, 1992.

PÁGINAS DE INTERNET

<http://www.monografias.com>
<http://www.misrespuesta.com>
<http://www.ssp.gob.mx>
<http://www.mastermagazine.com>
<http://www.definicionabc.com>
<http://www.politicadigital.com.mx>
<http://www.cddhcu.gob.mx>
<http://www.juridicas.unam.mx>
<http://www.cronica.com.mx>
<http://www.wikipedia.org>
<http://www.colex-data.es>

LEGISLACIÓN

- CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.
- CÓDIGO PENAL FEDERAL.
- LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL.
- LEY FEDERAL DEL DERECHO DE AUTOR (PROTECCIÓN DE LOS PROGRAMAS DE COMPUTACIÓN).
- LEY DE JUSTICIA PARA ADOLESCENTES PARA EL DISTRITO FEDERAL.