DELITOS INFORMATICOS

CONCEPTO Y FUNCION DEL DERECHO PENAL

Si bien el Derecho es uno solo, se lo divide en ramas para facilitar su estudio y aplicación: laboral (regula relaciones entre trabajadores y empleados), comercial (regula las relaciones en las que interviene por lo menos un comerciante), civil(relaciones de familia, contratos, obligaciones etc), del transporte, minero, etc.

El Derecho Penal es una de las ramas del derecho, y podemos definirlo como el conjunto de normas que describen conductas y frente a la realización de estas, aplica penas que generalmente consiste en la privación de la libertad, como por ejemplo, "El que matare a otro deberá cumplir una pena de ocho a veinticinco años de prisión".

El Derecho Penal funciona como un instrumento del Estado ya que por su intermedio la sociedad ejerce un control sobre los individuos de "comportamiento desviado", utilizando el castigo, aplicado de manera formal, fundado racionalmente. Asimismo, cumple una función de mantenimiento del orden establecido por el Estado, reparadora del equilibrio de un sistema social perturbado por el delito. El delito se define como aquellos actos que ofenden los bienes jurídicos de una sociedad (orden público, salud pública, etc.) o de los individuos que la integran.(vida, honor, libertad, propiedad etc).

La aplicación del Derecho Penal la hacen los jueces frente al caso concreto, y esa aplicación debe ser racional, penar conductas y no personalidades. La aplicación racional del mismo se logra preguntándose si en el caso concreto el hecho cometido es delito, y cual es la pena aplicable tomando la escala que marque el código (en el ejemplo, la escala sería de ocho a veinticino) y los antecedentes del declarado responsable.

CARACTERES DEL DERECHO PENAL

1.- Predominantemente público

El Derecho Penal ha sido reconocido como un orden normativo de carácter público, debido a la eminente intervención del Estado en su realización. En este sentido, podría señalarse que el Derecho Penal constituye la máxima expresión de la soberanía jurídica de un Estado que es quien tiene el poder punitivo (poder de imponer y aplicar la pena). El carácter público del derecho penal se manifiesta, precisamente, por la potestad estatal de imponer la pena.

Así por ejemplo, cuando la policía o los jueces penales toman conocimiento de la posible comisión de un delito (por ejemplo, a través de la denuncia de un ciudadano), se pone en marcha un circuito destinado a investigar, determinar las culpabilidades, y aplicar las penas correspondientes. Es una obligación para el Estado

Sin embargo, esta característica no es total, ya que hay delitos que pertenecen a la intimidad de las personas y para poner en marcha el aparato punitivo estatal requiere la denuncia del ofendido o víctima del delito. Son los llamados delitos de acción privada(abuso sexual, por ejemplo).

2- Sancionatorio

El Derecho Penal impone sus sanciones extremas cuando el juego de las disposiciones del restante derecho resultan insuficientes o impotentes para enfrentar una situación dada. Esto debe entenderse en el sentido de que el derecho penal protege bienes que otras ramas jurídicas también resguardan. Sucede que su intervención se produce cuando determinados hechos rebasan las soluciones que los derechos no penales poseen al respecto.

Si examinamos el sistema de sanciones que puede aplicar el derecho en general, advertiremos que el derecho penal tiene asignado una muy exclusiva e intransferible: la pena.

La pena es un castigo, un mal que se irroga a quien debe padecerlo, porque el derecho penal protege bienes jurídicos fundamentales del individuo y de la sociedad: la vida, la integridad física, libertad, honor, propiedad, fe pública, incolumidad de los poderes del estado, etc.

Es cierto que algunos de estos bienes pueden resultar lesionados y encontrar solución por vía de otro tipo de sanciones. Por ejemplo: el derecho de propiedad puede lesionarse por incumplimiento en el otorgamiento de la correspondiente escritura, etc. Pero estos hechos encuentran adecuada respuesta en el derecho civil o comercial, pues todo se reduce a una sanción de restitución o indemnización, y la comunidad absorbe silenciosamente esos conflictos.

No ocurre lo mismo cuando se produce un homicidio, lesiones, robos, atentados a la seguridad pública, etc, Como estos hechos rebasan las posibilidades de las otras sanciones, corresponde al derecho penal por intermedio de la pena, intervenir no para compensar, sino para ejemplarizar mediante el castigo de la pena. Ello porque para la sociedad, representan eventos intolerables que la conmueven profunda y públicamente.

DERECHO PENAL:

- **DEFINICION:**
- es una rama del Derecho que consiste en un conjunto de normas que describen conductas y frente a la realización de estas se aplican penas que generalmente consisten en la privación de la libertad

- **CARACTERES:**
- 1) **Predominantemente público**: el Estado es quien tiene el poder punitivo (poder de imponer y aplicar penas)
- 2) **Sancionatorio**: Impone sanciones

ESTRUCTURA DE LA LEY PENAL

Las leyes penales contienen dos partes:

a) El Precepto: que prohíbe o manda algún comportamiento.
b) La Sanción: que se establece por el incumplimiento del precepto.

Por sobre el ordenamiento penal está el ordenamiento constitucional (Constitución Nacional), que impone los límites o condiciones bajo las cuales el Estado puede ejercer el poder sancionador. Así:

1) Penas proporcionales y que respeten la dignidad humana: Nuestra Constitución establece el principio a la dignidad humana, por lo que no podría aplicarse a los delincuentes penas degradantes o inhumanas, torturas, etc.

Las penas deben guardar proporcionalidad con el delito cometido y con la responsabilidad del condenado.

2) Potestad legisferante del Estado Nacional: Solamente el Estado dicta leyes penales mediante el órgano correspondiente: Congreso Nacional.(art. 75° inc 12 de la CN). La facultad de este órgano legislativo es intransferible e inconfundible respecto de los otros dos poderes del Estado. Su violación es punible (CN art. 29°).

3) Ley previa o principio de legalidad: La CN ha establecido expresas exigencias para la aplicación de la ley penal. El principio fundamental está consagrado en el artículo 18 CN : Ningún habitante de la Nación puede ser penado sin juicio previo fundado en la ley anterior al hecho del proceso. Ello viene del viejo dogma: "Nullum crime nulla poena sine praevia lege", es decir: no hay crimen ni pena sin ley previa.

La función fundamental del principio de reserva consiste en garantizar la libertad del ciudadano contra toda pretensión punitiva arbitraria. La garantía significa que solo habrá pena por un hecho si previamente existe la ley que lo dispone.

La afirmación constitucional de que lo previamente determinado como "delito y pena" será castigado, implica reconocer que un vasto mundo de acciones humanas no está prohibido. Por eso, la CN coronando el principio de reserva señala que en su artículo 19 en que condiciones las acciones humanas quedan exentas de la autoridad de los magistrados y además que solamente la ley manda o prohíbe ciertos actos.

El principio de legalidad impone sus exigencias no solo al juez que aplica la ley, sino también al Poder Legislativo que la dicta, así, el Congreso de la Nación tiene la exigencia de reducir al máximo la posibilidad de decisión personal de los jueces en la configuración concreta del hecho que se prohíbe. Debe dictar todos los presupuestos que condicionan la pena y determinar la especie de pena, su duración mínima y máxima.

4.- Prohibición de Analogía

Se entiende por analogía la aplicación de la ley a un caso similar al legislado, pero no comprendido en su texto. En el sistema jurídico argentino, la analogía rige en amplios sectores (derecho civil, derecho comercial, etc). En estos derechos, la ley obliga expresa e imperativamente al magistrado a aplicar los principios de leyes análogas, e incluso lo principios generales del derecho porque no pueden dejar sin decisión una cuestión so pretexto de oscuridad, silencio o insuficiencia de las leyes.

Ello porque las controversias de derecho privado siempre deben tener una respuesta del órgano judicial. Sus razones residen en la necesidad de encontrar alguna solución judicial a las relaciones jurídicas planteadas entre particulares; porque de otro modo, la convivencia social sería intolerable por la inseguridad jurídica en que quedarían derechos y deberes de la comunidad.

En relación al Derecho Penal, si bien la CN no contiene un precepto expreso que prohíba su aplicación analógica, ello surge de la interpretación sistemática de las disposiciones de la CN. Así, el art. 18° de la CN, al exigir que el hecho esté contemplado en ley anterior para ser castigado, y el art. 19 CN al decidir que nadie está obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe, coloca un valladar importante, casi decisivo a todo intento de interpretación analógica.

Entonces, solo es delictivo lo que está prefigurado legal y estrictamente.

5.-Irretroactividad de la Ley Penal : La ley aplicable al delito desde el punto de vista temporal es la ley vigente al momento de la comisión del hecho punible. Se encuentra prohibida la aplicación retroactiva de la ley penal, o sea, aplicarle a un hecho punible, cuando se lo está por juzgar, una ley que no estaba vigente al momento de su comisión.

Excepciones a este principio: el principio de la irretroactividad de la ley sufre una excepción respecto de las leyes penales posteriores al momento de la comisión del delito, pero mas favorables al acusado.

CONCLUSIONES

.*En el Estado democrático de derecho, la comisión de un delito no determina la pérdida de dignidad de una persona.
*Debe respetarse el principio de que para ser penado, debe haber una ley anterior que describa ese hecho como punible.
La determinación legal o límites legales a la punibilidad son:

- la prohibición de la analogía
- la prohibición de la aplicación retroactiva de la ley penal

LEY PENAL

- **CONSTA DE DOS PARTES** :
  - 1) **EL PRECEPTO**:
  - Prohíbe o manda algún comportamiento
  - 2) **SANCION**:
  - Establece una sanción por el incumplimiento
  - Por ej.: *el que matare, prisión de 8 a 25 años*

LEY PENAL

- **CARACTERES**
  - 1**) Penas proporcionadas a la dignidad humana**: no pueden aplicarse penas degradantes o inhumanas o torturas, etc.
  - 2**) Potestad legisferante del Estado**: solamente el Estado dicta leyes penales mediante el órgano correspondiente: el Congreso de la Nación (art. 75 inc. 12 CN)
  - 3) **Ley previa o principio de legalidad**: "no hay crimen ni pena sin ley previa (art. 18 CN)
  - 4) **Prohibición de analogia**: solo se pena las conductas descriptas en la ley penal (art. 18 y 19 CN)
  - 5) **Irretroactividad de la ley penal**: se aplica la ley vigente al momento de la comisión del hecho punible salvo que la ley posterior sea favorable al acusado

---

TEORIA DEL DELITO

Para saber si frente a un caso concreto o hecho de la realidad, estamos en presencia de un delito, debemos aplicar la teoría del delito, las que nos proporciona un camino lógico para ello.

Estudia que condiciones deben darse en una conducta para que sea considerada un delito o ilícito penal, y se estructura en un método de análisis de diversos niveles. Cada uno de estos niveles presupone el anterior, y todos tienen la facilidad de ir descartando las causas

que impedirían la aplicación de una pena, y comprobando si se dan las condiciones de aplicación. De esta forma, se respeta el principio de legalidad.

En general, se la teoría del delito lo define como ***"toda acción típicamente antijurídica y culpable."*** (Carlos Fontan Balestra, Derecho Penal, Introducción y Parte General, Abeledo Perrot).

Analizamos:

1.-Acción

El delito parte de una acción o conducta humana, que puede realizarse por acción propiamente dicha (actividad –hacer algo) u omisión (inactividad –no hacer). Ejemplo: un ser humano puede matar a alguien por acción (envenenándolo) o por omisión (no alimentarlo cuando su alimentación depende de él).

En una conducta la acción queda eliminada (y por lo tanto no habrá delito) cuando:

- el sujeto actuó por fuerza física irresistible: es actuado o usado como instrumento, ejemplo, cuando usando fuerza física sobre sus manos se colocan sus impresiones digitales en un documento.
- Actos reflejos: Cuando la conducta es consecuencia de movimiento mecánico externo, ejemplo, el puntapié que destruye un objeto, que se origina al golpearse la rodilla del sujeto.
- Estado de inconsciencia absoluto: Ej: sonambulismo.

2.- Típica:

No cualquier acción es susceptible de pena. Para ello, la Acción (como acción u omisión) debe estar previamente descripta por la ley penal como un "tipo penal". Llamamos tipos a estos elementos de la ley penal que sirven para individualizar la conducta que se prohibe.

.

Cuando el legislador traza la parte especial de un código, se fija como tarea la descripción, lo mas precisamente posible de la materia incriminable.

A modo de ejemplo, vamos a analizar los artículos 79°, 80° y 81° del Código Penal.

Art. 79°: "Se aplicará prisión o reclusión de 8 a 25 años, al que matare a otro, siempre que en este Código no se estableciere otra pena"

Art. 80°: "Se impondrá reclusión perpetua o prisión perpetua pudiendo aplicarse lo dispuesto en el artículo 52°, al que matare:

1°) a su ascendiente, descendiente o cónyuge, sabiendo que lo son

2°) con ensañamiento, alevosía, veneno…"

Art. 81°: "Se impondrá reclusión de 3 a seis años, o prisión de 1 a 3 años:

1°) al que matare a otro, encontrándose en un estado de emoción violenta…

2°) al que, con el propósito de causar un daño en el cuerpo o en la salud, produjere la muerte de alguna persona, cuando el medio empleado no debía razonablemente ocasionar la muerte."

Vemos que el art. 79°) describe el tipo básico, el "homicidio simple", mientras que el artículo 80° describe tipos de "homicidio agravado", y el 81°, tipos de "homicidio atenuado".

Entonces, el legislador, sobre ese tipo simple que ha creado, puede crear otros, y así darle una pena mas grave cuando la victima del homicidio es un pariente "homicidio

agravado por el vínculo", o puede darle una pena mas leve cuando la muerte del tercero es obra de un estado emocional particular del autor y disminuir la pena. (emoción violenta).De este modo, se va elaborando una familia de tipos hasta agotar lo que considera los hechos incriminables dignos de pena.

Cuando una conducta se adecua a algunos de los tipos legales decimos que se trata de una conducta típica o que la conducta presenta la característica de tipicidad.

3.- Antijurídica

Para que haya delito no será suficiente con que la conducta presente la característica de tipicidad, sino que se requerirá que presente también un segundo carácter específico, la antijuridicidad, que implica que la conducta es contraria al derecho.

Una acción típica es antijurídica cuando no funciona una causal de justificación. Las causas de justificación son:
a) Estado de necesidad: cuando se cometió la conducta para evitar un mal mayor grave e inminente. (aborto por peligro en la salud de la madre)
b) cumplimiento de la ley: Ej. Las lesiones producidas mientras se practica un deporte, no son delito, puesto que los deportes son prácticas avaladas y permitidas por la ley y además sus practicantes brindan su consentimiento para ello.
c) legítima defensa propia y de terceros. Ej: lo mato porque era la única forma de evitar que me mate.

4.- Imputabilidad

Para que haya delito, la conducta típica y antijurídica debe ser también imputable o atribuible al autor del hecho. Ello requiere que el autor comprenda la criminalidad del acto, que tenga las suficientes facultades mentales o la madurez necesaria para comprender que lo que hizo estaba mal.

Las causas que excluyen la imputabilidad son:
-insuficiencia de las facultades
-alteración morbosa de las mismas
-grave perturbación de la conciencia
-minoridad

5.- Culpabilidad

Una conducta típica y antijurídica es culpable cuando al autor le es moralmente reprochable la realización de la conducta prohibida por la ley. Para que haya culpabilidad, el autor debe haber obrado con dolo (intención) o culpa (negligencia).

El autor actúa con dolo cuando ha querido la realización del hecho típico. Hay coincidencia entre lo que el autor hizo y lo que el autor quiso. El autor actúa con culpa cuando no ha querido la realización del hecho típico. El resultado es producto de su negligencia, del descuido o incumplimiento de su deber de cuidado.

Los delitos dolosos se caracterizan por la coincidencia entre lo que el autor hace y lo que quiere. Hay en el sujeto voluntad de causar ese resultado. El dolo puede ser directo (el autor puede representarse las consecuencias de sus actos como aceptadas y necesarias.) o eventual (el autor no considera ni desea el resultado pero igual decide su fin extratípico.

Acepta la acción con el peligro posible y probable, aprobando un eventual resultado no querido ni propuesto).

En los delitos con dolo directo, el resultado se quiere directamente, en el dolo eventual, se lo acepta como posibilidad.

En los delitos culposos, no hay representación de ese resultado, se produce por negligencia o descuido del autor.

CONCLUSION

Reunidas estas condiciones, la realización de la conducta descripta en el tipo pasa a la categoría de delito. Resumiendo lo expuesto precedentemente para la teoría penal general, los elementos integrantes del delito son:

- Un acto humano consistente en una acción u omisión.
- Dicho acto humano ha de ser antijurídico, es decir, debe lesionar o poner en peligro un interés jurídicamente protegido.
- Debe ser un acto típico, es decir, tiene que corresponder a un tipo penal definido por la ley y sancionado con una pena.
- El acto ha de ser culpable, es decir, imputable a dolo (intención) o culpa (negligencia). Una acción es imputable o culpable cuando puede ponerse a cargo de una determinada persona.

Resumiendo lo antedicho, un delito es una acción típica, antijurídica y culpable realizada por un ser humano y sancionada por una pena.

Aplicando el concepto de delito al Derecho Informático, se define al delito informático como:"*Toda acción (acción u omisión) culpable realizada por un ser humano, tipificada por ley, que se realiza en el entorno informático o mediante elementos informáticos, y está sancionado con una pena."*

En esta definición debe destacarse que el elemento informático puede intervenir como medio o como objeto. Interviene como medio cuando se utilizan elementos informáticos para realizar la acción delictiva (por ejemplo, utilizar una computadora para falsificar dinero).Interviene como objeto cuando la acción delictiva tiene como fin el daño a un sistema informático(por ejemplo, cuando un virus borra información de una computadora).

DELITO

- DEFINICION:
- ***"toda acción típica antijurídica y culpable"***

- ELEMENTOS:
- **Acción:** una conducta humana
- **Típica:** descripta en la ley penal
- **Antijurídica:** la conducta es contraria al derecho
- **Imputabilidad:** que sea atribuible al autor del hecho
- **Culpabilidad:** que el autor del hecho haya obrado con dolo o culpa

DELITOS INFORMATICOS EN EL CODIGO PENAL SEGÚN LA REFORMA DE LA LEY 26388.

En el año 2008 se dictó la ley 26388 de Delitos Informáticos

Ahora bien tengamos en cuenta que nuestra legislación penal tiene ya sus largos años, e indudablemente no contempló las nuevas tecnologías como objetos de delitos o como medios para la comisión de delitos.

Así, tristemente hemos podido ver como algunos de nuestros tribunales han sobreseído a personas que, por ejemplo, violaron casillas personales de correo electrónico. Estos tribunales sabían que la conducta incriminada en nuestro Código Penal era violar la correspondencia postal, que sería la conducta "X". Violar un correo electrónico no es una conducta "X", pues el correo electrónico es algo distinto al correo postal, y no se hallaba expresamente previsto en la norma.

Uno podrá pensar, ¿pero acaso a los fines y efecto jurídicos, el correo postal y el email, no son la misma cosa? ¿no podríamos extender las normas de protección del correo tradicional sobre el electrónico sin necesidad de reformar el Código Penal?. Pues en principio NO. Hacer eso implicaría la realización de una "analogía" prohibida en el derecho penal, extenderíamos el tipo penal a cuestiones que no contempla desde su texto, atentando contra las garantías constitucionales del debido proceso.

Así, un gran número de conductas decididamente nocivas, como pueden ser los ataques DoS, el fraude informático, el *hackeo* de sistemas, entre muchas otras, debían ser declaradas atípicas por nuestros jueces, al encontrarse desprovistos de "tipos penales" aplicables a esas conductas.

Bien, esta ley lo que nos trae es una serie de "tipos penales" que van a venir a encajar con ciertas conductas dirigidas contra o mediante elementos informáticos. Así nuestro jueces podrán decir que, realizado el acto "Y", y siendo "Y" una conducta expresamente contemplada por el Código, corresponde a su autor la pena de ...

La técnica de la ley

La nueva ley, no conforma un cuerpo legal autónomo, sino que incorpora un conjunto de modificaciones al Código Penal.

En general no crea nuevos delitos sino que incorpora nuevos conceptos a categorías ya existentes, ensanchando el tipo penal, y relevando así la necesidad de "forzar" las interpretaciones para sostener que un tipo penal determinado incluye cierta conducta aún cuando no la describa literalmente.

Principales cambios

I.- Asimilando conceptos:

Aún cundo pueda parecer elemental, la ley incorpora una serie de conceptos, cuya ausencia determinaba la declaración de atipicidad sobre muchos presuntos "delitos". Dice la ley:

El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

La Ley 26.388 modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos en el Código Penal, estas figuras son:

- **1). Pornografía infantil por Internet u otros medios electrónicos (art. 128 CP)**
- **2) Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º del CP)**
- **3) Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 152, párrafo 2º del CP)**
- **4) Acceso a un sistema o dato informático (artículo 153 bis CP);**
- **5) Publicación indebida de una comunicación electrónica (art. 155 CP)**
- **6) Revelación de Secretos**
- **7) Acceso ilegítimo a un banco de datos personales (artículo 157 bis, párrafo 1º CP);**
- **8) Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP);**
- **9)Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP, anteriormente regulados en el artículo 117 bis, párrao 1º, incorporado por la Ley de Habeas Data);**
- **10)Fraude informático (artículo 173, inc 16 CP)**
- **11)Daño o sabotaje informático (artículos 183 y 184 incisos 5º y 6º CP)**
- **12) Interrupción de las comunicaciones**

Ahora bien, comenzamos el desarrollo de cada una de los delitos mencionados:

DELITOS INFORMATICOS INCORPORADOS POR LA LEY 26388:

- **<u>Pornografía infantil por Internet u otros medios electrónicos (art. 128 CP)</u>**

Artículo 128 del Código Penal:

" Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales

explicitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explicitas en que participaren dichos menores . Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años."

Como la norma hace referencia a "cualquier medio" este delito puede cometerse tanto a través de redes informáticas como en formas tradicionales, tales como distribución de fotografías, revistas, videocasetes, dvds, etc., en lugares determinados.
La conducta tipificada por la norma consiste en: producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir, imágenes de pornografía infantil.
La ley define a la pornografía infantil como "toda representación de un menor de dieciocho años dedicado a actividades sexuales explicitas o toda representación de sus partes genitales con fines predominantemente sexuales". Se trata de una representación por lo que cualquier imagen, fotografía, dibujo o video, que cumpla con los requisitos enunciados podrá constituir el objeto del delito.

- **Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º del CP)**
- **Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 152, párrafo 2º del CP)**

La nueva normativa tipifica como delitos la violación, apoderamiento y desvío de comunicación electrónica y la publicación de una comunicación electrónica.

Los nuevos delitos contra la privacidad constituyen la reforma más importante de la ley 26388. Surgieron por la necesidad de penalizar las frecuentes violaciones a la privacidad del correo electrónico y de otras formas de comunicación

Se trata de un delito contra la libertad. La libertad pertenece a la clase de derechos fundamentales denominados derechos de la personalidad o inherente a la personalidad, como el derecho a a conservación de la propia existencia, a la integridad moral y física.

La privacidad ya estaba amparada en el Código Penal en diversos delitos, tales como el de violación de domicilio, el allanamiento ilegal, la violación de secretos y la de correspondencia. Ahora bien no cabe duda de que las nuevas tecnologías han aumentado los riesgos y peligros para el derecho a la privacidad.

El art. 153 del Código Penal expresa: " Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica , una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido, o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho y otro papel privado, aunque no esté cerrado, o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le este dirigida". En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido." La pena será de prisión de un mes a un año si el autor además comuncare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica ".Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

El objeto del delito informático es la comunicación electrónica. Ahora bien ¿que es una comunicación electrónica? Una comunicación electrónica es un mensaje enviado por un individuo a otra persona por medio de un sistema electrónico. Este concepto es tan amplio que se incluyen el clásico mensaje de correo electrónico, un chat, un fax, una llamada a través de VOIP, o un mensaje de texto enviado a través de un celular. La correspondencia o comunicación electrónica es tal, tanto mientras está en tránsito como cuando queda almacenada en un casillero de mensajes, bandeja de entrada, contestador automático o voicemail.

Sin embargo la comunicación electrónica debe interpretarse de acuerdo al desarrollo actual de las comunicaciones. Ya que en la actualidad las comunicaciones no ocurren solo entre dos personas sino también entre varias e incluso con máquinas. Por ejemplo el banco puede enviar un resumen de cuenta a la casilla de correo electrónico del cliente, un servidor comunica al usuario si el mensaje anterior que envió llegó o no a destino. Se trata en todos los casos de comunicaciones electrónicas La relación con numerosas empresas y sistemas está automatizada a través de ordenadores y con ellos también hay comunicación.

La protección se extiende a los papeles privados, o sea los que estando en la esfera de reserva de alguien, contienen una expresión escrita de su pensamiento, aunque no esté destinada a ser comunicada a un interlocutor. La naturaleza de papel privado no se altera porque su soporte sea magnético o informático.

Acciones penadas por la ley

I.- Violación apoderamiento y desvío de comunicación electrónica

a) Apertura o acceso a correspondencia

La acción de acceso o apertura es el acto típico mediante el cual se viola la reserva de la correspondencia. Consiste en abrir o acceder, indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido. Este acceso o apertura indebida puede tener lugar en diversos puntos de la red y de ello dependerá, entonces como se materializa. Por ejemplo ingresar a la cuenta de correo de una persona y revisar en su carpeta de mensajes enviados un correo que no le estaba dirigido, o en la de mensajes recibidos y acceder a dicho contenido. También se comete delito frente a la acción de revisar un teléfono móvil ajeno, abriendo el registro de mensajes (tipo de texto SMS o multimedia MMS) recibidos por el titular del aparato, para entrar a ellos, o si se abre un archivo que constituye el log de una comunicación que tuvo lugar por vía chat u otro servicio de mensajería instantánea(que permita gravar la conversación que tiene lugar).

b) Apoderamiento de una comunicación electrónica y de papeles privados

Otra acción típica prevista por el art. 153, consiste en apoderarse indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado aunque no esté cerrado. Tratándose de una comunicación electrónica (que incluye el correo electrónico) como objeto del delito, este apoderamiento de correspondencia debe ser interpretado en consonancia con el medio digital: entonces es posible apoderarse de un correo (por ej. mediante su copia) sin desapoderar a la víctima. Lo mismo puede decirse de un papel privado almacenado en un soporte informático. Si una persona lo abre y conoce su contenido incurre en el delito mencionado y si además de copiarlo destruye el original

podrá haber concurso con el de daño informático (art. 183, párrafo. 2 Cod. Penal). Ello es así puesto que en nuestro derecho el concepto de documento prescinde del soporte de papel y se tiene por escrito, cualquiera sea el medio en el cual se encuentre almacenado (Art. 6, Ley de Firma Digital y art. 77 Cod. Penal). Por lo tanto un papel privado puede estar almacenado en un ordenador, en una cuenta de correo electrónico, en un teléfono celular o dispositivo inteligente tales como una blackberry o palm.

c) Desvío o supresión de comunicaciones electrónicas.

El delito consiste en impedir que la correspondencia en curso y no dirigida al autor del hecho llegue a su destinatario, sea sacándola de su curso (supresión) o cambiando éste (desvío). La correspondencia está en curso mientras el destinatario final no la haya bajado del servidor y no la haya abierto, es decir no ha tomado conocimiento de ella. Incluso la comunicación puede haber llegado efectivamente a su casilla, pero aquel aún no la ha revisado.

d) Interceptación de comunicaciones electrónicas

La interceptación de comunicaciones electrónicas se refiere a las escuchas telefónicas ilegales. La acción típica consiste ahora en interceptar o captar comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

e) Comunicación o publicación ilegítima

En este caso el autor de la publicación ilegítima es al mismo tiempo el autor de la apertura o del apoderamiento de la comunicación electrónica.

- **Acceso a un sistema o dato informático (artículo 153 bis CP);**

El art. 153 bis del Código Penal expresa: Será reprimido con prisión de quince días a seis meses, sino resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

Mediante esta norma se ampara la reserva, la confidencialidad y el derecho a la privacidad del titular del sistema y del dato informático.

La acción punible consiste en acceder por cualquier medio a un sistema o dato informático de acceso restringido. La razón de esta prohibición es que la entrada no autorizada suele ser la antesala para la comisión de otros delitos como la estafa, el daño, la sustracción de datos personales, de claves o de secretos comerciales. Es en esa inteligencia que el legislador estableció que solo será de aplicación esta figura "si no resultare un delito más severamente penado".

El acceso al sistema o dato informático debe ser restringido es decir que se trata de un sistema o dato que tiene alguna medida de seguridad que impide el libre ingreso, caracterizando como punible la acción de entrar o acceder sin autorización, ya sea violando las barreras de protección establecidas (tecnológicas, físicas, etc.), sea por no estar

autorizado a acceder, o bien por haberse revocado los permisos conferidos o modificado las condiciones que habilitaban el acceso. El mencionado art. agrava la pena si el ataque o acceso se produce a un sistema o dato de un organismo público o estatal, como por ejemplo el caso de la página web de los padrones electorales.

Esta figura se comete simulando ser un usuario legítimo, mediante el acceso utilizando nombre de usuario y contraseña de un tercero; o accediendo a un sistema, dato, servidor, archivo informático, etc., sin contar con autorización; o excediendo los límites conferidos (tal el caso de un usuario autorizado a ver ciertos datos pero que usando el acceso legítimo lo transforma en ilegítimo); o aprovechando deficiencias de los sistemas de seguridad establecidos.

Podemos sintetizar, entonces, que esta figura penal de acceso indebido a un sistema o banco de datos requiere que se den al menos tres condiciones**:** (1) que no exista autorización para ingresar; (2) que se vulneren medidas de seguridad colocadas para impedir el acceso no autorizado o la modificación; y (3) que sea realizado con deliberada intención, es decir, "a sabiendas".

Se excluye de esta figura la comisión de un daño para la configuración del delito. Esto es, no es necesario que se produzca una modificación o alteración al sistema o dato para que exista delito, sino que la mera intrusión sin autorización configura una conducta indebida (típica).

- **Publicación indebida de una comunicación electrónica** (art. 155 CP)

El artículo 155 de Código Penal reprime con multa al que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. La multa prevista varía entre $1500 a $100.000. En un segundo párrafo el art. 155 del Cödigo Penal expresa que está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

Así como constituye delito violar la privacidad de una correspondencia mediante su acceso o sustracción, del mismo modo lo es publicar el contenido de una carta o correo electrónico que debe quedar en de la esfera íntima de una persona y no ser divulgada.

Por publicar cabe entender el dar a conocer a terceros por cualquier forma , ya sea reenviando un correo electrónico a un número indeterminado de personas, poniéndolo online en un sitio web o simplemente comentándolo verbalmente a terceros.

- **Revelación de Secretos**
- **Acceso ilegítimo a un banco de datos personales (artículo 157 bis, párrafo 1º CP);**
-
- **Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP);**
- **Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP, anteriormente regulados en el artículo 117 bis, párrao 1º, incorporado por la Ley de Habeas Data);**

Revelación de secretos

"Artículo 157.- Será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos" .

El autor del delito en este caso solo puede ser un funcionario público que tenga la obligación de guardar secreto. La acción típica consiste en revelar hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

Delitos relacionados con la protección de datos personales

Las tecnologías de la información han facilitado el manejo y recopilación de datos personales como nunca antes ha sucedido en la historia de la humanidad. Los bancos de datos personales conforman un vasto universo de información, donde la mayor parte de las actividades cotidianas de las personas quedan rutinariamente registradas. En las últimas tres décadas estas tecnologías han evolucionado y se han expandido tanto en lo que hace al tratamiento de datos personales que fue necesario aprobar normas especiales para regular este fenómeno.

La acumulación de datos personales en ordenadores ha llevado a reformular la concepción clásica del derecho a la privacidad. Tradicionalmente éste fue definido en forma negativa, como un derecho a excluir a terceros de la zona de reserva de una persona. Con el desarrollo de bancos de datos el derecho a la privacidad implica también el derecho de acceso, corrección y rectificación de esos datos personales. Es el derecho a controlar la información personal como una nueva dimensión del tradicional concepto del derecho a la privacidad.

La solución para amparar al individuo frente a los cambios radicales que importa la nueva tecnología fue adoptar leyes de protección de datos personales. El derecho a la protección de tales datos es un conjunto de reglas que guía a compañías y organizaciones en el uso que se hace de la información personal, es decir, la que identifica individuos o personas jurídicas.

La ley 25326 introdujo, entonces la protección de datos personales en nuestro derecho y a la vez reglamentó la acción constitucional de habeas data, creando dos nuevos tipos penales relacionados con la información personal: el acceso ilegítimo a bancos de datos personales y la inserción de datos falsos.

La reforma de la ley 26388, modificó el art. 157 bis del Código Penal de la siguiente manera.

"Artículo 157 Bis.- Será reprimido con la pena de prisión de un mes a dos años el que: 1.-A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2.-Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.3-. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años."

1.- Acceso no autorizado a un banco de datos personales

2.-Proporcionar o revelar información registrada en un banco de datos

3.- Inserción de datos en un banco de datos

Acceso no autorizado a un banco de datos: La acción típica consiste en acceder a un banco de datos personales. A sabiendas, (dolo) el acceso debe ser ilegítimo, es decir sin consentimiento. Los sistemas de confidencialidad y seguridad de datos son los que habrá adoptado oportunamente el responsable del tratamiento o el dueño de la base de datos. En general puede ser cualquier sistema de seguridad y no requiere que sean de determinada calidad o nivel.

La diferencia entre el art. 157 bis, con el 153 bis del Código Penal es que en el primero el acceso es a un banco de datos personales y en el segundo debe tratarse de un sistema o datos informáticos . Si se accede a un banco de datos que no tiene datos personales (por ej. que contiene datos estadísticos) no debe aplicarse el art. 157 bis del CP sino el 153 bis CP.

Proporcionar información o revelar información registrada en un banco de datos: Para comprender en que situaciones puede aplicarse este tipo penal, hay que diferenciar las bases de datos de uso público de la sujetas a confidencialidad. La norma solo sanciona al que proporciona o revela a otro, información registrada en un archivo o en un banco de datos personales sujeto a dos condiciones: a) que la ley establezca el secreto (del contenido de ese banco de datos) y b) que tal revelación o dación de información sea en forma ilegítima.

La ley de protección de datos personales (25326) establece la obligación de secreto en el art. 10. Según esa norma el deber de secreto o confidencialidad recae no solo sobre el responsable sino sobre todas las personas que intervengan en cualquier fase del tratamiento de datos personales. Esto incluye a los propios usuarios, a terceros, que tratan temporariamente estos datos o los que la consultan con una finalidad determinada.

Inserción de datos en un banco de datos: Se reprime la inserción de datos, sean estos falsos o verdaderos, en un archivo de datos personales. La inserción de datos verdaderos no obsta a que pueda lesionarse la privacidad de una persona, (por ejemplo, si se inserta indebidamente al legajo de un empleado el padecimiento de enfermedades), máxime cuando tratándose de un delito de acción privada (artículo 73 del Código Penal) se estará ante una víctima que explícitamente reclama que su privacidad ha sido violentada con la inclusión de ese dato.

La norma lleva implícito un dolo especial que consiste en el conocimiento e intención de alterar la información personal del titular de los datos personales, no admite ninguna forma culposa. Por ejemplo si en el curso de un procesamiento de datos, un empleado de una empresa inserta o hace insertar un dato personal en la base de datos, pero no lo hace con conocimiento de tal hecho, sino porque se trata de un dato cuyo error se arrastra incorrectamente de otro proceso, no se configura el tipo penal. Al hacer referencia a "insertare o hiciere insertar" permite que el delito se cometa a través de terceros .

- **<u>Fraude informático (artículo 173, inc 16 CP)</u>**

La Ley de Delitos Informáticos también ha introducido la figura de la defraudación mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos, previéndose una pena de prisión de 1 mes a 6 años.

El apoderamiento de datos relacionados con cuentas bancarias o tarjetas de crédito o débito es una de las modalidades más frecuentes de estafa informática. Los medios van desde las técnicas de ingeniería social hasta el phishing, en el que se engaña al usuario de la red social invitándolo a acceder al supuesto sitio web de una organización reconocida, cuando en realidad el usuario está accediendo al sitio web del hacker, quien de ese modo obtiene la información necesaria para cometer posteriormente las estafas.

En este sentido, cobran relevancia las medidas que puedan adoptar los usuarios de redes sociales tanto respecto de las personas con quienes intercambian información (los "amigos" dentro de la red) como respecto de los sitios a los que acceden por invitación de otro usuario o la información que dejan en esos sitios.

La acción típica es defraudar mediante una manipulación en un ordenador.

Modalidades delictivas de estafa:

Alteración de registros informáticos: Es una de las formas más tradicionales de realizar estafas informáticas: se altera un registro informático, cuyo contenido el sistema toma en cuenta para adoptar decisiones de pago o de disposiciones patrimoniales. De esa forma, el sujeto activo obtiene fraudulentamente sumas de dinero o beneficios, que de otra manera no le corresponderían. Por ejemplo, un insider accede a la cuenta bancaria y altera el monto, para tener más dinero del que le corresponde o se realiza una transferencia no autorizada a ella.

Uso no autorizado de tarjetas y claves falsas o sustraídas o de sus datos: En la jerga se lo conoce como carding, existiendo organizaciones internacionales dedicadas a intercambiar ese tipo de información con fines de comisión de delitos. No solo se puede falsificar la tarjeta de crédito, sino también la de débito, o la de acceso a cajero automático. Los perjudicados en estos casos son varios: en principio, nunca el usuario, porque está amparado por un seguro y por el sistema de tarjetas que evita que responda ante una denuncia. Pero el sistema de tarjetas de crédito y las empresas que procesan estas tarjetas son los más perjudicados cuando deben responder ante supuestos de uso ilícito de ellas.

Mise en scène en cajeros automáticos: En otros supuestos, muy comunes en toda América Latina, se han utilizado dispositivos unidos a una laptop y disimulados en el cajero automático con el fin de copiar datos sensibles de diferentes clientes de tarjetas de crédito para, posteriormente, proceder a su duplicación. En estos casos, ese mecanismo es idóneo para cometer una defraudación.

Estafa de telecomunicaciones: Esta modalidad de estafa tiene lugar cuando se obtiene la prestación de un servicio de comunicaciones sin haberlo abonado previamente.

Phising y robo de identidad: El Phising es una modalidad defraudataria que consiste en remitir un correo electrónico engañoso a clientes para que revelen información personal –tales como su número de tarjeta de crédito o de débito o claves de cuentas bancarias- a través de sitios web simulados o en una respuesta de correo electrónico. Usualmente los

correos electrónico y sitios web con gráficos atractivos para engañar a los clientes haciéndoles creer que el remitente o dueño del sitio web es el banco o una entidad gubernamental que ellos conocen. Desde hace varios años han aumentado considerablemente las modalidades delictivas relacionadas con los datos personales, que ya han pasado a formar un capítulo más del delito informático. Las finalidades de estos robos de identidad no tienen límites y no sólo alcanzan a entidades financieras sino también a registros de nombres de dominio (para secuestrar el nombre de éste), cuentas de hosting, y de google adword. El robo de identidad es un delito complejo, pues afecta diversos bienes jurídicos penalmente protegidos: la privacidad, la propiedad y el honor. En primer lugar el autor del hecho ilícito debe de alguna forma, violar la privacidad y la confidencialidad de las bases de datos para acceder a la información personal de carácter identificatorio para luego afectar el patrimonio al realizar un fraude de la entidad financiera. Una vez perpetrado éste, nuevamente se lesiona el honor e identidad del verdadero titular, que figurará como deudor en registros de morosos sobe la base de una obligación que nunca contrajo. A su vez esta registración le ocasionará denegatorias injustas de crédito al que probablemente tendría fácil acceso de no haber ocurrido el hecho y un sinnúmero de trámites (denuncia penal, reclamo ante la entidad financiera, pedido de rectificación de datos ante la empresa de informes comerciales) para lograr eliminar el dato, perdiendo incontables horas para realizar gestiones ante un burocracia interminable.

- **Daño o sabotaje informático (artículos 183 y 184 incisos 5º y 6º CP)**

Por su parte, el Art. 183 (CP) dispone que, quien alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático cualquier programa destinado a causar daños, incurrirá en una pena de 15 días a un año. La modificación introducida a este artículo permite considerar como objeto de ataque o pasible de daño (entendido como una alteración de las condiciones, propiedades, destrucción, inutilización, etc.) a los sistemas, programas, datos o archivos informáticos.

Como se desprende del análisis del Art. 183, el daño informático puede producirse ya sea por alteración, destrucción o inutilización**,** e igualmente por la introducción en un sistema de un programa destinado a causar un daño. En la primera de las conductas se exige que se produzca un daño y en la segunda la mera introducción de un programa con potencialidad dañina, ya es delito.

La Ley de Delitos Informáticos produjo modificaciones sustanciales en el CP, transformando en punibles conductas que con anterioridad no lo eran o que eran de dudosa punición, quedando en manos de la sana crítica de los jueces penales la interpretación de la norma para un caso no previsto expresamente.

La ley sanciona a quien alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

Se prevé una pena de prisión de 15 días a 1 año, que aumenta a prisión de 3 meses a 4 años cuando la acción se ejecuta en datos, documentos, programas o sistemas informáticos públicos o en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

En esta figura encuadran los virus informáticos, que son programas de computación destinados a causar daños, aunque no encuadraría el spyware, salvo que este cause un daño o esté destinado a causarlo. Es interesante destacar que la ley contempla el caso de quien daña un dato, documento, programa o sistema informático, así como el de quien comercializa, distribuye, hace circular o introduce un virus en un sistema informático aun cuando no se produzca ningún daño en el sistema infectado.

Las redes sociales son propicias para este tipo de accionar, dado que el intercambio de archivos o la descarga de material subido por los usuarios pueden involucrar casos de virus informáticos. Medidas relacionadas con la precaución a la hora de abrir o descargar material así como contar con antivirus y firewalls auténticos y debidamente actualizados ayudan a prevenir este tipo de ataques.

GROOMING

Otro de los aspectos a tener en cuenta y que cobró relevancia en estos últimos años, es el **Grooming**.

Se trata de un delito informático en el que los adultos se ganan la confianza de menores para luego mediante acciones deliberadas, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual. Utilizan las **redes sociales** y la computadora como medio y ponen en juego estrategias para evitar la identificación de los interlocutores.

Si bien se trata de un delito complejo teniendo en cuenta que los servidores, el groomer y la víctima pueden encontrarse todos en distintos países, desde la Ciudad de Buenos Aires, por ejemplo, se trabaja en la persecución de este delito obteniéndose importantes resultados en cuanto a persecución y aplicación efectiva de penas.

Espionaje de datos por parte de los Estados Nacionales

Otro aspecto relevante derivado de las Tecnología de la Información que tiene que ver con la protección de datos personales, es que esta protección no es absoluta y encuentra un único límite y es cuando están en juego cuestiones de **seguridad nacional**. En dicho contexto, los Estados podrán hacer uso de los datos personales de los ciudadanos. Sin embargo, este uso también será necesario controlarlo.

También el espionaje llevado a cabo entre Estados es una cuestión que se da a menudo y prueba de ello es lo acontecido, por ejemplo, en Estados Unidos en donde se vio afectado el propio presidente como consecuencia de los **ataques informáticos** efectuados por Rusia en contra de la candidata Clinton y apoyo al actual presidente.

Tanto éste, como otros nuevos fenómenos, se presentan como desafíos de análisis para los **profesionales del Derecho**. En esos términos, los alumnos y graduados de Abogacía y profesionales del área, deben tener una capacitación continua.