



San Raymundo Jalpan, Centro, Oaxaca, a 16 de marzo de 2018.

DIP. JOSÉ DE JESÚS LÓPEZ RODRÍGUEZ
PRESIDENTE DE MESA DIRECTIVA DE LA
LXIII LEGISLATURA DEL ESTADO.
P R E S E N T E.



La que suscribe **Diputada Felicitas Hernández Montaña**, integrante de la Fracción Parlamentaria del Partido Revolucionario Institucional, en esta LXIII Legislatura Constitucional del Estado, en términos de lo dispuesto por los artículos 50, fracción I, de la Constitución Política del Estado Libre y Soberano de Oaxaca, y 67, fracción I, de la Ley Orgánica del Poder Legislativo del Estado de Oaxaca, me permito someter a la consideración de este Honorable Congreso del Estado, una iniciativa con proyecto de Decreto por el que se adiciona el TÍTULO VIGÉSIMO SEXTO denominado "DELITOS COMETIDOS MEDIANTE EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN", que incluye un CAPÍTULO I denominado "DEPREDADOR SEXUAL", y el artículo 426; un CAPÍTULO II denominado "INTIMIDACIÓN", y el artículo 427; un CAPÍTULO III denominado "DELITOS CONTRA LA DIVULGACIÓN INDEBIDA DE INFORMACIÓN DE CARÁCTER PERSONAL", y los artículos 428, 429, 430 y 431; un CAPÍTULO IV denominado "INTROMISIÓN ABUSIVA DE LA PRIVACIDAD", y el artículo 432,

EL CONGRESO DEL ESTADO DE OAXACA

16 MAR 2018

DIRECCIÓN DE APOYO LEGISLATIVO

11:33hrs



y un CAPÍTULO V denominado "VIOLACIÓN DE CORRESPONDENCIA O MENSAJERÍA ELECTRÓNICA", con el artículo 433, todos al Código Penal para el Estado Libre y Soberano de Oaxaca, lo que someto a la consideración de este Pleno Legislativo del Estado, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación. Según el diccionario de la Real Academia de la Lengua Española, informática es el "conjunto de técnicas empleadas para el tratamiento automático de la información por medio de sistemas computacionales".

La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información, para ejecutar tareas que en otros tiempos realizaban manualmente.



Vivimos en un mundo que cambia rápidamente. Antes, podíamos tenerla certeza de que nadie podía acceder a información sobre nuestras vidas privadas. La información era solo una forma de llevar registros. Ese tiempo ha pasado, y con él, lo que podemos llamar intimidad. La información sobre nuestra vida personal se está volviendo un bien muy cotizado por las compañías del mercado actual. La explosión de las industrias computacionales y de comunicaciones ha permitido la creación de un sistema, que puede guardar grandes cantidades de información de una persona y transmitirla en muy poco tiempo. Cada vez más y más personas tienen acceso a esta información, sin que las legislaciones sean capaces de regularlos.

Los progresos mundiales de las computadoras, el creciente aumento de la capacidad de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información"¹, a lo que con más propiedad, podríamos

¹ Algunos autores se han referido al proceso de desarrollo de la influencia la tecnología informática como la «segunda revolución industrial» que sus efectos pueden ser aún más transformadores que los



decir que más bien estamos frente a la "ERA DE LA INFORMÁTICA".

Por tanto, abordar el estudio de las implicaciones de la informática en el fenómeno delictivo resulta una cuestión apasionante para quien observa el impacto de las nuevas tecnologías en el ámbito social. Efectivamente, el desarrollo y masificación de las nuevas tecnologías de la información y la comunicación (TIC) han dado lugar a cuestiones tales como el análisis de la suficiencia del sistema jurídico actual para regular las nuevas posiciones, los nuevos escenarios, en donde se debaten los problemas del uso y abuso de la actividad informática y su repercusión en el mundo contemporáneo.

Es por esta razón, que paralelamente al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamientos disvaliosos antes impensables y en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad.

de la industrial del siglo XIX. Referencia Ulrich Sieber, "Documentación Para Aproximación Al Delito Informático", publicado en Delincuencia, Editorial. PPU, Barcelona, España, 1992, Pág. 65.



La doctrina ha denominado a este grupo de comportamientos, de manera genérica, «**delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática**».

En efecto, tratándose del sistema punitivo, se ha suscitado una colosal discusión en cuanto a la vocación de los tipos existentes para regir las nuevas situaciones, que el uso y abuso de los sistemas computacionales han logrado con los llamados delitos informáticos o también llamada criminalidad informática.

Lo anterior tiene especial relevancia si consideramos los principios informadores del derecho penal, los que habrán de tenerse a la vista en todo momento. En efecto, no basta en este caso la "**intuición**" en cuanto a que se estima que una determinada conducta podría ser punible, el derecho penal exige una subsunción exacta de la conducta en la norma penal para que recién se esté en presencia de un "**hecho que reviste carácter de delito**"², que autoriza su investigación. En este sentido, se puede decir que dentro de la amplia gama de delitos que se pueden cometer a través de las nuevas tecnologías de la información y comunicación, se pueden catalogar como las más

² DONOSO ABARCA, Lorena, Análisis del tratamiento de las figuras Relativas a la Informática tratadas en el título XIII del Código Penal Español de 1995.



importantes el cibercrimen, el ciberterrorismo y la ciberguerra. Estas acciones están experimentando un fuerte apogeo que contrasta con la débil preparación de los Estados y organizaciones para hacerles frente.

El cibercrimen comprende un amplio espectro de delitos entre los que cabría citar la piratería de software, juegos, música o películas; estafas, transacciones fraudulentas, acoso y explotación sexual, pornografía infantil, fraudes de telecomunicaciones, amenazas, injurias, calumnias, etc. Como se puede deducir, el cibercrimen persigue fundamentalmente conseguir un beneficio económico, pero también incluye el dominio de internet con fines inmorales.

Dentro del cibercrimen, la mayoría de los ataques informáticos provienen del uso del phishing³, troyanos⁴ y los malware⁵. A través de los dos primeros, los delincuentes se pueden hacer

³ El phishing es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta <http://seguridad.internautas.org/html/451.html>

⁴ Los Troyanos Informáticos o Caballos de Troya (en inglés Trojan) es una clase de virus que se caracteriza por engañar a los usuarios disfrazándose de programas o archivos legítimos/benignos (fotos, archivos de música, archivos de correo, etc.), con el objeto de infectar y causar daño. <http://www.seguridadpc.net/troyanos.htm>

⁵ Malware es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. <http://www.infospymware.com/articulos/que-son-los-malwares/>



con contraseñas que utilizan para obtener información sensible a la que habitualmente no tendrían permiso para acceder. Por su parte, los malware están evolucionando de forma alarmante en los últimos años. Su carta de presentación admite diferentes formas: virus, caballo de Troya, puerta trasera (backdoor), programa espía (spyware), o un gusano. Además, a causa de un malware pueden derivarse otros tipos de ataques como puede ser la denegación de servicio.

El cibercrimen se consolida como un negocio en alza. Los ataques informáticos podrían haber afectado a cerca de 378 millones de víctimas en todo el mundo, siendo los países más afectados: Rusia, China, Sudáfrica y Estados Unidos. Éste último lidera el coste, a escala mundial del cibercrimen⁶.

El ciberterrorismo, aunque está muy vinculado con el cibercrimen, se diferencia de ésta en que no persigue principalmente un fin económico sino que se centra más en aquellas acciones en las que se persigue intimidar, coaccionar y causar daños con fines fundamentalmente políticos-religiosos.

⁶ El cibercrimen generó unas pérdidas de 87.000 millones de euros en todo el mundo entre noviembre del 2012-2013 y se ha convirtiéndose en «uno de los negocios más lucrativos que no ha sufrido la crisis». <http://www.abc.es/tecnologia/redes/20131105/abci-cibercrimen-millones-perdidas-201311052029.html>



El ciberespacio se está consolidando como un santuario de terroristas debido a que está siendo utilizado cada vez más por éstos. Las acciones que llevan a cabo en él pueden ser de financiación, guerra psicológica, reclutamiento, comunicación, adoctrinamiento, propaganda, entre otras.

Teniendo en cuenta que las guerras actuales se libran tanto en el campo de batalla como en la esfera de la información, la superioridad militar de un bando en el campo de batalla convencional, puede provocar que el más débil se focalice en la red con el fin de equilibrar la balanza de poder. Así, la invasión de Irak, comandada por Estados Unidos, brindó a la red un nuevo refugio, para los insurgentes, desde donde reorganizar su lucha contra las fuerzas occidentales de los "cruzados"⁷.

La falta de regulación y el enmascaramiento que ofrece la red hace que los grupos terroristas realicen sus acciones con total impunidad. El cierre de sitios web no supone ningún problema para ellos ante la facilidad con la que encuentran nuevos servidores donde colocar sus páginas y seguir con sus actividades.

⁷ Wael Adhami, La importancia estratégica de Internet para los grupos armados insurgentes en las guerras modernas, "International revue of the Red Cross", (diciembre 2007):306.



Hasta la aparición de Internet (1969) y su desarrollo (década de los 90), las guerras se habían llevado a cabo en los espacios terrestre, marítimo, aéreo y en el espacio electromagnético. Es a partir de la década de los 90 cuando la consolidación del crecimiento de la infraestructura tecnológica y el uso de las redes, hacen que cada vez se vea más al ciberespacio como un nuevo campo de batalla, donde se lleve a cabo la ciberguerra. Esta nueva forma de hacer la guerra no se limita solo a efectos sobre los equipos informáticos sino que sus consecuencias pueden trasladarse al mundo físico. Como defiende J.S Nye en su libro "El futuro del poder" (2010): "No se trata de una guerra sin derramamiento de sangre"⁸.

Ante tal amenaza los Estados se están organizando. Si el dominio de las tres dimensiones tierra, aire y mar; supuso la creación de los Ejércitos de Tierra, Aire y Amada respectivamente. Hoy, los retos y amenazas que presenta el ciberespacio están haciendo que los Estados estén creando "ciberejércitos", que en el caso de España, se trata del Mando Conjunto de Ciberdefensa⁹. Sin embargo no creamos que todos

⁸ J.S Nye, Ciberguerra y ciberpaz, "Project Syndicate" : [consultado mayo 2014]:disponible en <http://www.project-syndicate.org/commentary/cyber-war-and-peace/spanish>

⁹ BOD N°40 23FEB13, Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas españolas.



están compuestos de personas uniformadas frente a un ordenador. La mayoría de los países están contratando a personal experto (muchos de ellos hackers conocidos) para que trabajen en estos cometidos. Las actuaciones de estos ciberejércitos ya se están haciendo notar.

De acuerdo a lo que se menciona, es fácil advertir que de la categorización que se plantea en relación a la amplia gama de delitos que pueden cometerse mediante las TICS, el Poder Legislativo de nuestro Estado, tiene competencia para legislar y establecer nuevos tipos penales en materia de lo que la doctrina y el derecho comparado reconocen como cibercrimen, siendo comprensible que el desarrollo de las nuevas tecnologías ha fomentado o permitido la comisión de delitos, que ya existían antiguamente, como la estafa o el fraude, pero que ahora se realizan de una forma distinta, es decir, utilizando o aprovechando la existencia de vías telemáticas. Esto es lo que podemos categorizar como delitos informáticos. Y es que Internet supuso un increíble avance en el complejo mundo de las tecnologías, convirtiéndose también en un nuevo instrumento para la comisión de delitos.

Para entendernos, los delitos informáticos son aquellos delitos que se comenten empleando los diferentes medios electrónicos



e informáticos existentes. Entre otros, podemos destacar la revelación de secretos o la vulneración de la intimidad de las personas, (invadiendo, por ejemplo, los correos electrónicos o interceptando el envío de documentos), el "phishing", el fraude cometido a través de internet. Se trata de un delito relacionado siempre con su "identidad online" y con las credenciales de acceso de los distintos servicios que la víctima utilice en la red, como claves de acceso a banca online, loggins y passwords de usuarios de mensajerías instantáneas, de acceso a sus perfiles en redes sociales o contraseñas de los correos electrónicos del atacado.

A estos hay que unir el pharming (una modalidad de estafa), Un ejemplo común es el de redirigirnos a la página falsa del banco diseñada por los ladrones de forma automática, es decir, sin que nosotros necesitemos pulsar ningún enlace); el espionaje industrial; el delito contra la intimidad de menores, el cyberacoso, por citar sólo algunos de los delitos que de forma más frecuente se cometen a través de un medio tan amplio como Internet.

Por todo esto, a fin de regular el uso ético y moral de las tecnologías de la información y de la comunicación y con el propósito de proteger diferentes bienes jurídicos de la población



en relación con el uso de dichas tecnologías, me permito someter a la consideración de esta Soberanía la siguiente iniciativa con proyecto de:

DECRETO

ÚNICO: Se adiciona el **TÍTULO VIGÉSIMO SEXTO** denominado "**DELITOS COMETIDOS MEDIANTE EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN**", que incluye un **CAPÍTULO I** denominado "**DEPREDADOR SEXUAL**", y el artículo 426; un **CAPÍTULO II** denominado "**INTIMIDACIÓN**", y el artículo 427; un **CAPÍTULO III** denominado "**DELITOS CONTRA LA DIVULGACIÓN INDEBIDA DE INFORMACIÓN DE CARÁCTER PERSONAL**", y los artículos 428, 429, 430 y 431; un **CAPÍTULO IV** denominado "**INTROMISIÓN ABUSIVA DE LA PRIVACIDAD**", y el artículo 432, y un **CAPÍTULO V** denominado "**VIOLACIÓN DE CORRESPONDENCIA O MENSAJERÍA ELECTRÓNICA**", con el artículo 433, todos al Código Penal para el Estado Libre y Soberano de Oaxaca, lo que someto, para quedar como sigue:

ARTÍCULO 432.- ...

TÍTULO VIGÉSIMO SEXTO DELITOS COMETIDOS MEDIANTE EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN

CAPÍTULO I DEPREDADOR SEXUAL

ARTÍCULO 426.- A quien fingiendo una identidad o usando la real, realice el acercamiento entre éste o incluso un tercero, con un menor de edad, a través de redes sociales o cualquier otro medio vía internet, con el propósito de facilitar un encuentro sexual, comete el delito de depredación sexual.



A quien cometa este delito con personas mayores de 15 años y menores de 18 años de edad, se le impondrá una pena de siete a quince años de prisión y multa de quinientos a mil unidades de medida y actualización.

A quien cometa este delito con personas menores de 15 años de edad, se le impondrá una pena de quince a veintiocho años de prisión y multa de mil a diez mil unidades de medida y actualización.

CAPÍTULO II INTIMIDACIÓN

ARTÍCULO 427.- A quien, a través de medios informáticos, acose, hostigue, intimide, agrede o profiera cualquier forma de maltrato físico, verbal o psicológico en contra de usuarios de Internet, de forma reiterada y sistemática, se le impondrá una pena de seis meses a dos años de prisión y multa de cincuenta a ochenta unidades de medida y actualización.

Si la conducta descrita en el párrafo anterior es cometida por un servidor público o medie una relación de superioridad laboral o derivada de la influencia que la persona ejerza sobre la víctima, se le aumentará en una mitad de las penas previstas en el primer párrafo.

CAPÍTULO III DE LOS DELITOS CONTRA LA DIVULGACIÓN INDEBIDA DE INFORMACIÓN DE CARÁCTER PERSONAL

ARTÍCULO 428.- A quien, sin la autorización correspondiente, revele, difunda o ceda, en todo o en parte, información privada referente a imágenes, audio, video o la información sensible de usuarios, obtenidos por cualquier medio, se le impondrán de seis a doce años de prisión y multa de ciento cincuenta a doscientos unidades de medida y actualización.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para el usuario o para un tercero, la pena se aumentará de un tercio a la mitad.



ARTÍCULO 429.- A quien, sin la autorización correspondiente, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, contenidos en un Sistema Informático, se le impondrán de seis a doce años de prisión y multa de ciento cincuenta unidades de medida y actualización.

ARTÍCULO 430.- A quien dolosamente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la información personal de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un ordenador o Sistema Informático, se le impondrán de cinco a diez años de prisión y multa de cien a ciento cincuenta unidades de medida y actualización.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la información o para un tercero.

ARTÍCULO 431.- A quien ofrezca o preste servicios destinados a cumplir los mismos fines previstos en este capítulo, se le impondrán de cinco a diez años de prisión y multa de hasta cuarenta unidades de medida y actualización.

CAPÍTULO IV INTROMISIÓN ABUSIVA DE LA PRIVACIDAD

ARTÍCULO 432.- A quien, sin consentimiento del afectado, difunda, publique, copie, reproduzca, comparta, exhiba a través de Internet o cualquier otro medio electrónico imágenes, audio o videos de contenido sexual o erótico, tomadas por la misma víctima o por un tercero, que se hayan obtenido en el ámbito de la privacidad con o sin el consentimiento del afectado, se le aplicarán sanciones de seis a quince años de prisión y multa de quinientos a mil unidades de medida y actualización.

Los administradores de sitios de Internet que no bajen estas imágenes de manera inmediata a solicitud del afectado, serán sancionados con las mismas penas del inciso anterior.



CAPÍTULO V

VIOLACIÓN DE CORRESPONDENCIA O MENSAJERÍA ELECTRÓNICA

ARTÍCULO 433.- Se aplicará de uno a cinco años y multa de cien a doscientos unidades de medida y actualización:

I.- Al que abra indebidamente una comunicación escrita electrónica que no esté dirigida a él, y

II.- Al que indebidamente intercepte una comunicación escrita electrónica que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido.

No aplicará lo previsto en este artículo, cuando los padres abran o intercepten las comunicaciones escritas electrónicamente dirigidas a sus hijos menores de edad o inimputables y los tutores respecto de las personas que se hallen bajo su dependencia.

TRANSITORIOS

PRIMERO.- El presente Decreto entrará en vigor al día siguiente de su publicación en el Periódico Oficial del Gobierno del Estado.

SEGUNDO.- Publíquese en el Periódico Oficial del Gobierno del Estado.

ATENTAMENTE
SUFRAGIO EFECTIVO. NO REELECCIÓN
"EL RESPETO AL DERECHO AJENO ES LA PAZ"

DIP. FELICITAS HERNÁNDEZ MONTAÑO

LEGE LEGISLATURA

DR. FELICITAS HERNÁNDEZ MONTAÑO

SECRETARIO DE

ESTADO DE OAXACA