—LEGISLATURA—
H. CONGRESO DEL ESTADO DE AGUASCALIENTES

50 ANIVERSARIO
BENEMÉRITA
UNIVERSIDAD AUTÓNOMA
DE AGUASCALIENTES

ESTADOS UNIDOS MEXICANOS
ESTADO LIBRE Y SOBERANO DE AGUASCALIENTES
PODER LEGISLATIVO

Aguascalientes, Ags., a 15 de junio del 2023

ESTADO DE AGUASCALIENTES
SECRETARÍA GENERAL
RECIBIDO
15 JUN. 2023
RECIBE Ulloa
FIRMA
HORA 10:35
PRESENTA Promovente
FOJAS 8

HONORABLE SEXAGÉSIMA QUINTA LEGISLATURA
DEL H. CONGRESO DEL ESTADO DE AGUASCALIENTES
P R E S E N T E:

DIP. ANA LAURA GÓMEZ CALZADA Y DIP. JUAN LUIS JASSO HERNÁNDEZ, en nuestro carácter de integrantes de la LXV Legislatura del Honorable Congreso del Estado de Aguascalientes, con fundamento en lo dispuesto por los artículos 27, fracción I y 30, fracción I, de la Constitución Política del Estado de Aguascalientes; los artículos 16, fracciones III y IV, 108, 109, 112, y 114 de la Ley Orgánica del Poder Legislativo del Estado de Aguascalientes, y el artículo 153, fracción I, del Reglamento de la Ley Orgánica del Poder Legislativo del Estado de Aguascalientes, sometemos a consideración de esta Honorable Soberanía la **INICIATIVA CON PROYECTO DE DECRETO POR LA QUE SE ADICIONA EL ARTÍCULO 181 C DEL CÓDIGO PENAL PARA EL ESTADO DE AGUASCALIENTES,** al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

Con la llegada de las Tecnologías de la Información y la Comunicación se ha producido una gran incertidumbre sobre el tratamiento de los datos que compartimos e intercambiamos a través de ellas. Dada esa inquietud, varios países han introducido en sus ordenamientos jurídicos protocolos y políticas de seguridad en aras a controlar el flujo de información en internet y la protección de datos de los usuarios. Esas normas jurídicas van dirigidas a proteger los derechos e intereses del sector público como aquellos derechos fundamentales que gozan los ciudadanos.

Las tecnologías han ido evolucionando a la par que la sociedad, por ello es importante desarrollar programas, métodos y leyes que ayuden a regular esta nueva forma de delincuencia, cuya característica principal es su operación a través de la red.

Hoy en día la tecnología está presente en nuestra vida, entendiendo así que es fundamental para el desarrollo de la humanidad, los avances tecnológicos y la era de las comunicaciones digitales y el uso de las tecnologías de la información y la comunicación e internet, son cruciales para la evolución sociocultural que empodera todas las áreas de un país como la sociedad, economía, cultura, educación, salud, seguridad, entre otras, porque es una herramienta vital de innovación y trasformación tanto en aspectos positivos como negativos, por lo que es transcendental identificar los delitos

informáticos y plasmarlos en la Ley.

"Para adentrarnos al estudio de los llamados Delitos Informáticos, o en sus diferentes denominaciones como delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora o delincuencia relacionada con el ordenador, etc., entraremos al conocimiento y manejo de lo que es la computadora en nivel operacional y de estructuración.

De manera elemental, diremos que la computadora tiene una estructura a nivel operacional y a nivel estructural."[1]

"Es indispensable el uso de la computadora y del manejo del Internet, para la comisión de conductas delictivas denominadas "Delitos Informáticos", sin embargo, aun en la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe un concepto propio de los llamados delitos informáticos. Aun cuando no existe dicha definición con carácter universal, se han formulado conceptos funcionales atendiendo a las realidades concretas de cada país.

Por lo que se refiere a nuestro país, cabe destacar lo mencionado por Julio Téllez Valdés, al decir que hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, requiere que la expresión "delitos informáticos" esté consignada en los Códigos Penales, lo cual, en México, al igual que en otros muchos no ha sido objeto de tipificación aún.

El Departamento de Investigación de la Universidad de México, señala como delitos informáticos a "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

Para la comisión de dicha conducta antisocial, encontraremos a uno o varios sujetos activos como también pasivos, los cuales tienen características propias:

El Sujeto Activo posee ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, 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 decir, el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de

[1] https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap3.htm

recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional, pues son personas listas, decididas y motivadas, dispuestas a aceptar un reto tecnológico.

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

El sujeto pasivo del delito es sumamente importante, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas, debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos. Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables" y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otras más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada cifra oculta o cifra negra."[2]

"Hoy en día, el mundo está más conectado digitalmente que nunca. Los delincuentes se están aprovechando de esta transformación en línea para atacar, a través de sus puntos débiles, las redes, infraestructuras y sistemas informáticos. Esto tiene una enorme repercusión económica y social en todo el mundo, tanto para los gobiernos, como para las empresas o los particulares."[3]

"La problemática de los delitos informáticos requiere de un estudio especial en nuestro país a fin de determinar la medida en que las leyes penales vigentes constituyen un cuerpo normativo suficiente para prevenir y reprimir este tipo de conductas delictivas o si es menester la creación de figuras jurídico-penales que expresamente regulen esta nueva modalidad delictiva.

Desafortunadamente, en México se ha vislumbrado incipientemente este asunto, por lo que a la fecha no ha sido tipificado ninguna conducta ilícita derivada por el avance tecnológico, pretendiendo asimilarse diversos tipos que actualmente regula el Código

2 https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap3.htm
3 https://www.interpol.int/es/Delitos/Ciberdelincuencia

Penal, empero, no se debe olvidar que en materia penal no es aplicable la analogía, sino que el delito debe estar perfectamente tipificado en un ordenamiento legal, según se desprende del Artículo 14 constitucional.

Aspectos tales como la integridad y seguridad alrededor de los sistemas de cómputo, son aspectos no suficientemente desarrollados, cuyas consecuencias no se detienen en lo técnico o en lo económico, incidiendo, de manera cada vez más acentuada, en aquello que aparentemente no tenía relación: lo legal."[4]

Es de suma importancia legislar en materia penal con una visión actualiza de las conductas antisociales en lo relativo a las nuevas conductas de realizar los delitos como lo son en este caso los Delitos Informáticos; tomando en consideración que la Ley es perfectible y por ende tiene que estar en constante cambio de acuerdo con la evolución tecnológica.

"Tenemos un factor muy importante, uno que puede ser el causal de muchos problemas e indetectable en caso de no estar capacitado para distinguirlo, ese factor es el llamado Sabotaje Informático.

El sabotaje informático es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

Sin embargo, las técnicas que permiten cometer sabotajes informáticos son: BOMBAS LÓGICAS (LOGIC BOMBS), que es una especie de bomba de tiempo que debe producir daños posteriormente y que exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Esto sería, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Otra técnica, son los famosos GUSANOS, donde se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que

[4] https://dialnet.unirioja.es/ejemplar/39614

el virus es un tumor maligno. En consecuencia, los estragos del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Otra técnica son los tan conocidos VIRUS INFORMÁTICOS Y MALWARE, catalogados como elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya. Han sido definidos como "pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de auto reproducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar". Pero, el malware es otro tipo de ataque informático, que usando las técnicas de los virus informáticos y de los gusanos y las debilidades de los sistemas desactiva los controles informáticos de la máquina atacada y causa que se propaguen los códigos maliciosos.

Otra técnica, son los ATAQUES DE DENEGACIÓN DE SERVICIO, aquí los ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a muchos usuarios, el ejemplo típico de este ataque es el consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas e irreparables.

Todos estos riesgos del sabotaje informático son de gran volatilidad dentro de la actividad corporativa, reproducen un peligro que se expresa en pérdidas económicas, disminución de la capacidad competitiva, filtraciones de estrategias comerciales, vaciamientos de cuentas y falta de confianza hacia el cliente, y más importante, incapacidad para desarrollar su actividad de manera segura y transparente."[5]

[5] https://www.itwarelatam.com/2021/06/07/sabotaje-informatico-y-el-compliance/

"Cuando se habla de innovación tecnológica se suelen considerar siempre sus rasgos más positivos. Sin embargo, la multiconectividad en tiempo real también conlleva riesgos, y como ejemplo de esto, aquí revisaremos casos reales de delitos informáticos en México.

Tan solo al cierre del primer trimestre de 2018, se reportaban más de un millón de fraudes cibernéticos a nivel nacional, superando por mucho al fraude tradicional, que presentó un total de 659 440 casos en el mismo periodo, según datos de la CONDUSEF.

De un año para otro, el fraude cibernético desplazó al fraude tradicional en cuanto a número de quejas presentadas formalmente, creciendo como lo hacen otros delitos de la misma clase, tales como el robo de identidad (*phishing*) y la clonación de tarjetas.

Casos de delitos informáticos en México; comencemos con tres casos, que por su alcance e intenciones queremos destacar: Fallchill, WannaCry y Janeleiro.

- Fallchill

Es un malware que fue detectado en varios equipos de una empresa de telecomunicaciones en la Ciudad de México. Entre sus capacidades están las siguientes:

1. Extraer información de los discos duros de las computadoras donde se alojaba.
2. Iniciar y terminar procesos.
3. Intervenir cualquier archivo para modificarlo, ejecutarlo, moverlo o incluso eliminar elementos del sistema.
4. Por último, es capaz de borrarse a sí mismo, y así evitar dejar rastros de su presencia, lo que dificulta su detección en las redes vulnerables.

- WannaCry

Tuvo alcance en más de 150 países, incluido México en 2017. Este programa operaba mediante extorsiones, ya que tenía la función de "secuestrar" información para luego "pedir pagos por su rescate"; este es el *modus operandi* típico de un *ransomware*.

Se calcula que el número de víctimas de este malware, hasta 2018, fue de al menos 200,000 a nivel global; mientras que, en México, se estima que el 44% de las organizaciones fueron víctimas del secuestro de su información.

- Janeleiro

Este malware bancario creado originalmente para atacar corporativos de bancos en Brasil, del cual fue creada una variante para atacar usuarios en México, y poder robar su información bancaria y personal.

Este virus es distribuido a través de correos electrónicos, que contienen enlaces que redireccionan a los usuarios ventanas emergentes con formularios de banco apócrifos; de esta forma logran acceder y robar la información bancaria."[6]

Por lo tanto, es imperativo contar con una figura típica, antijuridica y culpable en el Código Penal para el Estado de Aguascalientes, considerando que los servidores públicos al servicio del estado son usuarios informáticos quienes resguardan y procesan infinidad de información de diferente índole por lo cual el daño que pudiera causar sería de una gran afectación, como pudiera ser en diferentes áreas como por ejemplo y citando al Registro Público de la Propiedad.

Por lo anteriormente expuesto, se propone el siguiente:

PROYECTO DE DECRETO

ÚNICO. – Se adiciona el artículo 181 C del Código Penal para el Estado de Aguascalientes, para quedar de la siguiente manera:

ARTÍCULO 181 C.- 6. El Sabotaje Informático consiste en acceder a sistemas y equipos de informática de alguna dependencia o particular, e indebidamente modifique, suprima, destruya, copie, extraiga, provoque pérdida de información o que obstaculice el funcionamiento normal del sistema, sin autorización de su propietario o poseedor legítimo.

Al responsable de Sabotaje Informático se le aplicarán de 1 a 4 años de prisión, y de 300 a 600 días multa, así como al pago total de la reparación de los daños y perjuicios ocasionados.

TRANSITORIOS

ÚNICO. - El presente Decreto iniciará su vigencia al día siguiente de su publicación en el Periódico Oficial del Estado de Aguascalientes.

[6] https://blog.orcagrc.com/casos-de-delitos-informaticos-en-mexico

ATENTAMENTE

DIP. ANA LAURA GÓMEZ CALZADA

DIP. JUAN LUIS JASSO HERNÁNDEZ

H. Congreso del Estado de Aguascalientes, **15 de junio del 2023.**