Foto: Soy 502

Guatemala frente a la era de la globalización de la tecnología y del ciberdelito

Lizandro Acuña

Resumen

El artículo tiene como objetivo analizar la tipología del ciberdelito o delitos informáticos a nivel global y cómo estos se dan en Guatemala. Asimismo, presenta una visión estadística de los delitos más recurrentes en Guatemala en relación con este flagelo, qué ha hecho el país frente a los delitos de la nueva era derivados de la digitalización por medio de la internet y las redes sociales para proteger a los usuarios y analiza el Decreto 39-2022 del Congreso de la República, Ley de Prevención y Protección Contra la Ciberdelincuencia, su compatibilidad con la legislación interna y el Convenio de Budapest sobre la ciberdelincuencia.

Palabras clave

Ciberdelito, ciberdelincuencia, Decreto, Convenio de Budapest, internet

Abstract

The article aims to analyze from a global synthesis the typology of cybercrime or computer crimes, consequently, it synthesizes a statistical vision of the most recurrent crimes in Guatemala in relation to the scourge; that the country has done against the crimes of the new era derived from digitization through the internet and social networks to protect users, in relation to this it outlines the analysis of Decree 39-2022 of the Congress of the Republic, Law on Prevention and Protection Against Cybercrime, its compatibility with domestic legislation and the Convention on Cybercrime.

Keywords

Cybercrime, cybercrime, Decree, Budapest Convention, internet

Síntesis global del ciberdelito

La evolución del hombre en el tiempo apareja descubrimientos y avances a nivel mundial en las diferentes esferas de la ciencia, la tecnología es quizá uno de los descubrimientos más significativos en la era del siglo XXI. La digitalización se ha convertido en la herramienta básica de los países a nivel mundial que proporciona grandes beneficios y oportunidades de desarrollo en los diferentes estratos sociales que la acceden. En la línea, la llamada era de la tecnología o de la digitalización apareja grandes retos y desafíos a nivel global; los riesgos y amenazas latentes en el ciberespacio exponen a los usuarios de la internet a los efectos del ciberdelito y la ciberdelincuencia que constituyen grandes retos para los países del mundo en contrarrestarlos.

El ciberespacio enlaza los elementos tecnológicos que se interconectan a través de la internet, la evolución de la tecnología ha propiciado el descubrimiento de toda una gama de herramientas tecnológicas y su expansión en su uso ha permitido acortar las distancias por medio de las llamadas Tecnologías de la Información y Comunicación (TIC) que se han convertido en las herramientas principales de los ciberdelincuentes para cometer actos ilícitos aprovechando su cobertura que traspasa fronteras y que ha generado un amplio campo para las organizaciones criminales en cometer delitos cibernéticos por medio de la suplantación de sistemas informáticos y el acceso ilícito a equipos de computación y de comunicación; herramientas claves

para asegurar los intereses de estas organizaciones delictivas.

El ciberdelito

Previo a desarrollar el estudio es importante conocer que se entiende por ciberdelito, también denominado delito informático o delito cibernético. El Ministerio de Justicia y Derechos Humanos de Argentina (2022) lo define de la siguiente manera:

> Son conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas.
>
> Consiste en estafas, robos de datos personales, de información comercial estratégica, suplantación de identidad, fraudes informáticos, ataques como cyberbulling, grooming, phishing cometidos por ciberdelincuentes que actúan en grupos o trabajan solos.

El ciberdelito, es un flagelo que debe normarse con una estrategia global, que involucre las regulaciones a lo interno de cada país, sustentado con normas de alcance internacional por su naturaleza, basadas en tratados y convenios internacionales; tema que se desarrollará subsecuentemente en este estudio.

La ciberdelincuencia

Son muchas las definiciones que proporcionan interesantes elementos al definir la ciberdelincuencia. Sin embargo, la Oficina de las Naciones Unidas Contra la Droga y el Delito (ONODC) reúne una serie de elementos mencionados en las diferentes definiciones con relación al flagelo:

> No hay ninguna definición universalmente aceptada de ciberdelincuencia. Sin embargo, la siguiente definición incluye elementos en común con las definiciones que existen sobre la ciberdelincuencia. La ciberdelincuencia es un acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito… (ONODC, 2020)

Al interpretar la definición, puede colegirse que la ciberdelincuencia tiene una característica principal que la diferencia de los delitos comunes: además de la facilidad para infringir la ley, exterioriza impunidad por falta de regulación a nivel mundial y de cultura de denuncia, dificultad para la investigación y persecución penal de los actores intelectuales, falta de conocimiento de las amenazas y riesgos para los usuarios de la internet, poca cobertura en estrategias de cooperación internacional, limitada capacitación de los aparatos competentes en la investigación y persecución penal, entre otras limitantes.

En consecuencia, se desarrollan los ciberdelitos más comunes cometidos a nivel internacional con la globalización de la internet, esto permite generar sistemas y estrategias de ciberseguridad para proteger a los usuarios de los riesgos a que están expuestos. A continuación, se describen los tipos de delitos informáticos reconocidos por Naciones Unidas, según el Foro Latinoamericano de Seguridad:

1. Fraudes cometidos mediante manipulación de computadoras

> MANIPULACIÓN DE LOS DATOS DE ENTRADA

(…) Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de estos.

> MANIPULACIÓN DE PROGRAMAS

(…) Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas.

Resumiendo, el caballo de trolla es uno de los métodos más utilizados para cometer este delito y consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

MANIPULACIÓN DE LOS DATOS DE SALIDA

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. (…) en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

MANIPULACIÓN INFORMÁTICA APROVECHANDO REPETICIONES AUTOMÁTICAS DE LOS PROCESOS DE CÓMPUTO

Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2. Falsificaciones informáticas

LAS FALSIFICACIONES INFORMÁTICAS COMO OBJETO

Cuando se alteran datos de los documentos almacenados en forma computarizada.

LAS FALSIFICACIONES INFORMÁTICAS COMO INSTRUMENTOS

Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó

a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas (…).

3. Daños o modificaciones de programas o datos computarizados

> 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. Las técnicas que permiten cometer sabotajes informáticos son:

> VIRUS

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. 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.

> GUSANOS

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.

(…) Ahora bien, las consecuencias 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.

> BOMBA LÓGICA O CRONOLÓGICA

Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, 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.

4. Acceso no autorizado a servicios y sistemas informáticos

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

> PIRATAS INFORMÁTICOS O HACKERS

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos

medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

> REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. (Foro Latinoamericano de Seguridad, s.f.)

> Como se aprecia, la diversidad de delitos informáticos ha alcanzado dimensiones transnacionales causando daños irreparables y costos dimensionales, afectando la seguridad de los usuarios y la seguridad de las naciones en el ámbito político, económico y social. Los delitos informáticos o ciberdelitos generan un efecto de daño directo en el patrimonio de personas individuales y jurídicas, incluyendo los delitos de acción privada de los cuales según los estudios presentan mayor índice de impunidad por la falta de denuncia vinculada al temor de ser expuestas las víctimas. Existen numerosos estudios que desarrollan el ciberdelito y su tipología, el presente, trata de hacer una síntesis de los principales delitos con relación al tema y tener una lectura de las amenazas a las que se está expuestos; no obstante,

por espacio se acota el análisis a los avances en Guatemala frente a la era de la globalización de la tecnología y del ciberdelito.

En relación con lo que antecede, Guatemala ya cuenta con la Ley de Prevención y Protección Contra la Ciberdelincuencia aprobada este año, que busca la prevención y protección contra la Ciberdelincuencia, en aras de contrarrestar los efectos del ciberdelito y proteger la gestión estatal del gobierno y la integridad de los que dependen del uso de la internet y de las redes sociales como consecuencia de las relaciones laborales, relaciones comerciales, educación, prestación de servicios y comunicaciones privadas. Subsecuentemente, se analiza la recién aprobada ley, desde dos aristas: su efecto tutelar y compatibilidad con la legislación interna e internacional.

Compatibilidad del Decreto 39-2022 con la legislación nacional e internacional

Previo a entrar al análisis de la ley, es imperativo reflexionar la situación actual de Guatemala frente al ciberdelito o delitos informáticos, aunque el país no sea blanco de los ciberataques dirigidos a los países desarrollados, no significa que no esté expuesto a los efectos de los de delitos más comunes que se han evidenciado por las denuncias realizadas por los

usuarios de la internet, redes sociales y las TIC, que han sido víctimas de la ciberdelincuencia en el país. En ese sentido, un artículo publicado por Sara Solórzano en Prensa Libre presenta cifras estadísticas de denuncias realizadas a través de Facebook, Instagram y WhatsApp en torno al comportamiento del flagelo en Guatemala:

> De acuerdo con los registros del Ministerio Público (MP) en los últimos 31 meses han sido promovidas 12 mil 650 denuncias por hechos ilícitos cometidos a través de Facebook, Instagram y WhatsApp.
>
> De acuerdo con el desglose de datos del MP, del 1 de enero al 9 de agosto de 2022, se han registrado unas 3 mil 554 denuncias por diversidad de actos ilegales que se cometen por medio de las aplicaciones anteriormente mencionadas, dicha cifra refleja que son unas 506 denuncias presentadas mensualmente, aproximadamente.
>
> Durante el 2021 se sumaron 5 mil 371 quejas, es decir, unas 477 al mes; en 2020 fueron 3 mil 365 y en 2019 la cifra era de 1 mil 547 denuncias. Los delitos que reflejan mayor incidencia son estafa propia, amenazas y extorsión.
>
> Las localidades donde más se cometen estos ilícitos son: Guatemala con 1 mil 316

> denuncias, seguido de Quetzaltenango con 219, Alta Verapaz con 177 y Chiquimula con 172, según datos proporcionados por el MP. (Solórzano, 2022.)

Como se lee, Facebook, Instagram y WhatsApp son las redes sociales que han sido utilizadas para cometer actos ilícitos en contra de los usuarios y de la misma manera han facilitado la denuncia de las víctimas, eso no significa que otros ciberdelitos con efectos colaterales de mayor dimensión no se cometan en el país, la falta de captura de estas estadísticas puede estar asociada a la falta de cultura de denuncia, no interpretarlos como delitos, falta de información del modus operandi, difícil detección o no representa una amenaza por el momento; alimentando la impunidad para los actores intelectuales de estos delitos.

Co la visión del comportamiento de los delitos informáticos según las cifras desglosadas, el Congreso de la República aprobó con 100 votos el Decreto 39-2022, Ley de Prevención y Protección Contra la Ciberdelincuencia, el cual tiene como objetivo: "proteger los datos personales de los guatemaltecos, fortalecer las reglas de convivencia social-digital del país, actualizar la legislación nacional en esta nueva era tecnológica y la tipificación de ciberdelitos, el fraude informático y la protección de datos personales en internet".

El Decreto 39-2022, tipifica nuevas conductas delictivas y vincula su espíritu con el Código Penal, Decreto 17-73 y el Código Procesal Penal Decreto 51-92, con

leyes especiales vigentes. En relación con los delitos de propiedad intelectual, armoniza su competencia al referir la aplicación del Decreto 57-2000, Ley de Propiedad Industrial y el Decreto 33-98 Ley de Derechos de Autor y Derechos Conexos.

Al normar la ciberdelincuencia, se genera un nuevo sistema de reglas procesales que permite la presentación de evidencias y aportar medios de pruebas digitales y electrónicos que permitan sustentar las investigaciones en relación con los casos ventilados en los procesos penales. Establece la separación de los delitos de acción privada y de acción pública y establece un régimen de responsabilidades penales, civiles, y administrativas para personas individuales y jurídicas que infrinjan la norma.

El Decreto 39-2022, sistematiza un régimen regulatorio de ciberdelitos, castigados con pena de prisión y pena de multa e inhabilitaciones contenidos en el Título II. De los Ciberdelitos, Capítulo I. que regula los delitos contra la Confidencialidad, la Integridad y Disponibilidad de los Datos y Sistemas informáticos o Sistemas que Utilicen Tecnologías de la Información y las Comunicaciones. Por su relevancia para el lector, y considerando que ya se desarrolló este tema a nivel global, se procede a enlistar los ciberdelitos: Acceso ilícito, acceso ilícito a datos con información protegida, interceptación ilícita, ataque a la integridad de los datos, ataque a la integridad del sistema.

Capítulo II. De los delitos informáticos: falsificación informática, apropiación de identidad ajena, abuso de dispositivos, fraude informático, agravantes generales.

Capítulo III. Ciberdelitos contra las personas y delito contra la diversidad sexual de niño, niña o adolescente: este capítulo enlaza la aplicación de código penal en los delitos sobre explotación sexual de niño, niña o adolescente; aumentando la pena en una tercera parte cuando los delitos se cometan utilizando sistemas informáticos o cualquier medio de comunicación electrónica; se regula el acoso por medio cibernéticos o ciberacoso, engaño con fines sexuales; sin embargo, se considera que en este tema existen algunas inconsistencias que se describen la tabla que se presenta más adelante.

En cuanto a los delitos y faltas en la propiedad intelectual, aumenta la pena en una cuarta parte si se comenten utilizando sistemas informáticos o tecnologías de la información o comunicaciones, acotando la aplicación de los Decreto 57-2000, Ley de Propiedad Industrial y el Decreto 33-98, Ley de Derechos de Autor y Derechos Conexos.

Su alcance, efecto y aplicación se fundamenta en el principio penal de extraterritorialidad al regular la extradición de los responsables de los delitos cometidos en la dimensión del ciberespacio, sucesivamente, se hace un esfuerzo por adecuar la normativa al derecho internacional, específicamente a los principios generales para la asistencia mutua, relativos a la cooperación internacional regulada por el Convenio

sobre la ciberdelincuencia establecido en Budapest el 23 de noviembre de 2011, desarrollados en el Capítulo III. Cooperación internacional. Prospectivamente, el artículo 31 de dicho Decreto, regula la cooperación en materia penal y procesal penal cuando se requiera internacionalmente sobre el tráfico e interceptación de comunicaciones observándose los tratados y convenios internacionales de los que Guatemala forma parte.

Algo que resalta es la creación del Centro de Seguridad Interinstitucional de Respuesta Técnica ante Incidentes Informáticos – Guatemala (CSIRT-GT), la cual estará bajo la coordinación del Consejo Nacional de Seguridad y se divide en dos coordinaciones: la coordinación de seguridad que corresponde al Ministerio de Gobernación y la coordinación de defensa que corresponde al Ministerio de la Defensa Nacional. La CSIRG-GT se regirá por una ley orgánica que lo regulará, el plazo para su elaboración es de 90 días a partir de la vigencia del Decreto 39-2022.

No obstante, el capítulo VI establece la Cooperación Internacional para Órganos de Aplicación de la Ley; crea la Red internacional de asistencia mutua contra los delitos informáticos (RED 24/7 Guatemala) adjunta al Ministerio Público (MP) con prestación de servicios las 24 horas al día de los 7 días de la semana como lo establece el Convenio de Budapest. Este ente ayudará en la asistencia inmediata para obtener indicios, medios de investigación y pruebas resultado de las acciones que constituyan delitos vinculados a datos informáticos.

El artículo 36 del Decreto, establece la obligatoriedad para el Estado de Guatemala de elaborar una política de cooperación basada en la observancia de tratados y convenios bilaterales y multilaterales, viabilizar los planes con políticas regionales en relación a los delitos informáticos, fortaleciendo la capacitación técnica y económica internacional para robustecer programas de prevención dirigidos al flagelo, adecuar la armonización del derecho penal sustantivo internacional, entre otros procedimientos de cooperación internacional.

Al regular el principio constitucional de Habeas Data se entiende que protege los principios y garantías inherentes a las personas en materia de derechos humanos, establecidas en la Constitución Política de la República de Guatemala (CPRG), en tratados y Convenios internacionales y la Ley de Acceso a la Información Pública, que derivan del acceso a la internet, otras tecnologías de la información y las comunicaciones. Se ejemplifica el Artículos 28, 29 y 30 de dicho Decreto, que establecen la obligación de orden de juez competente para las personas que deban proporción información relacionada a procesos de investigación, registro y secuestro de medios digitales e intercepciones.

No obstante, el Decreto 39-2022 contiene algunas inconsistencias descritas en la Tabla 1.

Tabla 1

Inconsistencias del Decreto 39-2022. Ley de Prevención y Protección Contra la Ciberdelincuencia

Dto. 39-2022	CPRG	Observaciones
Art. 7. Definiciones. d). CSIRT: Equipo de Respuesta a Incidentes de Seguridad Informática. **Z) Crueldad.**		CSIRT: Equipo de Respuesta a Incidentes de Seguridad. La definición de crueldad es bastante discrecional en su interpretación, al establecer la limitante de divulgar las manifestaciones incluso cuando son verdaderas, sin especificar a cuáles se refiere. Establece un candado a la libertad de emisión del pensamiento en el caso de los funcionarios públicos que están sujetos a la fiscalización social por medio de la crítica o denuncia de sus actos en el ejercicio del cargo.
Título II. De los Ciberdelitos		
Artículo 8. Acceso ilícito. **b) cuando el acceso se realice con la intención de obtener datos informáticos o con otra intención delictiva.**		b) La redacción es ambigua, en el sentido de que la simple obtención de datos constituye delito.
Artículo 16. Fraude Informático.		En este último párrafo no diferencia la autoría material e intelectual; en el entendido que quien obtiene la información es parte del delito al igual que quién la sustrae.
Capítulo III **Ciberdelitos contra las personas y delitos contra la integridad sexual del niño, niña o adolescente.** **Artículo 18. Agravante específica.**		El Decreto número 9-2009, Ley Contra la Violencia Sexual, Explotación y Trata de Personas, ya desarrolla agravantes en la tipología de los delitos sexuales cometidos en contra de menores de edad por ello, las agravantes específicas establecidas en el Decreto 39-2022 debieron someterse a un análisis profundo del principio de proporcionalidad en la aplicación de las penas; considerando que el Decreto 9-2009 desarrolla circunstancias agravantes como parte de las reformas al Decreto 17-73 del Congreso de la República, Código Penal.

Artículo 19. Acoso por medios cibernéticos o ciberacoso. **a) intimidar o asediar a una persona o grupo de personas con contenido falso o cruel, en posesión legítima o no del sujeto activo a través de las tecnologías de la información o comunicación, puede ser con la intención de ejercer dominio sobre la víctima, o para que ésta realice actos contra su voluntad.** **b) divulgar información confidencial de otra persona que afecten su honor o su salud física o psicológica, actuando o no de forma anónima o por cualquier sistema informático o cualquier medio de comunicación electrónico.** **En ambos casos, pueden ser con la intención de cometer otro ilícito.** **(...) se excluyen de la aplicación de este artículo, los casos de libertad de expresión reconocidos en tratados y convenciones de los que Guatemala forma parte, en materia de derechos humanos y los derechos que otorga expresamente la Constitución Política de la República (...)**	Artículo 35.- Libertad de emisión del pensamiento. Es libre la emisión del pensamiento por cualesquiera medios de difusión, sin censura ni licencia previa. Este derecho constitucional no podrá ser restringido por ley o disposición gubernamental alguna. Quien en uso de esta libertad faltare al respeto a la vida privada o a la moral, será responsable conforme a la ley. Quienes se creyeren ofendidos tienen derechos a la publicación de sus defensas, aclaraciones y rectificaciones. No constituyen delito o falta las publicaciones que contengan denuncias, críticas o imputaciones contra funcionarios o empleados públicos por actos efectuados en el ejercicio de sus cargos. (…) Es libre el acceso a las fuentes de información y ninguna autoridad podrá limitar ese derecho.	La CPRG garantiza la libertad de emisión del pensamiento por cualquier medio de difusión incluyendo con ello cualquier medio de la tecnología moderna. El centro del análisis sustenta sus bases que la Carta Magna; somete a la fiscalización social a los funcionarios y empleados públicos en el ejercicio de sus funciones. Entiéndase, el alcance de la norma constitucional, por medio de publicaciones que aparejen denuncias públicas, críticas o imputaciones derivadas de los actos en función al ejercicio del cargo público, sin que se incurra en delito o falta. El artículo 19. Del Decreto 39-2022, contradice la garantía constitucional de libertad de emisión del pensamiento y omite su armonización con el Decreto 9 de la Asamblea Nacional Constituyente, Ley de Emisión del Pensamiento, que desarrolla la garantía constitucional. En materia penal, vincula a los actores del delito de acoso por medios cibernéticos o ciberacoso con la delincuencia organizada, sin analizar profundamente el alcance de los delitos de calumnia y difamación regulados en el Código Penal, cuyo efecto encuadra en el tipo penal del nuevo delito regulado en el Decreto 39-2022. El inciso a) al crear la categoría de situación cruel y no limitar el alcance de la norma a los funcionarios y empleados públicos, propicia una interpretación laxa cuyo efecto puede concluir en acusaciones al fiscalizar la función de estos en el ejercicio del cargo. El inciso b) Pone la tapa al pomo, al prohibir el reenvío de información por medios electrónicos, redes sociales o cualquier otro medio que relacione a los funcionarios y empleados públicos en el ejercicio del cargo. En cuanto a la exclusión de la aplicación del artículo 19, relacionado a los casos de libertad de expresión reconocidos en tratados y convenciones internacionales de los que Guatemala forma parte en materia de derechos humanos, otorgados por la CPRG, es imperativo indicar que la Carta Magna prevalece sobre cualquier ley y que los convenios y tratados internacionales no desarrollan la materia y, por ende, al no excluir tácitamente a los funcionarios y empleados públicos el Decreto 39-2022 vulnera la libertad de pensamiento, misma que puede ser objeto de inconstitucionalidad parcial.

Nota: La Tabla describe algunas antinomias que contiene el Decreto 39-2022, especialmente su posible contradicción con la garantía constitucional de libertad de emisión del pensamiento. Fuente: Elaboración propia.

En relación con el Decreto 39-2022, se colige que la ley ordinaria o especial no puede contradecir a la CPRG, tratados y convenios internacionales en materia de derechos humanos de los que Guatemala es parte. La redacción de la ley debe ser clara y sencilla, de manera que facilite su comprensión y evitar su aplicación e interpretación laxa. Por la temática que desarrolla el Decreto 39-2022, es importante el análisis en las disciplinas que desarrolla, para ello hay dos caminos: el veto por el presidente de la República o la acción de inconstitucionalidad parcial.

Importancia de adherirse al Convenio sobre la Ciberdelincuencia (Budapest, 23.XI,2011)

Este debió ser el primer paso para el Estado de Guatemala previo a legislar el ciberdelito, el Convenio sobre la Ciberdelincuencia permite la adhesión de los países que no sean miembros del consejo de Europa y que no hayan participado en su elaboración:

> A partir de la entrada en vigor del presente convenio, el Comité de Ministros del Consejo de Europa podrá, previa consulta con los Estados contratantes del Convenio y habiendo obtenido su consentimiento unánime, invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo de Europa y que no haya participado en su elaboración.

(Convenio sobre la Ciberdelincuencia, Budapest, 2001)

Puede colegirse que el Convenio es incluyente y está abierto a los países que quieran adherírsele. En el caso de Guatemala, integra la lista de los países latinoamericanos que actualmente no han mostrado interés en dicha adhesión, aun cuando ya tiene vigente la "Ley de Prevención y Protección Contra la Ciberdelincuencia".

¿Conviene o no a Guatemala adherirse al convenio? La respuesta compete a las autoridades de Gobierno decidirlo, no obstante, se reafirma que fue el primer paso que debió dar el Estado de Guatemala por las razones siguientes: debe considerarse que una de las características del Convenio radica en que, al momento de ser firmado y ratificado, el Estado podrá decidir el o los territorios donde se aplique este. Referente a su objeto, el instrumento internacional describe en su artículo 39:

1. El objeto del presente convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las partes incluía las disposiciones:

- Del Convenio Europeo de Extradición, abierto a la firma el 13 de diciembre de 1957 en París (STE no 24)

- Del Convenio Europeo de Asistencia Judicial en Materia Penal, abierto

a la firma el 20 de abril de 1959 en Estrasburgo (STE n0 30),

- del Protocolo adicional del Convenio Europeo en Materia Penal, Abierto a la firma el17 de marzo de 1978 en Estrasburgo (STE no 99).

Como se aprecia, el Convenio armoniza su contenido con otros instrumentos legales en materia internacional lo que garantiza que los Estados parte automáticamente concierten sus cuerpos legales al legislar con otros convenios y tratados en materia de derechos humanos. En consecuencia, el Convenio viabiliza su regulación con los convenios o tratados celebrados entre dos o más países, incluyendo los celebrados a futuro, considerando que ningún tratado o convenio en la materia puede contradecirlo. Como puede colegirse, existen motivos racionales de reflexión para que el Estado de Guatemala se adhiera al Convenio, considerando que los esfuerzos para contrarrestar el ciberdelito no circunscriben solo a una ley, sino, en desarrollar otras estrategias focalizadas a la prevención, tecnificación y logística para minimizar los efectos de los delitos informáticos.

Referencias

Constitución Política de la Republica de Guatemala. [Const]. 1985. (Guatemala).

Convenio sobre la Ciberdelincuencia. Artículo 39. 23 de noviembre de 2001.

Decreto número 57-2008 de 2008 [con fuerza de ley]. Por medio del cual se expide la Ley de Acceso a la Información Pública. 22 de octubre de 2008.

Decreto o Decreto 39-2022 [con fuerza de ley]. Por medio del cual se expide la Ley de Prevención y Protección Contra la Ciberdelincuencia. 2 de agosto de 2022.

Hall, A. (s.f.). Tipos de delitos informáticos. http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

Méndez, R. (4 de agosto de 2022) Pleno Aprueba Ley Contra la Ciberdelincuencia. https://www.congreso.gob.gt/noticias_congreso/8867/2022/4

Ministerio de Justicia y Derechos Humanos de Argentina. (2022.) ¿Qué es el ciberdelito? https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

Oficina de las Naciones Unidas Contra la Droga y el Delito, ONODC. (2020.) La ciberdelincuencia, en resumen. https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html

Solórzano, S. (18 de agosto de 2022). Van más de 3,500 denuncias por delitos a través de redes sociales en Guatemala. *Prensa Libre.* https://www.prensalibre.com/guatemala/justicia/van-mas-de-3500-denuncias-por-delitos-a-traves-de-redes-sociales-en-guatemala/