

LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN EN EL CÓDIGO PENAL

THE INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE CRIMINAL CODE

■ **ESP. JESÚS RAMÓN GARCÍA RUIZ**

Magistrado, Sala de lo Penal, Tribunal Supremo Popular, Cuba

<https://orcid.org/0009-0007-8495-2680>

jesus@tsp.gob.cu

■ **M.Sc. INGRYD TERESA SANTOS DÍAZ**

Magistrada, Sala de lo Penal, Tribunal Supremo Popular, Cuba

<https://orcid.org/0009-0005-1991-2645>

ingryd@tsp.gob.cu

Resumen

El artículo ofrece los elementos básicos sobre el tratamiento que la ley penal sustantiva dispensa a las telecomunicaciones, las tecnologías de la información y la comunicación, y sus servicios, como bien jurídico necesitado de una particular protección, conforme al marco constitucional vigente desde 2019, asunto de suma importancia y actualidad en la sociedad cubana. A ese efecto, su primer propósito es el de servir como guía para una mejor comprensión de las regulaciones que contiene el nuevo Código penal. La exposición parte de los antecedentes más significativos del tema en el ordenamiento interno y el internacional, para, luego, abordar el tratamiento específico concedido a la protección de aquellas en el mencionado texto normativo.

Palabras clave: Telecomunicaciones; tecnologías de la información y la comunicación; delitos cibernéticos; contravenciones; instrumentos jurídicos internacionales.

Abstract

The article offers basic elements on the treatment that substantive criminal law gives to telecommunications, information and communication technologies and their services, as a legal asset in need of particular protection, in accordance with the constitutional framework in force since 2019, a matter of great importance and topicality in Cuban society. To this end, its first purpose is to serve as a guide for a better understanding of the regulations contained in the new Criminal Code. The exposition starts with the most significant background of the subject in domestic and international law, and then addresses the specific treatment given to those in the aforementioned regulatory text.

Keywords: *Telecommunications; information and communication technologies; cybercrimes; contraventions; international legal instruments.*

Sumario

I. Introducción; II. Antecedentes; III. Marco internacional de referencia; IV. Variantes de protección; 4.1. El espectro radioeléctrico; 4.2. Nueva circunstancia agravante de la responsabilidad penal; 4.3. Figuras penales agravadas; 4.4. Delitos contra la integridad de las telecomunicaciones y el universo informático; V. Conclusiones; VI. Referencias.

I. INTRODUCCIÓN

Según reflexiona Rovira del Canto (2001, pp. 457-508), la comunidad mundial se enfrenta a una segunda revolución industrial, la denominada *revolución informática*, que está sustituyendo el trabajo de las mentes humanas por máquinas, lo que califica como la *era de la información*, en la cual aparece una nueva sociedad, la *digital*, con una cibercultura y un ciberespacio propios y peculiares, en el que cada sujeto puede ser, potencialmente, emisor y receptor en un medio cualitativamente diferenciado, que constituye un mundo virtual segregado por la comunicación.

Por otra parte, este autor advierte que el lado negativo de esa nueva era, conocida también como *sociedad global del riesgo y de la información*,

plantea problemas nuevos para el Derecho, que son de crucial trascendencia, desde el punto de vista de la necesaria protección que deben recibir el funcionamiento y la seguridad de los sistemas informáticos y telemáticos, mediante los cuales se ejecuta un inusitado tráfico jurídico, que pasa por las esferas de los negocios, las relaciones comerciales, la administración y la sociedad en general, dependientes, cada vez más, de aquellos sistemas para su sostenimiento y desarrollo en tiempo real (Rovira del Canto, 2001, pp. 457-508).

Como bien se razona en el preámbulo de la Resolución 74/247 de la ONU, «Lucha contra la utilización de las tecnologías de la información y las comunicaciones [TIC] con fines delictivos», aprobada por la Asamblea General el 27 de diciembre de 2019, en aquel escenario se ponen de manifiesto varios desafíos, pues, si bien es cierto que las TIC encierran un enorme potencial para el desarrollo de los Estados, también lo es que generan nuevas oportunidades para los delincuentes y contribuyen a un incremento de la criminalidad y la complejidad de los delitos.

En esta situación, las tecnologías emergentes, como la inteligencia artificial, ofrecen posibilidades para prevenir y combatir el uso de las TIC con fines delictivos, fortaleza que va acompañada del riesgo real de su utilización para mejorar el rendimiento del delito y su impunidad. Es un hecho demostrado que la tasa y la diversidad de delitos cometidos en el mundo digital han aumentado, al igual que sus efectos nocivos sobre la estabilidad de la infraestructura esencial de los Estados, las empresas y el bienestar de las personas; la masa de delincuentes que se están sirviendo de las TIC para llevar a cabo sus actividades muestra una tendencia creciente, motivada por el dominio operacional que han desarrollado sobre estas tecnologías, en una sociedad dependiente de ellas, lo que trae como consecuencia que se haya amplificado el espectro de bienes jurídicos que se afectan por hechos cada vez más graves y lesivos, entre ellos, algunos tan sensibles como los derechos humanos y la seguridad de los Estados (ONU, 2020, p. 1).

Por tanto, según se afirma en el «Informe sobre la ejecución de la Estrategia de ciberseguridad de la Unión Europea para la década digital» (Comunicación conjunta al Parlamento Europeo y al Consejo), deviene incuestionable que el panorama del mundo globalizado convierte tales desafíos en reales amenazas, que se ponen de manifiesto en un incremento de las actividades cibernéticas malintencionadas que afectan la seguridad y la integridad de los productos y los servicios de las TIC, el

ciberspacio mundial y abierto, los derechos humanos, las libertades democráticas y los Estados (2021, p. 5).

Ante ese contexto de desafíos y amenazas, el maestro Fernández Bulté (1996), con su genial estilo criollo, graficó que la delincuencia ya se estaba moviendo a una velocidad inalcanzable, en aviones y autos sofisticados, mientras que el sistema penal lo hacía en vetustos coches tirados por caballos.¹

En el escenario actual, el profesor hubiera dicho que una parte importante de esa delincuencia ni siquiera se percibe en el espacio físico y que, ordenador por medio, usa, disfruta y abusa, a sus anchas, del espacio virtual para desplazarse, en milésimas de segundos, hasta cualquier lugar, más allá del planeta llamado Tierra, el que, para ellos, ya no forma parte de la Vía Láctea porque lo han movido hacia otra nube distinta, la *nube digital*, cuya creación por la inteligencia humana estuvo enfocada en objetivos y fines más dignos y respetables que los de cualquier actividad delictiva.

Por otra parte, en la Recomendación de la Conferencia de ministros de Justicia de los países iberoamericanos, relativa a la tipificación y sanción de la ciberdelincuencia, derivada de diversos intercambios técnicos y político-criminales (Buenos Aires, 2011; Montevideo, 2012; Madrid, Bogotá, Lima y Viña del Mar, 2013) se planteó, oficialmente, que las legislaciones penales todavía estaban permeadas de importantes carencias en los tipos penales referidos al ciberdelito, lo cual permitía que la delincuencia individual y la organizada lesionasen importantes bienes jurídicos o los pusieran en grave riesgo. Ello derivó en la propuesta de incorporar o armonizar, según el caso, las normas jurídicas penales nacionales, mediante la tipificación de determinadas conductas, para enfrentar el fenómeno antes descrito; la gestión de una mayor eficacia en la prevención, persecución y penalización de tales comportamientos delictivos; y el perfeccionamiento de la cooperación jurídica internacional, en función de la reducción de los espacios de impunidad (2014, pp. 1-2, 5).

Con anterioridad a la reforma del sistema jurídico-penal que se generó en Cuba a partir de 2021, esa crítica objetiva le venía como traje a la medida, ya que era notorio su rezago con respecto a la manera en que

¹ Nota tomada por el coautor durante la intervención del insigne jurista en el Seminario internacional sobre administración de justicia penal en América Latina (La Habana, 1996), inédita.

la comunidad internacional y muchos países estaban abordando la protección de las TIC en sus ordenamientos jurídicos penales, aunque desde 2015 —en la Conferencia de las Naciones Unidas sobre comercio y desarrollo, en el examen de la armonización de la ciberlegislación en América Latina— se había reconocido que este tema se encontraba en proceso de revisión, como parte de la reforma al Código penal de 1987 (2015, p. 30), para incluir diversos delitos informáticos.

La modernización se erigió, después, en una exigencia, derivada de los cánones que impone la Constitución de la República (CRC), en sus artículos 8, 11 y 16, incisos i) y m) [GOR-E (5), 2019, pp. 72-74], en los que se refrenda que los tratados internacionales ratificados por el Estado cubano se integran a la ley interna; que el espectro radioeléctrico forma parte del territorio nacional, sobre el cual el Estado ejerce su soberanía; y que, en el marco del ejercicio de su función soberana, aquel disfruta del pleno derecho a regular el uso y los beneficios de las telecomunicaciones en su territorio, conforme a la práctica universal y los compromisos internacionales dimanantes del Convenio, la Constitución y el Reglamento de la Unión Internacional de las Telecomunicaciones (UIT) (2012, s.p.), así como a condenar la utilización ilícita del ciberespacio y el espectro radioeléctrico para subvertir el orden y desestabilizar la nación. En el Artículo 2 del Decreto-Ley No. 35, de 13 de abril de 2021 [GOR-O (92), 2021, p. 2526], se define que las telecomunicaciones consisten en la transmisión, emisión o recepción a distancia de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

La actualización constituyó una de las políticas más trascendentales en la reforma del sistema legal penal, el que hoy cuenta con las leyes 143, Del proceso penal (LPRP) [GOR-O (140), 2021, pp. 4095-4251]; 147, Del proceso penal militar (LPRPM) [GOR-E (12), 2022, pp. 575-715]; 151, Código penal (CPE) [GOR-O (93), 2022, pp. 2557-2696] y 152, De ejecución penal (LEP) [GOR-O (94), 2022, pp. 2697-2738], complementadas con otras disposiciones normativas. En sus textos, no solo se desarrollan los preceptos destinados a la tutela de la integridad de las *telecomunicaciones, las TIC y sus servicios* (TEL-TIC-SER), en tanto bienes jurídicos, sino que, también, se garantiza el empleo eficaz y seguro de estos en la investigación, la persecución y el juzgamiento de los hechos delictivos, y en el cumplimiento de las sanciones impuestas a quienes los cometan.

Sin duda alguna, el movimiento de reforma del sistema normativo penal cubano se erige en un claro ejemplo de la pretensión del legislador de dotar al operador jurídico nacional de un moderno conjunto de instrumentos legales, que acerque sus posibilidades a las de la nueva generación de delincuentes, la mayoría de ellos nativos de la *era digital*, y, así, poder aproximarse a las velocidades con las que estos circulan en los espacios físicos y digitales.

La exposición que sigue ofrece a los operadores del sistema penal una visión general respecto a la manera en que se diseñaron los elementos básicos del proceso de modernización; se aspira a que sirva de guía para un estudio más profundo sobre el tema. A ese efecto, se identifican y desarrollan los antecedentes legales más significativos sobre la materia, en ley interna y en la internacional, así como las distintas variantes que el texto del CPE [GOR-O (93), 2022, pp. 2557-2696] emplea para proteger las TEL-TIC-SER.

Para abordar estos contenidos, se aplicaron diversos métodos y técnicas de investigación, entre los cuales resaltan el histórico-jurídico, el exegético-analítico, la revisión bibliográfica y el análisis de documentos, cuya combinación permitió aproximarse al cumplimiento del objetivo básico antes mencionado.

II. ANTECEDENTES

Si se busca desde el pasado, se encuentran normas jurídicas, penales y administrativas, que sirven como claros antecedentes del tema expuesto en este trabajo.

Un primer ejemplo, en el sistema jurídico-penal histórico, aparece en la Ley de enjuiciamiento criminal española, de 14 de septiembre de 1882, hecha extensiva a la Cuba colonial por Real Decreto de 19 de octubre de 1888, la que, en sus artículos del 816 al 823, instituyó un procedimiento especial para los *delitos cometidos por medio de la imprenta, el grabado u otro medio mecánico de publicación* (Núñez, 1954, pp. 30-32), en tanto se trataba de hechos delictivos que requerían un tratamiento procesal diferenciado, debido a su peculiar forma de ejecución y a la efectividad que implicaba el uso de tales medios, al sobredimensionar los efectos negativos del ilícito.

Por ende, esta preceptiva, preminentemente, estaba enfocada en la obtención de los medios de pruebas necesarios y la ocupación de

los instrumentos o efectos de ciertos delitos que ya estaban tipificados en el Código penal español de 1870, respecto a los cuales Antón Oneca (1970) comenta que, desde la invención de la imprenta, los poderes públicos se preocupaban bastante por controlar esta fuente de difusión y propaganda con fácil clandestinidad, y añade que, cuando el Gobierno ordenó a la comisión codificadora la inclusión —en el proyecto de código que se estaba elaborando— de tales tipos penales que ya estaban en una ley especial, la respuesta de sus miembros al encargo fue presentar su renuncia en pleno, argumentando que, con el régimen común, serían responsables hasta los vendedores de periódicos (pp. 239-240).

Por otra parte, el Código de defensa social (CDS) (Publicación de legislaciones, 1973), promulgado el 4 de abril de 1936, mediante el Decreto-Ley No. 802 [GOR-E (108), 1936], cuya puesta en vigor se suspendió por dos años hasta 1938, en su Artículo 41, inciso v (p. 54), estableció, como una interesante circunstancia agravante proveniente del hecho, que este se ejecutara por medio de imprenta, grabado, cuadros expuestos al público, cinematógrafo, proyecciones luminosas, radiotelégrafo, teléfono, radioteléfono, televisión o cualquier otro medio de difusión.

Además, en su Artículo 479 (Título X, Capítulo II) sancionaba a los que:

A) Impidieran o entorpecieran las comunicaciones telegráficas, telefónicas, semafóricas o radiofónicas, de uso público, destruyendo o inutilizando los aparatos u objetos destinados a tales servicios, produciendo la dispersión de la corriente o inutilizando cualquier otro medio semejante; y B) Sin la autorización correspondiente, construyeren, instalaren u operaren ilegalmente estaciones trasmisoras de radio, o líneas o tendidos de telégrafo o telefónico. (pp. 345-346)

En la Ley No. 21, de 15 de febrero de 1979 [GOR-O (3), 1979, pp. 47-268], que derogó el CDS, se suprimió la citada circunstancia agravante de la responsabilidad penal y se abordó el asunto en dos tipos penales:

- El de *propaganda enemiga*, previsto en el Artículo 108 (p. 85), que formaba parte de los delitos contra la seguridad interior del Estado e incluía, como una condición objetiva de punibilidad, la agravación del marco sancionador cuando, para la ejecución de los hechos, se utilizaban medios de difusión masiva, además de penalizar, en otro apartado, al que permitiera la utilización de estos medios con aquel fin.

- El de *posesión u operación de un equipo transmisor sin autorización*, previsto en el Artículo 250 (p. 118), en la familia de los delitos contra el orden público y en el que se sancionaba a la persona que poseyera u operara un equipo radiotransmisor sin la debida autorización o con abuso de esta, siempre que el hecho no integrara un delito de mayor entidad. De esta forma, se incluyó el tipo legal del Artículo 479 B) (pp. 345-346) de la ley sustantiva derogada.

La Ley No. 62, de 29 de diciembre de 1987, Código penal (CP) [GOR-E (3), 1987, pp. 57-157], siguió el mismo sendero que su predecesora, sin introducir cambios en las expectativas vinculadas con estos temas.

Ante la creciente tendencia a utilizar las nuevas tecnologías electrónicas para proteger el patrimonio y el notorio cambio de actuación de la delincuencia, con la Ley No. 87 de 1999, se extendió el tradicional concepto de *llaves* que contenía el Artículo 328, inciso c), del CP, relacionado con el delito de robo con fuerza en las cosas, para estimar como tales, además, *las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia u otros de iguales propósitos*; con ello, se suplió la laguna legal existente hasta ese momento, que había generado decisiones judiciales injustas, al penalizar, como hurto, hechos delictivos en los que el agente activo accedió al lugar donde estaban ubicados los bienes ajenos haciéndose, subrepticamente, de estos modernos medios de seguridad (Université de Fribourg, 2008, p. 10).

Esta definición legal reproduce la del párrafo tercero del Artículo 239 del Código penal español de 1995 (Morales, Fernández y Álvarez, 2018, pp. 804-807), con la única diferencia de que la cubana añade la expresión «u otros de iguales propósitos», para cubrir cualquier tecnología futura que fuera puesta en práctica o uso, con el objetivo de asegurar los bienes muebles de posibles sustracciones.

Otro antecedente, de mucha inmediatez en este caso, fue la Ley No. 93, de 20 de diciembre de 2001, Contra actos de terrorismo [GOR-E (14), 2001, pp. 63-70], la que, en su Artículo 24, estableció el delito de «actos en ocasión del uso de los medios y técnicas informáticas [sic]», que fijaba la sanción de cinco a 20 años de privación de libertad contra la persona que, para facilitar cualquiera de los hechos ilícitos previstos en dicha ley:

- a) Utilice equipos, medios, programas, redes informáticas o cualquier otra aplicación informática, intercepte, interfiera, use, altere,

dañe, inutilice o destruya datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de información y de comunicaciones o telemáticos, de servicios públicos, sociales, administrativos, de emergencia, de seguridad nacional o de cualquier otro tipo, de entidades nacionales, internacionales o de otro país;

b) haga uso o permita la utilización de correo electrónico, otros servicios o protocolos de internet, o de cualquier equipo terminal de telecomunicaciones;

c) cree, distribuya, comercie o tenga en su poder programas capaces de producir los efectos a que se refiere el apartado a). (p. 68)

Este tipo legal se reprodujo en el Artículo 168 del CPE [GOR-O (93), 2022, pp. 2613-2614], cuya aplicación, en virtud del principio de especialidad, será preferente a las modalidades comisivas que aparecen en la familia de los delitos contra la integridad de las TEL-TIC-SER, porque así lo exige el Artículo 149 del propio texto (p. 2609), cuando, por la forma de ejecución del hecho, o por los medios y métodos empleados, se evidencie que el sujeto activo tiene el propósito de intimidar u obligar a un gobierno o a una organización internacional a realizar un acto o abstenerse de realizarlo o, de igual manera, provocar estados de alarma, temor o terror en la población, en un grupo de personas o en una determinada, poner en peligro inminente o afectar la vida, la integridad física o mental de estas, provocar afectaciones a bienes de significativa consideración o importancia, el medio ambiente, la paz internacional o la seguridad del Estado cubano.

Con el Decreto-Ley No. 389 de 2019 [GOR-E (27), 2019, pp. 155-159], se modificaron las leyes sustantiva y procesal de ese momento, lo que trajo consigo la introducción de las técnicas especiales de investigación que, en la actualidad, se definen en el Artículo 327 de la LPRP [GOR-O (140), 2021, p. 4155], como los métodos para la obtención de la información que utilizan recursos técnicos, tecnológicos, humanos o de otras características, de acuerdo con la actividad delictiva de que se trate, aplicados por los encargados de la investigación y la instrucción penal. De conformidad con el Artículo 328.2, tales técnicas han de resultar «idóneas o necesarias para la investigación de hechos delictivos concretos que por su gravedad, connotación u organización lo requieran, incluyendo operaciones cuyo origen o destino sea el exterior del país»,

conforme a las regulaciones establecidas para la cooperación jurídica internacional (p. 4155).

En esa última disposición se inserta la *vigilancia electrónica* que conceptualiza el Artículo 338 (p. 4156), entendida como aquella en la que se utilizan medios para la interceptación y el registro de escuchas y grabación de voces, localización y seguimiento de personas, objetos o bienes, fijaciones fotográficas y filmación de imágenes, intervención de los medios informáticos y sus soportes de información, programas y sistemas operativos o de aplicaciones o de otras TEL-TIC-SER, que permitan conocer y demostrar el hecho delictivo.

La LPRP [GOR-O (140), 2021, pp. 4095-4251] y su similar, la LPRPM [GOR-E (12), 2022, pp. 575-715] representan, en sí mismas, un evidente esfuerzo del legislador cubano por modernizar el proceso penal y ponerlo a tono con la era en que les toca regir, a cuyo efecto basta citar el Artículo 47.1 (p. 4102), en el que se regula la posibilidad de aplicación o utilización de los medios científico-técnicos y las TIC que resulten útiles e indispensables, en las actuaciones y diligencias del proceso penal, siempre que se garantice el debido proceso, la integridad, plenitud, autenticidad, confidencialidad y seguridad de los datos e informaciones que contengan, y el respeto al honor y la integridad moral de las personas.

Otros ejemplos de la renovación procesal penal se reflejan en:

- Los artículos 325 y 326 (pp. 4154-4155), que regulan la captación y grabación de las comunicaciones orales y de la imagen, mediante la utilización de dispositivos electrónicos u otros medios técnicos e informáticos, con el objetivo de probar la existencia del delito, la participación de los intervinientes o cualquier otra circunstancia con trascendencia jurídico-penal.
- Los artículos 469, 470 y 473 (pp. 4181-4182) que abren la posibilidad de celebrar el juicio oral por medio de videoconferencia.
- El Artículo 742.1 k) (p. 4229), en el que se incluyen, entre las variantes de la asistencia penal internacional, las solicitudes para conservar y revelar datos electrónicos, incluidos los referidos al tráfico almacenado por medio de sistemas o dispositivos informáticos, para la obtención de pruebas durante la investigación y persecución de delitos, con particular destaque de los vinculados con la corrupción administrativa y económica, el crimen organizado transnacional, el terrorismo, el tráfico

y la trata de personas y el de drogas o sustancias de efectos similares, que tienen una especial relevancia negativa para la comunidad mundial y, a ese efecto, son abordados en diferentes tratados internacionales.

- El Artículo 743.2 (p. 4229), en el que se especifica que las solicitudes de asistencia penal internacional se tramitan utilizando la transmisión electrónica o cualquier otro medio seguro, y mediante escrito cursado por la vía diplomática, con el cumplimiento de ciertos requisitos taxativamente relacionados en el precepto.

Unidos a los mencionados, existen otros precedentes de Derecho administrativo no menos importantes, que han regulado o regulan la materia en estudio, entre los cuales han de mencionarse los siguientes:

- El Decreto No. 171, de 30 de abril de 1992 [GOR-O (5), 1992, pp. 49-52], que compendió en tres artículos lo que se debe entender y penalizar como contravenciones personales de las regulaciones del uso del espectro radioeléctrico.

- El Decreto-Ley No. 157, de 18 de enero de 1995 [GOR-O (5), 1995, pp. 65-68], sobre los servicios de telecomunicaciones de carácter limitado, cuyo objetivo fue el de otorgar facultades más flexibles y autónomas al organismo rector de las comunicaciones en el país, para permitir utilizar las nuevas modalidades de los servicios y sistemas de telecomunicaciones generados por el desarrollo tecnológico e introducidos en el territorio nacional, de conformidad con las normativas técnico-operacionales y demás disposiciones dictadas en situaciones coyunturales. Esta normativa también diseñó un régimen contravencional, que prevé como posibles sanciones la suspensión temporal de la licencia y la clausura de las instalaciones implicadas, la imposición de multa y el decomiso administrativo de los medios empleados, con independencia de las responsabilidades penales en que pudiera quedar incurso el infractor.

- La Resolución No. 98, de 17 de abril de 1997 [GOR-O (16), 1995, pp. 248-250], del ministro de Comunicaciones,² que dio carácter *limitado* al servicio de telecomunicaciones destinado al turismo, el cuerpo diplomático acreditado en el país y otras personas admitidas, mediante contratación, decisión que se adopta al detectarse que personas no autorizadas habían logrado descodificar, interceptar o recibir e, incluso, distribuir a terceros ese servicio, con fines comerciales, o no.

² El entonces Ministerio de Comunicaciones pasará, luego, a denominarse Ministerio de la Informática y las Comunicaciones.

- La Resolución No. 99, 17 de abril de 1995 [GOR-O (16), 1995, pp. 250-252], del ministro del ramo, que declaró *limitadas* las señales de televisión no nacionales; a tales efectos, en el apartado tercero de la norma se establecieron determinadas especificaciones para el uso de antenas y demás dispositivos destinados a la recepción de señales de televisión por personas naturales o jurídicas nacionales, en edificios públicos, multifamiliares, viviendas y demás inmuebles.
- La Resolución No. 127, de 24 de julio de 2007 [GOR-O (57), 2007, pp. 899-910], que dictó el mencionado ministro, destinada a implementar el Reglamento de seguridad para las tecnologías de la información, que faculta a los inspectores designados a imponer, a los infractores, las sanciones administrativas u otras medidas punitivas previstas en su Artículo 99 (p. 908), entre las que se encuentran:
 - a) La invalidación temporal o definitiva de las autorizaciones concedidas por el Ministerio de la Informática y las Comunicaciones (MIC);
 - b) la suspensión y/o cancelación temporal o definitiva de los servicios de informática y comunicaciones;
 - c) la ocupación cautelar de los medios, instrumentos, equipamientos y otros utilizados para cometer la infracción, y el posterior decomiso de estos; y
 - d) la aplicación de otras medidas que correspondan en ley.

Por último, como parte de la función tutelar de determinados bienes jurídicos relevantes para la sociedad, el legislador se enfocó en concordar lo más posible el texto del CPE con el resto del ordenamiento jurídico vigente sobre TEL-TIC-SER, sobre todo en cuanto al deslinde entre los hechos que pudieran constituir contravenciones y los que se elevarían al rango de delitos; a ese fin, tomó en cuenta lo establecido en las siguientes disposiciones jurídicas:

- El Decreto-Ley No. 370, de 17 de diciembre de 2018 [GOR-O (45), 2019, pp. 763-777], sobre la informatización de la sociedad cubana, que estatuye un sistema de contravenciones y sanciones asociadas al uso de las TIC.
- El Decreto-Ley No. 360, de 31 de mayo de 2021 [GOR-O (92), 2019, pp. 786-801], sobre la seguridad de las TIC y la defensa del ciberespacio nacional, en el que, también, se plantea un conjunto de sanciones administrativas por el incumplimiento de la seguridad de las TIC.

- El Decreto-Ley No. 35, de 13 de abril de 2021, De las telecomunicaciones, las tecnologías de la información y la comunicación y el uso del espectro radioeléctrico [GOR-O (92), 2021, pp. 2525-2548].
- El Decreto No. 42 de 2021, de 24 de mayo de 2021, Reglamento general de las telecomunicaciones y las tecnologías de la información y la comunicación [GOR-O (92), 2021, pp. 2548-2562].
- El Decreto No. 43 de 2021, de 24 de mayo de 2021, Reglamento sobre el uso del espectro radioeléctrico [GOR-O (92), 2021, pp. 2562-2575].
- La Resolución No. 128, de 24 de junio de 2019 [GOR-O (45), pp. 831-840], del ministro de la Informática y las Comunicaciones (IC), referida al reglamento sobre la seguridad de las TIC y el ciberespacio nacional.
- Las resoluciones 105, 107 y 108, de 9 de agosto de 2021 [GOR-O (92), 2021, pp. 2575-2601], del titular del sector, que contienen, por su orden, las reglamentaciones sobre el modelo de actuación nacional para la respuesta a incidentes de ciberseguridad, el uso de los servicios de radiocomunicaciones por satélites, y la interconexión, el acceso y las instalaciones esenciales de redes de telecomunicaciones.

III. MARCO INTERNACIONAL DE REFERENCIA

Ante la tendencia exponencial al alza de la ciberdelincuencia, la comunidad mundial ha tomado conciencia clara de la utilidad que tienen los instrumentos jurídicos internacionales, para encauzar los esfuerzos hacia la gestión de opciones que fortalezcan las respuestas jurídicas o de otra índole, a nivel nacional e internacional, para enfrentar el fenómeno.

El CPE [GOR-O (93), 2022, pp. 2557-2696] hubiera constituido una pieza demasiado imperfecta y descontextualizada, de no haber tenido en cuenta los referentes de varios instrumentos jurídicos internacionales que sientan pautas relacionadas con la protección de las TEL-TIC-SER, entre los que aparecen los siguientes:

- El Convenio, la Constitución y el Reglamento de la UIT (2012, s.p.). Los textos fueron adoptados por la Conferencia de Plenipotenciarios y toman como bases las actas finales de varios encuentros similares (Ginebra, 1992; Kioto, 1994; Minneapolis, 1998; Marrakech, 2002; Antalya, 2006; Guadalajara, 2010; Busán, 2014 y Dubái, 2018). En esta última reunión, los representantes de los Estados parte se enfocaron en:

a) El fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las TIC.

b) La función de la UIT en la protección de la infancia en línea.

c) La lucha contra la falsificación de dispositivos de telecomunicaciones y tecnologías de la información y la comunicación.

d) La asistencia a los Estados miembro para combatir y disuadir el robo de dispositivos móviles.

e) La protección del usuario/consumidor de servicios de telecomunicaciones.

f) El papel de la UIT en el fomento del uso de las TIC para combatir la trata de personas.

- El Convenio de Budapest, de 23 de noviembre de 2001 (Organización de Estados Americanos, s.f.), relativo al enfrentamiento a la cibercriminalidad en el marco europeo, en cuyo preámbulo se deja constancia expresa de:

a) La necesidad de llevar a cabo, con prioridad, una política penal común destinada a prevenir la criminalidad en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional.

b) La preocupación que suscita el riesgo de que las redes informáticas y la información electrónica sean utilizadas para cometer infracciones penales y que las pruebas de dichas infracciones sean almacenadas y transmitidas por medio de esas redes.

c) La urgencia de que la lucha contra la cibercriminalidad esté bien organizada, lo que precisa de una cooperación internacional en materia penal acrecentada, rápida y eficaz.

- Las declaraciones de los congresos internacionales sobre el tratamiento al delito y la justicia penal, celebrados en Doha (2015) y Kioto, (2021); documentos en los que se convoca a la prevención y el enfrentamiento eficaz de las actividades delictivas contra las TIC.

- Las Recomendaciones de las reuniones de la Red Iberoamericana de Ministerios Públicos especializados en ciberdelincuencia, celebradas en Lisboa (2018) y Santiago de Chile (2019), así como las de la Conferencia regional de políticas y estrategias sobre ciberdelitos en la Comunidad del Caribe, celebrada del 12 al 14 de junio de 2019 en Santo Domingo (2019).

De especial trascendencia resulta el proyecto de Convención de la Organización de las Naciones Unidas sobre la lucha contra la utilización de las TIC con fines delictivos (2021), presentado por Rusia, el 29 de junio de 2021, a la Secretaría de ese organismo internacional, como resultado de las labores ejecutadas por el Comité intergubernamental especial de expertos designados a ese efecto en cumplimiento de la Resolución 74/247, de la Asamblea General de la ONU, de 27 de diciembre de 2019 (ONU, 2020).

Dicho proyecto se encuentra en proceso de emisión de criterios por parte de los Estados miembro del organismo internacional; en agosto de 2022, el TSP explicó al órgano nacional de relaciones, encargado de acopiar aquellos, los avances obtenidos en este campo, a partir del tratamiento dispensado a esta materia en la legislación que integra el sistema jurídico-penal cubano, recién reformado.

En cuanto al texto de la futura convención, merecen destaque sus propósitos, que serán:

a) Promover y fortalecer las medidas para una prevención eficaz de los delitos y otros hechos ilícitos en la esfera de las TIC y la lucha contra estos.

b) Prevenir los actos contra la confidencialidad, integridad y accesibilidad de las TIC e impedir los abusos en la esfera de su utilización, proporcionando la punibilidad de los actos que abarcaría la convención y potenciando la autoridad suficiente para una lucha eficaz contra tales delitos y otros hechos ilícitos, facilitando su detección, investigación y la persecución de sus autores, tanto a nivel nacional como internacional, mediante acuerdos de cooperación entre los Estados.

c) Desarrollar una cooperación internacional de mayor eficiencia, que incluya la capacitación y prestación de asistencia técnica en la prevención de delitos en la esfera de las TIC y la lucha contra estos.

A contrapelo de las crecientes tendencias globalizadoras que pretenden reducir a la nada el concepto real de soberanía nacional, el Artículo 3 (2021, p. 5) reconoce que los Estados parte cumplirán sus obligaciones con arreglo a ese futuro instrumento internacional, en consonancia con los principios de la soberanía estatal, la igualdad soberana de los Estados y la no intervención en los asuntos internos de otros; sin que cualquiera de ellos quede facultado para ejercer, en territorio extranjero, la jurisdicción y las funciones que la legislación nacional de ese otro

reserve exclusivamente a sus órganos, a menos que la propia conven-
ción disponga alguna cláusula diferente.

Desde el Artículo 5 hasta el 27 (pp. 8-18), se propone un significativo
conjunto de hechos para que sean tipificados como delitos en la ley
interna de los futuros Estados parte; la mayoría de ellos ya fueron taxa-
tivamente previstos en el CPE [GOR-O (93), 2022, pp. 2557-2696]. Son
de resaltar los siguientes:

a) El acceso indebido a la información digital, su interceptación y mani-
pulación ilícita. El Artículo 4 i) se refiere a los materiales (datos), inde-
pendientemente de su formato y sus características, contenidos en (y
procesados por) dispositivos, sistemas y redes de la información y las
comunicaciones;

b) el mal funcionamiento de las redes de la información y las comu-
nicaciones, las que se identifican en el Artículo 4 g) como el conjunto
de equipamiento de ingeniería diseñado para gestionar los procesos
tecnológicos con el uso de los medios de comunicación y telecomuni-
caciones;

c) la creación, el uso y la distribución de programas malignos, concep-
tualizados en el inciso c) del mencionado precepto como aquellos cuya
característica objetiva es la modificación o eliminación, el copiado o
bloqueo no autorizado de la información o la neutralización de los me-
dios de protección de la información en formato digital;

d) la manipulación ilícita de la infraestructura crítica de la información,
que, de acuerdo con lo previsto en el Artículo 4 m), es el conjunto de
instalaciones de la infraestructura crítica de la información, al igual que
las redes de comunicación utilizadas para organizar la interacción
de las instalaciones de la infraestructura crítica de la información entre
sí; a tono con el inciso n), tales instalaciones comprenden los sistemas
de información y las redes de información de las autoridades guberna-
mentales, y los sistemas de información e informatizados para la ges-
tión de los procesos tecnológicos en el ámbito de la industria de la
defensa, la sanidad, la enseñanza, el transporte, las comunicaciones,
la energía, la esfera crediticio-financiera, la nuclear y otras importantes
de la vida del Estado y la sociedad;

e) el acceso no autorizado a los datos personales. En Cuba, la Ley
No. 149, de 14 de mayo de 2022, De protección de los datos perso-
nales [GOR-O (90), 2022, pp. 2463-2479], en su Artículo 3 (p. 2464),

define estos como la información concerniente a una persona natural identificada o identificable, que puede llevar a su identificación; además, aclara que una persona es identificable cuando su identidad puede determinarse, directa o indirectamente, por medio de cualquier información;

f) el tráfico ilícito de dispositivos elaborados o adaptados para cometer alguno de los delitos identificados en la convención;

g) el empleo de las TIC en delitos convencionales de robos, producción y tráfico de materiales u objetos con pornografía de menores de edad, inducción al suicidio o su provocación, hechos en los que se involucran menores en la comisión de ilícitos y pongan en peligro su vida o salud, elaboración y utilización de la información digital para confundir al usuario, incitación a la actividad subversiva o armada, el terrorismo y las actividades extremistas, distribución de estupefacientes o sustancias sicotrópicas, tráfico de armas, rehabilitación del naciismo, justificación del genocidio o crímenes contra la paz y la humanidad, distribución ilícita de medicamentos y artículos médicos falsificados, hechos reconocidos como delitos con arreglo al Derecho internacional, infracción de derechos de autor y derechos conexos.

El proyecto deja a elección de los Estados parte el definir, como delito, en su ley interna, cualquier otro hecho ilícito cometido, premeditadamente, con la utilización de las TIC y que haya causado daños considerables.

IV. VARIANTES DE PROTECCIÓN

4.1. EL ESPECTRO RADIOELÉCTRICO

Conforme al Artículo 11 a) de la CRC [GOR-E (5), 2019, p. 72], el 4.1 a) del CPE [GOR-O (93), 2022, p. 2559] agrega el espectro radioeléctrico como elemento inmaterial de aplicación de la ley penal, lo que canaliza el ejercicio del derecho soberano del Estado cubano para tipificar como delitos y penalizar las agresiones de mayor connotación contra las TEL-TIC-SER en su territorio, en sintonía con la práctica universal y los compromisos internacionales contraídos en esa materia.

En el inciso l), del Anexo de definiciones de términos empleados en el CPE, se conceptualiza que el espectro radioeléctrico

constituye un recurso de carácter escaso, limitado, inalienable, imprescriptible e inembargable, sobre el cual el Estado ejerce su soberanía, y no puede cederse en propiedad a personas naturales o jurídicas; se conforma por las ondas radioeléctricas que se definen como las ondas electromagnéticas cuyo límite superior de frecuencia se fija convencionalmente por debajo de 3000 GHz, y que se propagan por el espacio sin guía artificial. (p. 2693)

Esta definición reproduce la que aparece en los artículos 96 y 97 del mencionado Decreto-Ley No. 35, de 13 de abril de 2021 [GOR-O (92), p. 2543], cuya virtualidad o inmaterialidad se erige en un gran desafío para los tradicionales principios relativos a la aplicación espacial del Derecho penal nacional, concebidos a la vista de elementos territoriales realmente tangibles, visibles y, hasta cierto punto, suficientemente controlables por el Estado, como son la tierra, el mar y el espacio aéreo.

4.2. NUEVA CIRCUNSTANCIA AGRAVANTE DE LA RESPONSABILIDAD PENAL

En el Artículo 80.1 q) del CPE [GOR-O (93), 2022, p. 2585] se prevé, como circunstancia agravante de la responsabilidad penal, la utilización de las TEL-TIC-SER, con el fin de facilitar la ejecución del delito, imposibilitar u obstruir su descubrimiento, o agravar sus consecuencias, la que puede aplicarse en cualquiera de los delitos previstos en la legislación sustantiva penal en los que sea factible emplear estas tecnologías y sus servicios, para lograr tales fines, excepto cuando el tipo legal lo incluya como uno de sus elementos objetivos, conforme a la regla establecida en el precepto 71.3 de la propia disposición (p. 2580).

En este sentido, se tomó en cuenta que la delincuencia se mueve hacia el uso cada vez más elevado de las TIC, para intensificar la efectividad de su labor ilícita, lo que incrementa la potencial lesividad social del delito, tanto por sus nocivas consecuencias como por la probabilidad de que los intervinientes activos queden impunes, debido a las dificultades reales de prevenir, detectar y enfrentar sus actos.

Esta previsión no es realmente novedosa en el sistema jurídico-penal sustantivo cubano, pues tuvo antecedente en el Artículo 41.V del vetusto CDS (Publicación de legislaciones, 1973, p. 165), después ausente en las posteriores leyes penales del país; con la reforma, se ha producido

una vuelta al pasado, adaptándolo a los nuevos tiempos. Su inserción en el texto legal fue objeto de disquisiciones y controversias; al efecto, se suscitaron dos posiciones:

1. La de quienes la consideraban necesaria, pero con una formulación general, parecida a la que tenía el CDS, en la que no importaba un objetivo concreto.
2. La de quienes alegaban que no era preciso tener en cuenta esa circunstancia porque, en un futuro inmediato, la tendencia estaría dirigida a que el delito fuera un fenómeno ciberdependiente, o sea, no concebido sin el uso de las TEL-TIC-SER. Este segmento planteaba, irónicamente, si sería pertinente una circunstancia atenuante, en lugar de la agravante, porque no estaba lejano el tiempo en el cual lo raro, inusual o extravagante sería que el hecho ilícito se cometiera mediante los métodos y medios tradicionales, por ejemplo, en un robo con fuerza en las cosas, fracturar una puerta a golpes de mandarina, cuando el agente tenga en su poder la tarjeta magnética que abre su mecanismo de seguridad.

Finalmente, el punto de equilibrio entre ambas posturas se halló en contemplar el empleo de estas tecnologías y sus servicios con determinados objetivos (facilitación del hecho delictivo, obstrucción de la investigación y persecución, magnificación de sus consecuencias lesivas).

4.3. FIGURAS PENALES AGRAVADAS

El legislador entendió que, al margen de la especial protección de las TEL-TIC-SER en una familia de delitos creada a ese efecto, otros tipos penales también debían recibir un incremento de las penalizaciones, cuando se cometieran con el empleo de medios informáticos, redes sociales o medios de comunicación social, en sus espacios físico y digital.

En tal sentido, el CPE [GOR-O (93), 2022] inserta dicha condición objetiva de punibilidad y sanciona el hecho con mayor rigor en los delitos siguientes:

- a) Propaganda contra el orden constitucional (Artículo 124.2.3, p. 2603).
- b) Difusión de noticias o predicciones falsas, con el propósito de provocar desórdenes o alteraciones públicos (Artículo 266.2, p. 2640).
- c) Instigación a delinquir (Artículo 268.4, p. 2640).

d) Falsificación de documentos públicos y bancarios o de comercio [Artículos 332.3 b) y 333.3 b)], «si los hechos consisten en introducir, alterar, borrar o suprimir datos informáticos que integran el documento, generando datos no auténticos, con la intención de que sean percibidos o utilizado [sic] en el tráfico jurídico como legítimos» (pp. 2658-2659).

e) Estafa [Artículo 423.3 e)], si «para ejecutar el hecho se introducen, alteran, borran o suprimen datos informáticos, o se interfiere de cualquier forma el funcionamiento de un sistema informático» (p. 2687).

f) Calumnia [Artículo 391.2 b), pp. 2675-2676].

g) Injuria [Artículo 392.2 b), p. 2676].

h) Actos contra la intimidad personal y familiar, la propia imagen y voz, identidad de otra persona y sus datos [Artículo 393.3 d), p. 2676].

i) Delitos contra la creación literaria y artística [Artículo 428.3 b)], si los hechos «se cometen a escala comercial y a través de medios o sistemas informáticos» (pp. 2688-2689).

A fin de lograr la mejor comprensión de esta condición objetiva agravante, el legislador identificó los medios de comunicación social como «las plataformas que comparten contenidos de interés público, a través de distintos formatos, canales y soportes» —Anexo 1 q) del CPE [GOR-O (93), 2022, p. 2694].

4.4. DELITOS CONTRA LA INTEGRIDAD

DE LAS TELECOMUNICACIONES Y EL UNIVERSO INFORMÁTICO

También, como consecuencia del necesario respeto al principio de legalidad que refrenda el propio texto jurídico penal en su Artículo 2.1 [GOR-O (93), 2022, p. 2558], y para satisfacer amplios reclamos de la doctrina y otros sectores de la sociedad cubana, el Título IX del CPE [GOR-O (93), 2022, pp. 2644-2646] contiene un conjunto específico de figuras típicas que están perfiladas para proteger determinados bienes jurídicos concretos, por lo que tienen vida propia, con independencia de otros tipos penales presentes en varias familias de delitos y que pueden ser cometidos empleando medios y tecnologías de esa naturaleza.

En cuanto a las ideas expuestas en el párrafo precedente, los expertos de los ministerios de IC y el Interior que intervinieron en la elaboración del anteproyecto de norma jurídica sustantiva pusieron especial énfasis en que esta familia de tipos delictivos, calificados por ellos como *deli-*

tos cibernéticos, tuviera una clara identificación de los bienes jurídicos que se protegen, en su caso la integridad, confiabilidad y disponibilidad de la información y las comunicaciones, además de la seguridad e indemnidad del equipamiento tecnológico y sus soportes, sin obviar que la ciberseguridad es un asunto de seguridad y defensa nacional en los momentos actuales, lo que permite que no sean confundidos ni mezclados con otros ilícitos que se cometen con el empleo de las TIC como instrumentos, o usando como medio los espacios virtuales que ofrecen las redes de comunicación social, que son los denominados *delitos cinéticos*, según la terminología que emplean comúnmente los especialistas en seguridad informática.

De lo anterior se infiere que la prioridad estuvo en que la nueva ley penal sustantiva ofreciera una tutela específica y concentrada, tanto al *software* como al *hardware* de los sistemas informáticos que, en la jurisprudencia española, se identifican como aquellos que permiten almacenar y procesar información, o sea, tanto las computadoras, impresoras, escáneres, memorias, lectores de código de barras, estructura de una red de computadoras, como los manuales de uso, sistema operativo, archivos, documentos, aplicaciones, bases de datos, entre otros (Morales, Fernández y Álvarez, 2018, p. 902), independientemente de que en ese texto normativo también debían coexistir ciertos tipos penales tradicionales que requerían una modernización producto del cambio en el modo de actuación de la delincuencia, ahora apoyada en el uso de las TEL-TIC-SER para atacar bienes jurídicos distintos a los que son objeto de análisis en el presente epígrafe.

Antes de reseñar las principales ideas respecto a figuras delictivas que integran esta familia, resulta necesario hacer referencia a algunos aspectos que son objeto de preocupaciones para un sector nada despreciable de los operadores jurídicos y de otras materias afines:

La creación de este nuevo conjunto de tipos penales ejemplifica la expansión del Derecho penal, sin que pueda decirse que se trata de una creación jurídico-positiva simbólica, a pesar de que hasta hoy en Cuba no haya sido juzgado ni uno de estos hechos típicos. Su inserción taxativa en el texto legal es necesaria por tres causas:

- *Primera:* La sociedad cada día se sumerge más en una dependencia de estas nuevas tecnologías, al punto de que llegará el momento en que nada se mueva sin su uso o aplicación.

- *Segunda:* Los nuevos delincuentes hicieron un infeliz y rápido descubrimiento del rendimiento adicional que les aporta su empleo a gran escala en la comisión de hechos ilícitos, a lo que se añade que también llegará el día en que, sin su uso y aplicación, poco podrán hacer en su faena criminal.
- *Tercera:* El vertiginoso desarrollo del Derecho internacional público en materia de prevención, investigación y enfrentamiento a los delitos cibernéticos y cinéticos, lo que ha dado paso a un creciente conjunto de instrumentos jurídicos internacionales que no pueden ser olvidados por el legislador en el proceso de creación de la ley interna del Estado, so pena de quedar al margen de la comunidad internacional.

Para poder incluir a las TEL-TIC-SER en la esfera de protección del Derecho penal, en atención a la vigencia del principio de legalidad que impera en la materia, era necesaria la transformación radical del tradicional concepto de *bienes*, cuya estima como cosas físicas no acoplaba con la inmaterialidad que tienen, por ejemplo, el espectro radioeléctrico y los casos de *software* o datos obrantes en un registro digital; se tornaba inteligente, entonces, mutar hacia otra definición legal que los abarcara.

De esa manera, en la disposición especial quinta a) de la LPRP [GOR-O (140), 2021, p. 4249] y en el apartado 1 e) de los términos y las expresiones anexos al CPE [GOR-O (93), 2022] se puntualizó que constituyen «bienes: los activos de cualquier tipo, corporales o incorporeales, muebles o inmuebles, tangibles o intangibles y los documentos o instrumentos legales que acrediten la propiedad u otros derechos sobre dichos activos» (p. 2693). En realidad, tal concepto es una reproducción del que aporta el Artículo 2 d) de la Convención de las Naciones Unidas contra la corrupción, aprobada mediante la Resolución 58/4 de la Asamblea General de esta organización, el 31 de octubre de 2003 (ONU, 2004, p. 8).

No obstante, en la práctica judicial cubana, ya había sido introducida una definición al respecto, por el Dictamen No. 441, de 17 de marzo de 2014, del Consejo de Gobierno del TSP [GOR-O (15), 2014, pp. 329-330], emitido en virtud de la consulta que hizo a este órgano el ministro-presidente del Banco Central de Cuba, con el propósito de precisar el alcance de aquel término jurídico para calificar los delitos contemplados en la Convención internacional contra la delincuencia organizada transnacional (2004, s.p.), así como para aplicar las sanciones accesorias

de comiso y confiscación de bienes. El máximo órgano judicial del país precisó que

bajo el concepto jurídico de bienes, figuran aquellas cosas que sirven al hombre para satisfacer sus necesidades, dando lugar a derechos reales que determinan relaciones jurídicas que, en correspondencia con lo normado en el apartado 1 del Artículo 46 del Código civil confieren a su titular, frente a cualquier otra persona jurídica o natural, la facultad de ejercitar su derecho dentro de los límites que establece el ordenamiento jurídico. (p. 329)

La determinación de las dinámicas consustanciales al territorio, el momento en el que se atacan o se usan las TEL-TIC-SER para la comisión de hechos delictivos, y el instante en que se producen sus efectos negativos, constituye un exigente ejercicio para los operadores del Derecho penal, en lo que concierne a la detección oportuna de hechos de esta naturaleza, su investigación efectiva y penalización.

Lo anterior se erige en una situación de orden empírico, más que teórico, porque la aplicación territorial, personal y temporal de la ley penal sustantiva a estos casos no debe constituir, en sí misma, un problema insalvable, habida cuenta de que el actual texto jurídico punitivo mantiene la tendencia de sus precedentes inmediatos, cuando se afilia a un criterio mixto, con predominio del principio de territorialidad, pero complementado por otros que posibilitan la aplicación extraterritorial (Quirós, 2002, pp. 55-56), entre ellos, el personal, regulado en los apartados del uno al tres, del Artículo 5, del CPE [GOR-O (93), 2022, p. 2560], que establecen que la ley penal cubana es aplicable a:

a) Los cubanos y personas sin ciudadanía residentes en Cuba, que cometan un delito en el extranjero, si se encuentran en Cuba o son extraditados.

b) Los cubanos que cometan un delito en el extranjero y sean entregados a Cuba para ser juzgados por sus tribunales, en cumplimiento de los tratados internacionales en vigor para la República de Cuba.

c) Los extranjeros y personas sin ciudadanía, no residentes en Cuba, que cometan un delito en el extranjero, si se encuentran en Cuba y no son extraditados, tanto si residen en el territorio del Estado en que se perpetran los actos como en cualquier otro y siempre que el hecho sea punible también en el lugar de su comisión; sin que sea exigible este último requisito, si el acto constituye un delito contra los intere-

ses fundamentales, políticos o económicos de la República de Cuba, o contra la humanidad, la dignidad humana o la salud colectiva, o es perseguible en virtud de tratados internacionales en vigor para la República de Cuba.

Respecto a lo antes dicho, el CPE [GOR-O (93), 2022, pp. 2557-2696], establece los siguientes parámetros que son aplicables a los hechos en estudio:

a) Un delito se considera cometido en territorio cubano, si la persona realiza en él actos preparatorios o de ejecución, aunque el resultado se produzca en el extranjero, o viceversa, conforme a lo preceptuado en el Artículo 4.5 (p. 2559). De este precepto, se infiere que el hecho tiene que estar vinculado de algún modo con el territorio nacional, sea antes, durante o después de su producción, lo que excluye aquellos otros eventos delictivos, cometidos extrafronteras nacionales en los que sus efectos tampoco afectan al país.

b) El lugar de comisión del hecho delictivo es aquel en el cual la persona ha actuado o ha omitido la obligación de actuar o en el que se produzcan sus efectos, de acuerdo con el Artículo 16.1 (p. 2562).

c) El momento de ejecución es aquel en el cual la persona ha actuado o ha omitido la obligación de actuar, independientemente del momento en que el resultado se produzca.

Por último, el uso y la aplicación de las TEL-TIC-SER en la sociedad cubana ha exigido la existencia de un marco legal administrativo amplio, que incluye el tema contravencional, de suerte que esto último motiva el lógico temor de que los ilícitos penales puros integrados en esta familia no se distingan adecuadamente de los tipos contravencionales vigentes.

Como actores, y a la vez testigos, del proceso de reforma del sistema jurídico-penal, se afirma que una de las mayores preocupaciones de los decisores políticos y los legisladores del país fue que, en la nueva norma jurídico-penal, se constatará el necesario deslinde entre *delito* y *contravención* en esta materia, a cuyo efecto se tuvieron en cuenta los criterios siguientes:

a) A diferencia de las infracciones contravencionales, que generalmente son cometidas por los administradores, operadores o usuarios de los sistemas, los ilícitos penales básicos y derivados pueden ser ejecutados por cualquier persona, o sea, que el sujeto activo es genérico (quien...),

con independencia de que en el apartado tres del Artículo 296 (p. 2696) se inserte una regla de agravación del marco sancionador, cuando el interviniente en el delito sea un funcionario, empleado u otra persona que tenga a su cargo la custodia, operación, seguridad o mantenimiento del sistema, red, base de datos, programa informático o medios, equipos o tecnologías para la difusión de señales satelitales, televisivas o radiales. Esta regla se justifica por la necesaria conminación a que deben quedar sujetas las citadas personas, como garantes en quienes recaen responsabilidades concretas relacionadas con la integridad y seguridad de las TEL-TIC-SER.

b) Estos tipos penales no están diseñados para formas culposas de comisión, o sea, son intencionales, con formulaciones tanto de dolo genérico como específico, según sea el caso.

c) En sentido general, describen formas activas de ejecución, por lo que se requiere que el sujeto comisor realice algún acto, que haga, pero no que deje de hacer.

Solo el tipo legal del Artículo 290 (p. 2645) contiene una forma omisiva de ejecución del hecho, sustentada en lo previsto en el Artículo 8.4 a) (p. 2559) del propio texto jurídico sustantivo, cuando el sujeto en quien recae el deber jurídico de impedirlo permita que otro no autorizado acceda a un sistema informático, soporte de información, programa de computación, base de datos o cualquier otra aplicación informática, o que lo(la) use, con el propósito de apoderarse, utilizar, conocer, revelar o difundir la información que se almacene, transmita o capture en (o a través de) estos.

El tratamiento que la ley penal sustantiva diseña, para enfrentar las acciones ilegales que lesionan o ponen en riesgo relevantemente los bienes jurídicos protegidos en esta familia, se compendia en tres capítulos:

- El primero, protege la seguridad de las TEL-TIC-SER, y la disponibilidad, integridad y confidencialidad de la información que contienen o procesan (artículos 289-294, pp. 2644-2645).

En cuanto a su contenido regulatorio, se argumenta que la *información* que se protege como bien jurídico se considera en las diferentes formas en que debe ser respetada su confidencialidad, integridad y disponibilidad, así como la de los sistemas informáticos en los que aquella se encuentra almacenada o a los que se transfiere (Acurio del Pino, 1997, p. 21).

Debido a la complejidad técnica de la materia, se recomienda a los operadores del sistema legal penal que se auxilien de las definiciones especializadas que ofrece la norma administrativa, para determinar el contenido del bien jurídico protegido en este capítulo. La Resolución No. 127 de 2007, del ministro de IC [GOR-O (93), 2022, pp. 899-910], en su Artículo 2 (p. 902), establece que la seguridad de las tecnologías de la información es aplicable a la confidencialidad, integridad y disponibilidad de la información tratada por los ordenadores y las redes de datos, y equipara la seguridad de aquellas a la de la información, los ordenadores, los datos y la informática.

Además, en esta norma jurídica se conceptualizan:

a) La *confidencialidad*, como la condición que asegura que la información no pueda estar disponible o ser descubierta por personas, entidades o procesos no autorizados, o para estas(os) (p. 908).

b) La *integridad*, cual la condición que garantiza que la información solo puede ser modificada, incluidos su creación y borrado, por el personal autorizado; o sea, significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga (p. 909).

c) La *disponibilidad*, como la propiedad que garantiza que los usuarios autorizados tengan acceso a la información y los activos asociados cuando se requiera; se significa que el sistema, tanto de *hardware* como de *software*, se mantiene funcionando y está en capacidad de recuperarse rápidamente en caso de fallo (p. 909).

Por otra parte, los tipos penales de los artículos 290, 291 y 292 (p. 2645) del citado capítulo exigen que el sujeto activo cometa el hecho *sin la debida autorización o sin estar debidamente autorizado*, elemento objetivo este que ha sido motivo de críticas, con base en que, supuestamente, nadie puede estar facultado para ejecutar acciones de la naturaleza prevista en dichas figuras delictivas. Quienes así piensan incurren en un evidente error de apreciación, ya que las normas administrativas rectoras de la materia permiten que, en determinados supuestos, los administradores, operadores y usuarios de los sistemas informáticos accedan al contenido digital de estos con los propósitos que se insertan en esos preceptos, por lo que su actuación es lícita; de ello son preclaros ejemplos las definiciones legales y técnicas que aporta la Resolución No. 127 de 2007, [GOR-O (93), 2022, pp. 899-910], sobre la *confidencialidad, integridad y disponibilidad* de la información.

Al precedente argumento se agrega que el CPE [GOR-O (93), 2022, pp. 2557-2696] no es el único que emplea esta redacción, ya que en los artículos 264 y 264-bis de la ley penal sustantiva española (Morales, Fernández y Álvarez, 2018, pp. 902-904) también aparece este elemento objetivo como parte del *delito informático*.

- El segundo capítulo sanciona la difusión ilegal de señales satelitales, televisivas y radiales, servicios de telecomunicaciones u otros similares, a cuyo efecto el Artículo 295 (p. 2646) está diseñado para asegurar que la difusión de estas señales se ejecute conforme al modelo legal que el Estado fija para la actividad, desde el punto de vista del servicio a los intereses de la sociedad (bien jurídico protegido).

Dicho tipo penal se incluye en este título para seguir una sistemática en el objeto de protección de la ley penal, en este caso, la actividad de difusión, individual, colectiva o grupal, o masiva de la información, que se hace mediante las TEL-TIC-SER, la que no puede ser ejecutada por terceros no autorizados, con fines de lucro u otro tipo, incluido el del socavamiento de las bases ideológicas del sistema sociopolítico del país.

En el Artículo 55 de la CRC [GOR-E (5), 2019, p. 81] se regula que los medios fundamentales de comunicación social, en cualquiera de sus manifestaciones y soportes, son de propiedad socialista de todo el pueblo o de las organizaciones políticas, sociales y de masas; y no pueden ser objeto de otro tipo de propiedad, al tiempo que se concede al Estado la facultad exclusiva de establecer los principios de organización y funcionamiento de estos, recientemente regulados en una ley, aún no publicada en el momento en que se escribe este texto.

- El tercer capítulo, conformado por el Artículo 296 [GOR-O (93), 2022, p. 2646], agrupa las disposiciones complementarias, con el objetivo de introducir reglas para resolver el posible conflicto de normas, en consonancia con lo establecido en el Artículo 12 del propio CPE (p. 2561). A ese fin, se prevé que los delitos integrantes de esta familia se sancionan como tales, siempre que no constituyan otro de mayor entidad, y con independencia de los que se cometan para su ejecución o en ocasión de ella.

También, contiene regulaciones destinadas a incrementar los marcos penales hasta el doble de sus límites mínimos y máximos, si el hecho produce un grave perjuicio, o se comete contra sistemas internacio-

nales o de otro país, o se ponen en riesgo el normal funcionamiento y desarrollo de sistemas, sectores y servicios vitales o estratégicos para la defensa y la seguridad nacional o la información oficial clasificada. O sea, que se hace referencia expresa a una tríada de condiciones objetivas de punibilidad que agravan las consecuencias penológicas.

Comparando esta previsión con la ley penal sustantiva española —Código penal de 1995, reformado en 2010 y 2015—, se aprecia que, en su Artículo 264, regula los que la jurisprudencia de ese país denomina *delitos informáticos*, y que forman parte de la familia de los delitos contra el patrimonio y el orden socio-económico, insertados, específicamente, en los tipos penales que sancionan las acciones ilícitas causantes de daños a las TEL-TIC, aunque, de acuerdo con lo previsto en el Artículo 573.2, también pueden ser catalogados como *delitos de terrorismo*, si los hechos se cometen con la finalidad de subvertir el orden constitucional, suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas, o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o abstenerse de hacerlo, o alterar gravemente la paz pública, desestabilizar gravemente el funcionamiento de una organización internacional o provocar un estado de terror en la población o una parte de ella (Morales, Fernández y Álvarez, 2018, p. 902).

En lo atinente a la primera de estas condiciones objetivas de punibilidad, a diferencia de la expresión *grave perjuicio* que utiliza el Artículo 296 del CPE [GOR-O (93), 2022, p. 2646], en el Código penal español concordado se emplean disímiles sintagmas para agravar la sanción, entre ellos, *perjuicio ocasionado*, *perjudicado gravemente* y *daños de especial gravedad*. La jurisprudencia de ese país entiende que el resultado grave de los daños causados en los datos informáticos debe ser analizado casuísticamente, atendiendo a criterios que permitan percibir esa gravedad, como pueden ser: la pérdida definitiva de los datos informáticos o la posibilidad de recuperarlos, y, en este último caso, el costo económico de la reparación, la complejidad técnica de los trabajos de recuperación, la duración de las tareas dirigidas a ella y el valor del perjuicio causado al titular, bien como lucro cesante o como daño emergente (Morales, Fernández y Álvarez, 2018, pp. 903).

El legislador cubano, en cambio, evitó emplear el término *daños*, ya que este se asocia a criterios cuantitativos directamente derivados del contenido regulatorio del Artículo 85 del Código civil (Pérez Gallardo, 2019,

p. 116), cuyo significado es estrecho para los ilícitos de la naturaleza analizada; de ahí que se empleara la expresión *grave perjuicio*, como una condición objetiva de punibilidad que agrava el marco sancionador del correspondiente delito cometido, de acuerdo con el Artículo 296.2 del CPE [GOR-O (93), 2022, p. 2646].

La segunda condición objetiva de punibilidad se asocia al normal funcionamiento de las relaciones internacionales y entre los Estados, ya que cualquier injerencia en estos, mediante agresiones a sus sistemas de TEL-TIC-SER, pueden ocasionar consecuencias graves al país. Esta circunstancia fáctica, en el caso hispano, provoca que el ilícito se convierta en un *delito de terrorismo*, si se desestabiliza gravemente el funcionamiento de una organización internacional, mientras que, en el cubano, aquel se integrará cuando, además de cometerse el hecho contra sistemas internacionales o de otro país, esté presente en el sujeto activo el propósito concreto de intimidar u obligar a un gobierno u organización internacional a realizar un acto o abstenerse de realizarlo, o provocar afectaciones a la paz internacional o la seguridad del Estado.

La última condición objetiva de punibilidad, o sea, la referida a poner en riesgo el normal funcionamiento y desarrollo de sistemas, sectores y servicios vitales o estratégicos para la defensa y la seguridad nacional, está asociada a lo que se conoce como *infraestructura crítica de la información*, que aparece definida en el Artículo 4, inciso m), del proyecto de Convención de la Organización de las Naciones Unidas sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos (2021, p. 7).

V. CONCLUSIONES

El contenido de los artículos 8, 11 y 16, incisos i) y m), de la Constitución y la trascendental importancia de esta materia para la sociedad cubana exigieron que la ley penal sustantiva cubana ofreciera un tratamiento protector a las telecomunicaciones, las tecnologías de la información y la comunicación, y sus servicios.

El proceso de modernización de la ley penal sustantiva, en este ámbito, constituyó una de las políticas más trascendentales de la reforma del sistema jurídico-penal, y uno de sus principales aciertos, en general.

Existen antecedentes de disposiciones normativas, penales y administrativas, que demuestran que el tema, según su estado de desarrollo en cada momento, no fue ajeno a la atención del legislador.

Son varios los instrumentos jurídicos internacionales que incluyen directrices sobre la protección de las telecomunicaciones, las tecnologías de la información y la comunicación, y sus servicios, entre los que son relevantes: el Convenio, la Constitución y el Reglamento de la Unión Internacional de las Telecomunicaciones (2012, s.p.), el Convenio de Budapest y las Declaraciones de los congresos internacionales xiv y xv sobre el tratamiento al delito y la justicia penal.

Como parte del desarrollo del Derecho internacional público en esta materia, en el seno de la ONU hoy se debate un proyecto de Convención internacional sobre la lucha contra la utilización de las TIC con fines delictivos, cuyas propuestas fueron tenidas en cuenta y se incluyeron en el texto del Código penal.

Los distintos elementos normativos que la nueva ley penal sustantiva enfoca en la protección de las telecomunicaciones, las tecnologías de la información y la comunicación, y sus servicios, se sustentan en los antecedentes nacionales y referentes internacionales, además de haberse nutrido con los criterios y las propuestas de especialistas de los ministerios de las Comunicaciones y del Interior, sobre todo, en temas de seguridad informática, ciberseguridad y enfrentamiento al ciberdelito.

La estrategia de protección real y efectiva a las telecomunicaciones, las tecnologías de la información y la comunicación, y sus servicios, en el Código penal, está estructurada sobre la base de los elementos siguientes:

- La inclusión del espectro radioeléctrico, como parte del territorio nacional, en el que pueden ocurrir hechos delictivos sancionables por los tribunales cubanos.
- El diseño de una circunstancia agravante de la responsabilidad penal y de figuras agravadas en 10 tipos penales, debido al empleo de las tecnologías de la información y la comunicación, las redes sociales o los medios de comunicación social.
- La conformación de una familia específica de delitos que protegen la integridad de las telecomunicaciones, las tecnologías de la información y la comunicación, y sus servicios.

Sobre este tema no está dicha la última palabra; existe conciencia de la necesidad de que el campo de protección de las telecomunicaciones, las tecnologías de la información y la comunicación, y sus servicios se mantenga en constante actualización; así lo exigen el desarrollo vertiginoso de estas y su aplicación exponencial en todas las esferas de la sociedad, causante de que, cada día, crezca su empleo en la ejecución de cualquier tipo de actividad delictiva, o a que ellas sean objeto de acciones ilícitas.

Cualquier variante futura en el desarrollo del Derecho penal convencional deberá tomar en cuenta que, en principio, este constituye un arma para ser empleada por el Estado como *ultima ratio*, solo para prevenir y enfrentar aquellas acciones u omisiones que entrañen mayor lesividad en la integridad de las telecomunicaciones, las tecnologías de la información y la comunicación, y sus servicios; mientras que, en los demás casos, se deberá seguir acudiendo al Derecho penal administrativo o contravencional.

VI. REFERENCIAS

Acurio del Pino, S. (1997). *Delitos informáticos. Generalidades*. Pontificia Universidad Católica del Ecuador. http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Antón Oneca, J. (1970). El Código penal de 1870. *Anuario de Derecho Penal y Ciencias Penales*, 2(23), 229-252. https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-P-1970-20022900252

Código de defensa social, de 4 de abril de 1936. (1973). Publicación de legislaciones (vol. 3, ed. de bolsillo). MINJUS.

Comunicación conjunta al Parlamento Europeo y al Consejo. (Agosto 6, 2021). Informe sobre la ejecución de la Estrategia de ciberseguridad de la Unión Europea para la década digital. Oficina de Publicaciones de la Unión Europea. <https://op.europa.eu/es/publication-detail/-/publication/e1315d6e-114f-11ec-b4fe-01aa75ed71a1/language-es>

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. (2015). *Examen de la armonización de la ciberlegislación*

- en América Latina*. https://unctad.org/system/files/official-document/dtlstict2015d4_es.pdf
- Conferencia regional de políticas y estrategias sobre cibercriminos en la Comunidad del Caribe, celebrada en Santo Domingo. (Junio 12-14, 2019). Consejo de Europa. <https://rm.coe.int/3148-1-1-3-dom-rep-outline-regconfstrategiespoliciescyber-12-14jun2019/168094e79c>
- Consejo de Gobierno, Tribunal Supremo Popular. (Marzo 17, 2014). Dictamen No. 441. GOR-O (15), 329-330.
- Constitución de la República de Cuba. (Abril 10, 2019). GOR-E (5), 69-116.
- Convención de la Organización de las Naciones Unidas sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos (proyecto). (2021). Oficina de Naciones Unidas contra la Droga y el Delito. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_S.pdf
- Convención de las Naciones Unidas contra la Corrupción. (2004). Oficina de Naciones Unidas contra la droga y el delito. https://www.unodc.org/pdf/corruption/publications_unodc_convention-s.pdf
- Convención de las Naciones Unidas contra la delincuencia organizada transnacional. (2004). En Instrumentos jurídicos de las Naciones Unidas. <https://www.hchr.org>
- Convenio de Budapest, relativo al enfrentamiento a la cibercriminalidad en el marco europeo. (Noviembre 23, 2001). https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf
- Convenio, Constitución y Reglamento de la Unión Internacional de las Telecomunicaciones, de 22 de diciembre de 1992. (2012). *Derecho internacional, instrumentos administrativos*. <https://www.dipublico.org/10356/convenio-constitucion-y-reglamento-de-la-UIT>
- Declaración de Kioto, sobre la promoción de la prevención del delito, la justicia penal y el estado de Derecho: hacia el cumplimiento de la Agenda 2030 para el desarrollo sostenible. (2021). Oficina de las Naciones Unidas contra la Droga y el Delito. <https://www.unodc.org/documents/commissions/Congress/>

Kyoto Declaration_booklet/21-02818_Kyoto_Declaration_eBook_S.pdf

- Decreto-Ley No. 157, De los servicios de telecomunicaciones de carácter limitado. (Enero 18, 1995). GOR-O (5), 65-68.
- Decreto-Ley No. 370, Sobre la informatización de la sociedad cubana. (Diciembre 17, 2018). GOR-O (45), 763-777.
- Decreto-Ley No. 389, Modificativo del Código penal, de la Ley contra actos de terrorismo y de la Ley de procedimiento penal. (Octubre 8, 2019). GOR-E (27), 155-159.
- Decreto-Ley No. 35, De las telecomunicaciones, las tecnologías de la información y la comunicación y el uso del espectro radioeléctrico. (Abril 13, 2021). GOR-O (92), 2525-2548.
- Decreto-Ley No. 360, Sobre la seguridad de las tecnologías de la información y la comunicación, y la defensa del ciberespacio nacional. (Mayo 21, 2021). GOR-O (92), 786-801.
- Decreto No. 171, De las contravenciones personales de las regulaciones del uso del espectro radioeléctrico. (Abril 30, 1992). GOR-O (5), 49-52.
- Decreto No. 42, Reglamento general de las telecomunicaciones y las tecnologías de la información y la comunicación. (Mayo 24, 2021). GOR-O (92), 2548-2562.
- Decreto No. 43, Reglamento sobre el uso del espectro radioeléctrico. (Mayo 24, 2021). GOR-O (92), 2562-2575.
- Informe del 13.º Congreso de las Naciones Unidas sobre prevención del delito y justicia penal. (2015). Oficina de las Naciones Unidas contra la Droga y el Delito. https://www.unodc.org/documents/congress/Documentation/Report/ACONF222_17s_V1502932.pdf
- Ley No. 21, Código penal. (Febrero 15, 1979). GOR-O (3), 47-268.
- Ley No. 62, Código penal. (Diciembre 30, 1987). GOR-EES (3), 51-97.
- Ley No. 87 de 1999, Modificativa de la Ley No. 62 de 1987. (2008). Université de Fribourg. https://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20080616_25.pdf
- Ley No. 93, Contra actos de terrorismo. (Diciembre 20, 2001). GOR-E (14), 63-70.

- Ley No. 143, Del proceso penal. (Diciembre 7, 2021). GOR-O (140), 4095-4251.
- Ley No. 147, Del proceso penal militar. (Diciembre 21, 2021). GOR-E (12), 575-715.
- Ley No. 149, De protección de datos personales. (Mayo 14, 2022). GOR-O (90), 2463-2479.
- Ley No. 151, Código penal. (Septiembre 22, 2022). GOR-O (93), 2557-2696.
- Ley No. 152, De ejecución penal. (Septiembre 1.º, 2022). GOR-O (94), 2697-2738.
- Morales García, O., Fernández Palma, R. y Álvarez Feijoo, M. (2018). *Código penal con jurisprudencia* (3.ª ed.). Aranzadi.
- Núñez Núñez, E. R. (1954). *Ley de enjuiciamiento criminal* (2.ª ed. corregida, aumentada y puesta al día por D'Estéfano Pisani, M. A., t. 2). Jesús Montero.
- Pérez Gallardo, L. (2019). *Ley No. 59/1987. Código civil de la República de Cuba* (actualizado, anotado y concordado, 5.ª ed.). ONBC.
- Quirós Pérez, R. (2002). *Manual de Derecho penal* (vol. 1). Félix Varela.
- Recomendación de la Conferencia de ministros de Justicia de los países iberoamericanos relativa a la tipificación y sanción de la ciberdelincuencia. (2014). <https://ficp.es/wp-content/uploads/Recomendacion-Ciber-VERSI%C3%93N-A-LA-FIRMA.pdf>
- Recomendaciones de las reuniones de la Red Iberoamericana de Ministerios Públicos especializados en ciberdelincuencia, celebradas en Lisboa. (2018). Asociación Iberoamericana de Ministerios Públicos. <https://www.aiamp.info/index.php/redes-permanentes-aiamp/red-de-ciberdelincuencia/documentos/presentacion-red-ciberdelincuencia-en-asamblea-general-2018>
- Recomendaciones de las reuniones de la Red Iberoamericana de Ministerios Públicos especializados en ciberdelincuencia, celebrada en Santiago de Chile. (2019). Asociación Iberoamericana de Ministerios Públicos. <https://www.aiamp.info/index.php/redes-permanentes-aiamp/red-de-ciberdelincuencia/documentos/conclusiones-ii-reunion-ciberred-castellano>

Resolución No. 98, del ministro de Comunicaciones, sobre el carácter limitado al servicio de telecomunicaciones destinado al turismo, cuerpo diplomático acreditado en el país y a otras personas admitidas al servicio, mediante contratación. (Abril 17, 1995). GOR-O (16), 248-250.

Resolución No. 99, del ministro de Comunicaciones, que declara de carácter limitado las señales de televisión no nacionales. (Abril 17, 1995). GOR-O (16), 250-252.

Resolución No. 127, del ministro de la Informática y las Comunicaciones, Reglamento de seguridad para las tecnologías de la información. (Agosto 30, 2007). GOR-O (57), 899-910.

Resolución No. 128, del ministro de la Informática y las Comunicaciones, Reglamento de la seguridad de las TIC y el ciberespacio nacional. (Junio 24, 2019). GOR-O (45), 831-840.

Resolución No. 74/247, Asamblea General de la ONU, de 27 de diciembre de 2019, Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. (Enero 20, 2020). Organización de Naciones Unidas. <https://documents.un.org/doc/undoc/gen/n19/440/32/pdf/n1944032.pdf?token=xkZlqr1YNmRoTEEqDo&fe=true>

Resolución No. 105, ministro de la Informática y las Comunicaciones, Reglamento sobre el modelo de actuación nacional para la respuesta a incidentes de ciberseguridad. (Agosto 17, 2021). GOR-O (92), 2575-2589.

Resolución No. 107, ministro de la Informática y las Comunicaciones, Reglamento para el uso de los servicios de radiocomunicaciones por satélites. (Agosto 17, 2021). GOR-O (92), 2589-2593.

Resolución No. 108, ministro de la Informática y las Comunicaciones, Reglamento de interconexión, acceso e instalaciones esenciales de redes de telecomunicaciones. (Agosto 17, 2021). GOR-O (92), 2593-2601.

Rovira del Canto, E. (2001). Tratamiento penal sustantivo de la falsificación informática. En López Ortega, J. J. (Dtor.). Internet y Derecho penal. *Cuadernos de Derecho Judicial*, (10), 457-508.