CAPÍTULO X
SEGURIDAD Y EMERGENCIAS

Las telecomunicaciones son esenciales para la seguridad y también en situaciones de emergencia o desastre. Desde comunicaciones entre los ciudadanos de a pie en situaciones de desastres naturales hasta las operaciones de inteligencia para combatir la trata de personas, los servicios de telecomunicaciones pueden marcar la diferencia cuando los segundos son cruciales para la vida y la integridad de las personas.

La terminología empleada en temas de seguridad y emergencia varía de país en país, en algunos la seguridad y las emergencias por desastre son atendidas por las mismas entidades, en otras actúan diferentes autoridades de manera coordinada. Algunos países tienen planes de telecomunicaciones para situaciones de seguridad y emergencia, otros carecen de ellos. En cualquier caso existe consenso en que la seguridad, la prevención y atención de emergencias es una responsabilidad de todos, compartida por el sector público, privado y la ciudadanía y donde las telecomunicaciones desempeñan un rol básico.

La seguridad y las emergencias ponen a prueba la solidez de las instituciones, toda vez que la oportunidad y la pertinencia de la respuesta de las autoridades competentes son cruciales para salvaguardar la integridad y la vida de las personas, así como de sus bienes y preservar la paz en la sociedad. Las telecomunicaciones tienen una labor fundamental en la atención a situaciones de seguridad (pública y nacional) y las emergencias. Los retos para que las telecomunicacio-

nes estén disponibles, sean interoperables y logren comunicar efectivamente y sin demora a las diferentes entidades públicas y privadas que intervienen, son retos compartidos por todos los países en mayor o menor medida.

La atención debida de situaciones que ponen en riesgo la seguridad demandan un liderazgo desde el sector público para el diseño y aplicación de políticas públicas en las cuales las telecomunicaciones sean un instrumento esencial para la prevención, detección, respuesta, mitigación y recuperación en situaciones de seguridad y emergencia. La temática de seguridad, emergencia y telecomunicaciones tiene varias facetas, unas de cara a la sociedad como el número de emergencia y la información a la población, otras que operan tras bambalinas como la designación y protección de infraestructura crítica y los planes de comunicaciones para situaciones de emergencia, y otras más que son eclécticas, como la ciberseguridad.

1. CONCEPTOS GENERALES

Las definiciones de seguridad pública, seguridad nacional y situaciones de emergencia son variadas, por lo cual se proponen a continuación definiciones para fines explicativos. La seguridad pública está encargada de proteger la vida, la integridad y la propiedad de las personas, de preservar la paz, el orden, las libertades y los derechos fundamentales. La seguridad nacional es la encargada de proteger a los estados nacionales frente a amenazas y riesgos de la mayor trascendencia que podrían afectar significativamente a la población o incluso podrían comprometer la estabilidad y/o existencia misma del Estado-nación de que se trate. Las situaciones de emergencia pueden suceder por actos y hechos ya sea del ser humano (p. ej. incendio provocado por negligencia, accidente automovilístico), por la naturaleza (p. ej. el paso de un huracán, el desgajamiento de un cerro, el desbordamiento de ríos), por equipos de tecnologías de la información (p. ej. ataques de virus informáticos) o por fenómenos sanitarios (p. ej. diseminación de un virus como el de la influenza AH1N1, epidemias).

Seguridad pública, seguridad nacional y la prevención y atención a situaciones de emergencia están estrechamente vinculadas al punto que un incidente puede ser una situación de emergencia y de seguridad pública y al mismo tiempo estar comprometiendo la seguridad nacional.

En el Reino Unido el concepto de seguridad nacional ha evolucionado conforme a las circunstancias del mundo contemporáneo para comprender además de la tradicional protección del Estado-nación frente a otros Estados-nación o entes de derecho internacional, muchos otros supuestos. Conforme a la primera Estrategia de Seguridad Nacional (*National Security Strategy*, 2008) el Reino Unido reconoce que el mundo ha cambiado y que con el fin de la Guerra Fría no existe un Estado que le represente una amenaza directa; sin embargo afirma que han surgido una serie de riesgos y amenazas para su población y que están vinculados entre sí, y que además pueden tener factores que los potencian. Estos riesgos, amenazas y factores pueden tener afectaciones que por las magnitudes que pueden alcanzar ahora se contemplan dentro del rubro de seguridad nacional. Los riesgos y amenazas comprenden el terrorismo internacional, el crimen organizado trasnacional, las armas de destrucción masiva, las pandemias, los desastres por condiciones climáticas o por acciones del ser humano, el conflicto e inestabilidad internacional, los Estados fallidos y frágiles. Los factores incluyen la pobreza, la iniquidad, el cambio climático, la globalización, los cambios demográficos, la competencia por energía y la deficiente gestión gubernamental. Por su parte, el Reino Unido identifica desafíos económicos a la seguridad nacional (p. ej. crisis financieras globales), tecnológicos (p. ej. ciberataques) y demográficos (p. ej. migración global).[546]

En México de acuerdo al marco jurídico se distingue entre seguridad nacional, seguridad pública y la prevención y atención de emergencias o desastres (protección civil).

- La seguridad nacional en México conforme a la Ley de Seguridad Nacional es aquella necesaria para la protección de la nación mexicana, su soberanía, independencia, su territorio, su orden constitucional, sus instituciones y la democracia, así como para la defensa del Estado mexicano respecto de otros países o sujetos de derecho internacional.[547] Dicha ley considera como amenazas a la seguridad nacional actos en contra del Estado mexicano de espionaje, sabotaje, terrorismo, rebelión, traición a la patria y ge-

546 Cfr Reino Unido, *The National Security Strategy of the United Kingdom*, presentado por el Primer Ministro al Parlamento, marzo de 2008, interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf (fecha de consulta. 20 de septiembre de 2011), pp. 3-5 y 10-24.

547 Artículo 3 de la Ley de Seguridad Nacional (México)

nocidio, la interferencia extranjera en asuntos nacionales, actos que impidan actuar contra el crimen organizado o que obstaculicen actividades de inteligencia o contrainteligencia, actos de tráfico ilegal de materiales nucleares, armas químicas, biológicas y convencionales de destrucción masiva, financiamiento a acciones y organizaciones terroristas así como actos para destruir o inhabilitar infraestructura estratégica o crítica o aquella indispensable para la provisión de bienes o servicios públicos.[548] Son de destacarse las profundas diferencias conceptuales de seguridad nacional para México y para el Reino Unido.

- Por disposición de ley la seguridad pública en México es la destinada a "salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos y comprende la prevención especial y general de los delitos, la investigación para hacerla efectiva, la sanción de las infracciones administrativas, así como la investigación y la persecución de los delitos y la reinserción social del individuo".[549] Por mandato constitucional en seguridad pública concurren la Federación, las entidades federativas y los municipios.[550]

- Las situaciones de emergencia[551] y desastre[552] en México son atendidas dentro de lo que se denomina protección civil. La finalidad de la protección civil es la protección de la vida y bienes de la población, la planta productiva, los servicios públicos y el medio ambiente. Los desastres pueden ocasionarse por fenómenos antropogénicos (p. ej. producidos por la actividad humana), geológicos (p. ej. sismos, erupciones, deslaves), hidrometeorológicos (p. ej. huracanes, inundaciones, heladas, sequías),

548 Artículo 5 de la Ley de Seguridad Nacional (México).
549 Artículo 2 de la Ley General del Sistema Nacional de Seguridad Pública (México).
550 Artículo 21, párrafo noveno, de la Constitución.
551 "Emergencia: Situación anormal que puede causar un daño a la sociedad y propiciar un riesgo excesivo para la seguridad e integridad de la población en general, generada o asociada con la inminencia, alta probabilidad o presencia de un agente perturbador", artículo 2, fracción XVIII, de la Ley General de Población (México).
552 "Desastre: Al resultado de la ocurrencia de uno o más agentes perturbadores severos y o extremos, concatenados o no, de origen natural o de la actividad humana, que cuando acontecen en un tiempo y en una zona determinada, causan daños y que por su magnitud exceden la capacidad de respuesta de la comunidad afectada", artículo 2, fracción XVI, de la Ley General de Población (México)

químico-tecnológicos (p. ej. fugas tóxicas), sanitario-ecológicos (p. ej. epidemias, plagas, contaminación del agua) y socio-organizativos, generados por errores o acciones humanas.

Para la seguridad y las emergencias son indispensables las telecomunicaciones en diferentes formas y con finalidades distintas, según se expone a continuación.

2. NÚMERO DE EMERGENCIA

El número telefónico para reportar emergencias es el medio para solicitar auxilio de servicios médicos, bomberos o policía cuando la vida o la integridad física están en peligro, cuando exista un riesgo para la salud o para la seguridad individual o pública o para la propiedad o el medio ambiente, entre otros[553]. Las mejores prácticas exigen que en un país se cuente con un solo número de emergencia y que se realicen campañas permanentes de difusión con la finalidad de que la población se familiarice con aquél y en caso de emergencia pueda recordarlo con facilidad. Adicionalmente se requiere que al comunicarse con el número de emergencia, el operador pueda de manera inmediata transferir la llamada a la instancia indicada (p. ej. ambulancia, bomberos, policía, atención psicológica para posibles suicidas) o pueda atender directamente a la persona que está viviendo la emergencia (p. ej. instruir en primeros auxilios en tanto llega la ambulancia).

Al comunicarse con el operador del número de emergencia lo óptimo es que aquél pueda identificar la ubicación de la persona que llama con la finalidad de enviar al personal de emergencia aun cuando quien llamó no haya podido proporcionar la dirección en la que se encuentra. Las funcionalidades y capacidades del número de emergencia y sus servicios deben actualizarse periódicamente para que la población se beneficie de los avances tecnológicos y también para evitar que la tecnología nueva impida o limite la posibilidad de acceder a servicios de emergencia a través del número respectivo.

553 Cfr UE, *Recomendación de la Comisión de las Comunidades Europeas de 25 de julio de 2003 relativa al tratamiento de la información sobre la ubicación de las personas que efectúan llamadas en redes de comunicaciones electrónicas para su uso en servicios de llamadas de urgencia con capacidad de localización*, 2003/558/CE, Recomendación 2, inciso a).

La UE a través de la Directiva Servicio Universal[554] estableció la obligación de todos los Estados miembros de implementar el número 112 para recibir y atender llamadas de emergencia. Este número 112 opera en algunos países como el único para emergencias y en otros países coexiste con el número de emergencia local. La operadora del centro del número 112 responde directamente a la solicitud o transfiere la llamada a la instancia adecuada (p. ej. bomberos, ambulancia). El 112 debe estar disponible gratuitamente para llamadas desde cualquier línea fija y móvil, así como en ciertos casos para comunicaciones por VoIP (*Voice over Internet Protocol*). Asimismo este número debe proveer la localización de la persona que llamó. Los Estados miembros de la UE deben asegurar que las personas con discapacidad accedan a los servicios de emergencia en igualdad de circunstancias que los demás. Dado el tránsito de personas dentro de la UE, los operadores de servicios móviles están obligados a enviar gratuitamente un mensaje de texto SMS para informar sobre la existencia del número de emergencia 112 a toda persona que cuente con servicio móvil y viaje de un país de la UE a otro.[555] Por su parte, el denominado *eCall* es un servicio que permite que automáticamente se realice una llamada de emergencia con información sobre la localización exacta del vehículo, cuando ocurre un accidente o cuando alguna persona que esté viajando en el vehículo la active.[556]

En los EUA el número 911 es el que se utiliza a nivel nacional para reportar emergencias y solicitar auxilio en alguna emergencia. En principio el número 911 recibía la llamada para enrutarla a los servicios que se requirieran, pudiendo tener el número del cual se estaba generando la llamada para que la operadora pudiera devolverla en caso de que la comunicación se interrumpiera. Ahora –en lo que se conoce como E911 o *enhanced* 911– se permite la ubicación geográfica de quien llama. En el caso de los servicios fijos, la ubicación del llamante está disponible de manera generalizada. En cuanto a los servicios móviles, la FCC estableció dos fases con la finalidad de que en la primera el operador de

554 Cfr. UE, Directiva Servicio Universal, artículo 26.

555 UE, *Reglamento (CE) No. 544/2009 del Parlamento Europeo y del Consejo de 18 de junio de 2009 por el que se modifican el Reglamento (CE) No. 717/2007 relativo a la itinerancia en las redes públicas de telefonía móvil en la Comunidad y la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas*, artículo 6.

556 Cfr. UE, *Factsheet 49: eCall - saving lives through in-vehicle communication technology*, ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=2842 (fecha de consulta: 12 de abril de 2013).

la red proveyera tanto el número llamante como la célula o radiobase desde la cual se generaba la llamada y en la segunda, el operador de red suministrara la latitud y la longitud con una variación de 50-300 metros de la ubicación de la persona llamante al 911. Los proveedores de servicios móviles satelitales tienen la obligación de proveer el número llamante y su ubicación.[557]

Los desafíos contemporáneos más importantes para el 911 han provenido de los servicios conocidos como VoIP pues éstos se proporcionan sin importar la ubicación geográfica y con el simple hecho de contar con acceso a internet. El usuario puede tener contratado el servicio VoIP en EUA y contar con un número telefónico de EUA, pero utilizarlo desde cualquier otro país. Por tanto la FCC expidió reglas para que los proveedores de VoIP en EUA (1) tuvieran que dar acceso al número 911 y (2) proveyeran a la operadora del 911 con el número del llamante y la dirección registrada por el usuario. Nótese que esta dirección registrada por el usuario no implica que sea la ubicación desde la cual se está haciendo la llamada al número de emergencia, por lo cual la FCC obligó a los proveedores de VoIP a informar a sus clientes de las limitaciones que tiene usar el número 911 por su teléfono VoIP y obtener la aceptación expresa del cliente de conocer sus límites.[558]

El Plan Nacional de Banda Ancha de EUA (2010) propone que el servicio del 911 se convierta en uno de siguiente generación (*Next Generation 911* o NG911). El NG911 tendría nuevas capacidades, como permitir el envío y retransmisión de texto, fotos, video y correos electrónicos, lo que haría posible proporcionar más información a las instancias de atención a emergencias para una más adecuada y rápida respuesta a la contingencia. Si bien el Plan Nacional de Banda Ancha de EUA señala que se está ya en la transición hacia el NG911, reconoce también que hay diversos retos financieros y regulatorios para lograrlo.[559]

En México la Ley General del Sistema Nacional de Seguridad Pública ordena que exista un número único de atención a la población para emergencias y el servicio de denuncia anónima, obligando además a la Federación, las entidades federativas y las municipales a realizar la compatibilidad de sus servicios de telecomunicaciones con las bases

557 Cfr. FCC, www.fcc.gov/guides/emergency-communications (fecha de consulta 21 de septiembre de 2011).

558 Cfr FCC, www.fcc.gov/guides/emergency-communications (fecha de consulta: 21 de septiembre de 2011)

559 Cfr EUA, *National Broadband Plan* (2010), Capítulo 16, www.broadband.gov/plan/16-public-safety/ (fecha de consulta. 21 de septiembre de 2011).

de datos criminalísticos y de personal del Sistema Nacional de Seguridad Pública.[560] Adicionalmente el Centro Nacional de Prevención del Delito y Participación Ciudadana debe promover un servicio de comunicación para reportar emergencias, faltas y delitos.[561] Por su parte el Acuerdo Nacional por la Seguridad, la Justicia y la Legalidad establece como compromiso asegurar la cobertura de números únicos para la atención a emergencias (066) y para la denuncia ciudadana anónima (089).[562] En 1999 el número 066 fue asignado a nivel nacional al Sistema Nacional de Seguridad Pública por la Cofetel.[563] En las reformas a la LFT de 2012 se establece que la Cofetel determinará "una marcación corta conformada por signos poco habituales para evitar que la señal de auxilio sea producto de error" y que las señales de auxilios se enviarán automáticamente a un sistema nacional de atención de emergencias.[564] No se establece si esa "marcación corta" seguirá siendo el 066 o no. Con la Reforma Constitucional de 2013 será el Iftel el encargado de asignar la numeración telefónica referida para números de emergencia.

La implementación del número 066 y su cobertura en la República Mexicana ha tenido retos constantes que van desde la coordinación entre autoridades federales, estatales y municipales hasta la falta o insuficiente funcionalidad del sistema en algunos sitios para transferir eficientemente las llamadas a los cuerpos de emergencia. A esos desafíos se suma el que existen además del número 066, el 065 de la Cruz Roja, el 074 de Caminos y Puentes Federales y el 078 de la Secretaría de Turismo. Sería importantísimo que se fijara un número de emergencia único y que éste se difundiera a lo largo y ancho del país. En una situación de emergencia, ni una persona con la memoria más privilegiada podrá dilucidar serenamente para saber qué número marcar. Finalmente cabe señalar que los concesionarios de redes públicas de telecomunicaciones tienen dentro de sus títulos de concesión la obligación de proporcionar gratuitamente acceso a los servicios de llamadas de emergencia.[565]

560 Artículo 111 de la Ley General del Sistema Nacional de Seguridad Pública (México).
561 Artículo 130 de la Ley General del Sistema Nacional de Seguridad Pública (México).
562 Compromiso VIII del Acuerdo Nacional por la Seguridad, la Justicia y la Legalidad (México).
563 Asignación de fecha 8 de marzo de 1999.
564 Artículo 44 fracción XIX de la LFT.
565 Cfr. Cofetel, *Bases de la Licitación Pública 20 convocada por la Comisión Federal de Telecomunicaciones*, Anexo 10, Condición 2.4 del modelo de título de concesión para instalar, operar y explotar una red pública de telecomunicaciones.

3. INFRAESTRUCTURA CRÍTICA DE TELECOMUNICACIONES

La infraestructura crítica o estratégica es de tal manera esencial para funciones sociales vitales, la salud, la integridad física, la seguridad, el bienestar social y económico y para un gobierno efectivo, que su perturbación o destrucción afectaría gravemente a un país en lo económico, en la pérdida de la confianza o de vidas.[566] La infraestructura crítica pueden ser bienes, sistemas, redes, procesos, instalaciones, tecnologías y servicios.

Aunque hay consenso en que los sectores energético y de transportes tienen infraestructuras críticas, no existe un catálogo determinado para éstas. De ahí la importancia de que se prevea un mecanismo para incluir nuevas infraestructuras como críticas. La necesidad de proteger las infraestructuras críticas no puede pasar por alto que hay información sensible que podría utilizarse para destruirlas o inutilizarlas. Por tanto se debe reconocer e identificar qué información es sensible con la finalidad de que las personas que tienen acceso a ella por virtud de su trabajo, la resguarden debidamente.[567]

La infraestructura crítica necesita planes para el manejo de riesgos, el restablecimiento y la continuidad de servicios, entre otros. La Asam-

566 Cfr UE, *Directiva 2008/114/CE del Consejo de la Unión Europea de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección*, artículo 2, inciso a); Canadá, Public Safety, www.publicsafety.gc.ca/prg/em/ci/index-eng.aspx (fecha de consulta. 21 de septiembre de 2011), y EUA, Department of Homeland Security, www.dhs.gov/files/programs/gc_1189168948944.shtm (fecha de consulta. 21 de septiembre de 2011)

567 "Artículo 2 Definiciones A efectos de la presente Directiva, se entenderá por: (..) d) información sensible sobre protección de infraestructuras críticas", datos específicos sobre una infraestructura crítica que, de revelarse, podrían utilizarse para planear y actuar con el objetivo de provocar una perturbación o la destrucción de instalaciones de infraestructuras críticas, (. .)" y "Artículo 9 Información sensible sobre protección de ICE [Infraestructura Crítica Europea]. 1 Toda persona que maneje información clasificada en el marco de la aplicación de la presente Directiva en nombre de un Estado miembro o de la Comisión será sometida al oportuno procedimiento de habilitación Los Estados miembros, la Comisión y los órganos de vigilancia competentes garantizarán que la información sensible sobre protección de ICE comunicada a los Estados miembros o a la Comisión no se utilice para fines distintos de la protección de infraestructuras críticas 2 El presente artículo se aplicará asimismo a la información no escrita intercambiada en reuniones en las que se debatan cuestiones sensibles.", UE, *Directiva 2008/114/CE del Consejo de la Unión Europea de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección*

blea General de la Organización de las Naciones Unidas ha señalado que la protección efectiva de la infraestructura crítica de información incluye "determinar las amenazas y reducir la vulnerabilidad a que están expuestas las infraestructuras de información esenciales, reducir al mínimo los daños y el tiempo de recuperación en caso de daño o ataque e identificar la causa del daño o la fuente del ataque".[568]

Por su parte la OCDE ha expedido recomendaciones a nivel nacional e internacional para la protección de infraestructura crítica de información. Es de destacarse que la OCDE indica expresamente que a nivel nacional es necesario que el gobierno demuestre un liderazgo y compromiso para la protección de la infraestructura crítica, lo cual comprende contar con objetivos de política pública, realizar consultas con el sector privado para establecer compromisos en la implementación de éstos, llevar a cabo una revisión sistemática de la política pública, el marco jurídico y la autorregulación, elaborar una estrategia nacional sobre infraestructura crítica de información, trabajar conjuntamente con el sector privado para el manejo de riesgos, compartir información, realizar investigación y desarrollar proyectos sobre seguridad de la infraestructura crítica de información.[569]

Cuando las infraestructuras son propiedad de particulares es muy probable que éstos cuenten con planes de seguridad y protección de dichas infraestructuras que pueden o no ser suficientes si aquellas fuesen consideradas críticas o estratégicas. Por ello los Estados deben asegurarse de que la infraestructura crítica, ya sea propiedad de u operada por el gobierno o por el sector privado, cuente con el plan de seguridad adecuado para emergencias o desastres. En cualquier caso es indispensable la participación coordinada del gobierno, el sector privado y la sociedad.

La UE expidió en 2008 la Directiva sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.[570] Esta Directiva se enfoca en los sectores

568 Organización de las Naciones Unidas, Resolución aprobada por la Asamblea General 58/199. Creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales, 30 de enero de 2004.

569 Cfr. OCDE, *Recommendation of the Council on the Protection of Critical Information Infrastructures*, aprobada por el Consejo de la OCDE en su 1172a sesión el 30 de abril de 2008.

570 UE, *Directiva 2008/114/CE del Consejo de la Unión Europea de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.*

energético y de transportes, destacando que se pueden incluir otros sectores como el de las TIC.571 La revisión de esta Directiva estaba programada para 2012.[572] El Parlamento Europeo expidió una Resolución sobre la protección de infraestructuras críticas de la información en la cual reconoció que la Comisión Europea está estudiando la posibilidad de revisar la Directiva en comento, solicitando el Parlamento que "se examine la posibilidad de ampliar su ámbito de aplicación, en concreto incluyendo al sector de las TIC y los servicios financieros".[573]

En específico en cuanto a infraestructura crítica de TIC o infraestructura crítica de información, la UE ha reconocido que aquéllas "forman una parte vital de la economía y la sociedad europeas, sea porque proporcionan bienes y servicios fundamentales, sea porque constituyen los cimientos de otras infraestructuras críticas. En general se consideran infraestructuras críticas de información (ICI) ya que su alteración o destrucción afectaría gravemente a funciones sociales fundamentales".[574] Adicionalmente la UE estableció un Plan de Infraestructuras Críticas de Información para (1) la preparación y prevención, (2) la detección y respuesta, (3) la mitigación y recuperación, (4) la cooperación internacional y (5) identificar infraestructuras críticas de información con base en ciertos criterios.[575] Este plan es revisado periódicamente para referir los logros alcanzados y fijar las siguientes etapas de acción.[576]

EUA cuenta con un Plan Nacional de Infraestructura[577] y además a través de una Directiva presidencial[578] estableció 17 sectores de in-

571 *Ibidem*, Considerando (5), artículo 3, numeral 3

572 *Ibidem*, artículo 11

573 UE, *Resolución del Parlamento Europeo, de 12 de junio de 2012, sobre la protección de infraestructuras críticas de información – logros y próximas etapas: hacia la ciberseguridad global*, numeral 3

574 UE, *Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la protección de infraestructuras críticas de información «Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia»*, COM(2009) 149 final, 30 de marzo de 2009, 1 Introducción.

575 Cfr *Ibidem*

576 UE, *Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la protección de infraestructuras críticas de información «logros y próximas etapas: hacia la ciberseguridad global»*, COM(2011) 163 final, 31 de marzo de 2011

577 EUA, *National Infrastructure Protection Plan (2009)*, http //www dhs.gov/xlibrary/assets/NIPP_Plan pdf (fecha de consulta: 1 de diciembre de 2012)

578 EUA, Homeland Presidential Directive 7 Critical Infrastructure Identification, Priorization

fraestructura crítica, ordenando la inclusión de nuevos sectores que se fueran identificando como estratégicos como ocurrió con el caso de manufactura crítica en 2008.[579] Los sectores referidos son de agricultura y alimentación, bancario y financiero, químico, de instalaciones comerciales, comunicaciones, manufactura crítica, diques y presas, bases de la industria para la defensa, servicios de emergencia, energético, instalaciones gubernamentales, salud pública y atención a la salud, tecnologías de la información, monumentos e iconos nacionales, reactores, materiales y desechos nucleares, correo y mensajería/transporte de carga, sistema de transporte y agua. Cada sector cuenta con un departamento o agencia federal encargado de elaborar e implementar un plan específico de su sector.

Para el caso del sector de comunicaciones, el National Communications System es el responsable y cuenta con la participación de otras agencias como la FCC y la National Telecomunications and Information Administration. El sector de tecnologías de la información está a cargo del Departamento de Homeland Security. El sector de comunicaciones cuenta con programas como el NS/EP Priority Communications que busca asegurar la prioridad en el acceso a servicios de telecomunicaciones para aquellas personas que trabajan en seguridad nacional o atienden emergencias. Por su parte el sector de las tecnologías de la información tiene el programa de United States Computer Emergency Readiness Team (US-CERT) para proteger la infraestructura de internet contra ataques cibernéticos.[580]

Canadá cuenta con una estrategia nacional y un plan de acción para infraestructura crítica,[581] considerando sectores de infraestructura crítica los activos y sistemas de energía y servicios públicos, de comida, TIC, finanzas, transportes, gobierno, salud, agua, seguridad pública y manufactura.[582] Canadá establece la obligación compartida en temas de infraestructura crítica tanto de los gobiernos de los distintos niveles

and Protection, 17 de diciembre de 2003 (fecha de consulta: 1 de diciembre de 2011).

579 EUA, Department of Homeland and Security, http://www.dhs.gov/files/programs/gc_1189168948944 shtm (fecha de consulta: 1 de diciembre de 2012).

580 Cfr. EUA, *Communications Sector-Specific Plan*, 2010, http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf (fecha de consulta: 26 de septiembre de 2011), y EUA, Information Technology Sector-Specific Plan, 2010, http //www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech-2010.pdf (fecha de consulta· 26 de septiembre de 2011).

581 Canadá, Public Safety, http.//www.publicsafety.gc ca/prg/em/ci/index-eng.aspx (fecha de consulta: 21 de septiembre de 2011)

582 Canadá, *National Strategy for Critical Infrastructure*, http.//www.publicsafety.gc ca/prg/em/ci/_fl/ntnl-eng.pdf (fecha de consulta: 22 de septiembre de 2011).

(federal, provincial, territorial y local), los propietarios y operadores de la infraestructura como de todos los habitantes que deben estar preparados para enfrentar una emergencia en las primeras 72 horas. "La tasa de incidencia y grado de los desastres naturales se incrementa, así como la posibilidad de que interrupciones de la infraestructura crítica puedan prolongar la pérdida de servicios esenciales. Los riesgos y vulnerabilidades se incrementan por el complejo sistema de interdependencias entre la infraestructura crítica, que puede llevar a efectos cascada cruzando fronteras y sectores. Estas implicaciones de interdependencia aumentan por la cada vez mayor dependencia de la sociedad en las tecnologías de la información".[583] Aun cuando el ministerio Public Safety Canada es el responsable de la coordinación general del Plan de Acción de Infraestructura Crítica, Industry Canada, responsable del sector de telecomunicaciones, lo es también para la infraestructura crítica de TIC.[584]

En México se consideran instalaciones estratégicas "a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, así como de aquellas que tiendan a mantener la integridad, estabilidad y permanencia del Estado Mexicano, en términos de la Ley de Seguridad Nacional".[585] Se consideran una amenaza a la seguridad nacional los actos para destruir o inhabilitar la infraestructura estratégica o la indispensable para la provisión de bienes y servicios públicos.[586] El secretario técnico del Consejo de Seguridad Nacional es responsable de realizar el inventario de infraestructura estratégica.[587] La Federación está a cargo de la protección de las instalaciones estratégicas mientras que las entidades federativas y municipales participan como coadyuvantes.[588]

583 "As the rate and severity of natural disasters increases, so does the possibility that disruptions of critical infrastructure could result in prolonged loss of essential services The risks and vulnerabilities are heightened by the complex system of interdependencies among critical infrastructure, which can lead to cascading effects expanding across borders and sectors The implications of these interdependencies are compounded by society's increasing reliance on information technologies", Ibidem, p.4 [traducción de la autora]

584 Canadá, *Action Plan for Critical Infrastructure,* http://www.publicsafety.gc.ca/prg/em/ci/_fl/ct-pln-eng.pdf (fecha de consulta: 22 de septiembre de 2011).

585 Artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública (México)

586 Artículo 5, fracción XII, de la Ley de Seguridad Nacional (México)

587 Artículo 15, fracción XI, de la Ley de Seguridad Nacional (México).

588 Artículos 147 y 148 de la Ley General del Sistema Nacional de Seguridad Pública (México).

4. COMUNICACIONES PARA SITUACIONES DE EMERGENCIA

Las situaciones de emergencia o desastre pueden agravarse por falta de comunicaciones adecuadas por la destrucción, indisponibilidad o saturación de las redes de telecomunicaciones. "Las comunicaciones de emergencia se definen como la capacidad de los equipos de respuesta a emergencias [p. ej. bomberos, policías, primeros auxilios, médicos] de intercambiar información vía datos, voz y video, según estén autorizados, con la finalidad de cumplir con sus misiones. Las agencias para la atención a emergencias en todos los niveles de gobierno deben tener comunicaciones interoperables y perfectas para responder a las emergencias, establecer el comando y control, mantener una situación de alerta, y funcionar bajo un escenario operativo común, para incidentes de gran escala".[589]

Las comunicaciones de emergencia deben tener como características fundamentales:[590]

- La *operatividad* que hace posible que el personal de emergencias pueda tener comunicación para la realización de sus actividades.

- La *interoperabilidad* la cual consiste en que exista comunicación e intercambio de información entre distintas entidades de atención a emergencias, sean públicas o privadas, e independientemente de si son federales, estatales o locales, y que dicha comunicación se dé a los niveles de mando que se requiera. La interoperabilidad implica una comunicación eficiente, confiable y segura. La interoperabilidad puede ser un reto considerando que cada autoridad competente puede tener un sistema distinto de las otras autoridades, la existencia de equipo no compatible, la utilización de frecuencias distin-

589 "Emergency communications is defined as the ability of emergency responders to exchange information via data, voice, and video as authorized, to complete their missions. Emergency response agencies at all levels of government must have interoperable and seamless communications to manage emergency response, establish command and control, maintain situational awareness, and function under a common operating picture, for a broad scale of incidents.", EUA, *National Emergency Communications Plan*, 2008, p. 2 [traducción de la autora]

590 Cfr. EUA, *National Emergency Communications Plan, 2008, p. 2; y Dale Hatfield y Phil Weiser, Toward a Next Generation Strategy: Learning from Katrina and taking advantage of new technologies,* Mobile Satellite Ventures, 2005, pp. 6-11.

tas por parte de las autoridades competentes o bien, por la insuficiencia de recursos.

- La *confiabilidad* para la continuidad de las comunicaciones a pesar de que la infraestructura principal haya sido destruida o dañada. Lo anterior en atención a que las redes de telecomunicaciones generalmente no están preparadas para un desastre mayor (p. ej. ante un corte de energía eléctrica prolongado, las baterías de respaldo resultan insuficientes).

- La *ubicuidad* que significa que el personal de atención a emergencias pueda comunicarse independientemente de su ubicación, ya sea que esté en espacios abiertos o dentro de edificios, en zonas urbanas o alejadas de las ciudades.

- La *flexibilidad* para incorporar –según se requiera– a personal de distintas entidades.

- La *seguridad* con la finalidad de que la información que se transmita esté encriptada para evitar que se intercepte.

- La *complementariedad* entre distintos tipos de redes y tecnología, es decir las comunicaciones de emergencia no pueden basarse exclusivamente en redes fijas ni en redes móviles sino que deberán también incluir redes satelitales. Recuérdese que el desastre ocurrido por el paso del huracán *Katrina* –el más devastador en EUA– destruyó las comunicaciones fijas, móviles y de radiodifusión, haciendo indisponible también el número de emergencia 911.[591] En este caso las comunicaciones que estuvieron disponibles fueron las vía satelite.

Cuando existe una emergencia o un desastre natural o generado por el ser humano, las redes de telecomunicaciones que permanecen operando se saturan fácilmente debido a las comunicaciones tanto de los equipos de emergencia como de las personas que desean entrar en contacto con sus seres queridos para saber cómo se encuentran. Por lo tanto es vital que se cuente con el programa de prioridad en servicios móviles, a través del cual el personal que forma parte de equipos de

591 Cfr EUA, *National Emergency Communications Plan*, 2008, nota al pie de página 4.

emergencia puede acceder al servicio móvil con prioridad respecto de los usuarios comunes. Lo anterior permite que en situaciones de emergencia o desastre dichos equipos puedan comunicarse con prioridad respecto del resto de los usuarios para realizar sus labores de auxilio y apoyo a la población.[592] Adicionalmente se sugiere a la población que en el momento de una emergencia o desastre utilicen mejor el servicio de datos (p. ej. mensajes de texto o SMS) que ocupa menos ancho de banda que las comunicaciones de voz o video, para que no se saturen las redes.

La Convención de Tampere sobre la Provisión de Recursos de Telecomunicaciones para Mitigación de Desastres y Operaciones de Alivio (Convención de Tampere) tiene por objeto el uso de recursos para desastres. Conforme a la Convención de Tampere se podrá: (1) desplegar equipos de telecomunicaciones para predecir, monitorear y proveer información sobre peligros naturales o a la salud, así como respecto a desastres, (2) compartir información de peligros naturales/salud y desastres, (3) difundir información al público e (4) instalar y operar telecomunicaciones para uso de las entidades de ayuda humanitaria.[593]

El Estado parte de la Convención de Tampere que requiera asistencia de telecomunicaciones lo deberá informar al coordinador operativo de la Convención o al Estado del cual esté solicitando dicha ayuda, indicando el alcance y tipo de asistencia requerida.[594] No se podrá prestar asistencia de telecomunicaciones sin el consentimiento del Estado receptor de que se trate.[595] El Estado receptor de la asistencia debe proveer ciertos privilegios, inmunidades y facilidades al equipo que prestará la ayuda de telecomunicaciones (p. ej. exención de ciertos impuestos).[596] Asimismo el Estado receptor está obligado a reducir o eliminar las barreras regulatorias en relación con los equipos y servicios de telecomunicaciones que se prestarán (p. ej. eliminar temporalmente restricciones a la importación de equipos o al uso de frecuencias).[597]

592 Cfr. EUA, *National Communications Systems*, Wireless Priority Service, http://wps.ncs.gov (fecha de consulta 28 de septiembre de 2011) y Canadá, Industry Canada, http://www.ic.gc.ca/eic/site/et-tdu.nsf/eng/h_wj00016.html (fecha de consulta: 28 de septiembre de 2011).
593 Artículo 3, numeral 2, de la Convención de Tampere.
594 Artículo 4 de la Convención de Tampere
595 Artículo 4, numeral 5, de la Convención de Tampere.
596 Artículo 5 de la Convención de Tampere.
597 Artículo 9 de la Convención de Tampere.

A esta fecha México no ha suscrito la Convención de Tampere ni tiene un plan de telecomunicaciones para situaciones de emergencia. Los concesionarios de redes públicas de telecomunicaciones dentro de sus títulos de concesión pueden tener la obligación de contar con un plan de acciones para prevenir la interrupción de los servicios y para proporcionar servicios de emergencia de cuando suceda un caso fortuito o de fuerza mayor.[598]

5. INFORMACIÓN A LA POBLACIÓN

En situaciones de peligro, emergencia o desastre es menester mantener informada a la población sobre lo que está sucediendo, las maneras de prevenir o reducir riesgos, las áreas restringidas, dónde obtener ayuda, entre otros temas. La información debe ser precisa, oportuna y útil y debe estar disponible antes del incidente (cuando es posible, por ejemplo, con el avance de un huracán), durante el incidente y después de éste. La forma en la que se hace llegar el mensaje a la población es de suma importancia y debe considerarse también que la comunicación sea accesible a personas con distintos tipos de discapacidad. Todos los medios de comunicación pueden ser útiles para transmitir información sobre situaciones de peligro, emergencia y desastre; sin embargo no todos los medios pueden estar disponibles en un momento específico de emergencia o desastre.

En EUA el Sistema de Alerta sobre Emergencias (*Emergency Alert System*) obliga a las empresas de radio y televisión abierta y restringida (por cable, satelital, alámbrica e inalámbrica) a transmitir las comunicaciones del Presidente de los EUA durante emergencias nacionales o de las autoridades locales cuando se trate de información de emergencia importante (p. ej. situaciones meteorológicas que representen una amenaza a la población).[599] Asimismo dichas empresas en EUA están obligadas a que la información sobre emergencias sea accesible a personas con discapacidad auditiva y visual. Conforme a ello la información de emergencia en audio debe traer subtitulaje u otros métodos de

598 Cfr Cofetel, *Bases de la licitación 20 convocada por la Comisión Federal de Telecomunicaciones*, Anexo 10, condición 2 4 del modelo de título de concesión para instalar, operar y explotar una red pública de telecomunicaciones

599 Cfr FCC, www.fcc.gov/guides/emergency-alert-system-eas (fecha de consulta: 18 de octubre de 2011)

presentación visual para alertar a personas con discapacidad auditiva de una situación de emergencia, como por ejemplo a través de bandas en las cuales va avanzando texto en la pantalla. En cuanto a la información de emergencia que se transmita por video o por una banda, se deberá proveer un sonido distintivo que advierta a la persona con discapacidad visual que se está transmitiendo información sobre alguna emergencia y que debe utilizar otro medio de comunicación (p. ej. radio, teléfono) para recibir toda la información.[600]

En México los concesionarios y permisionarios de estaciones de radio y televisión abierta o restringida están obligados a transmitir en cadena nacional información que a juicio de la Secretaría de Gobernación sea de trascendencia nacional.[601] En este sentido las transmisiones en cadena nacional significan difundir la misma información al mismo tiempo en todas las estaciones de radiodifusión y dicha información puede ser respecto a situaciones de emergencia. En los títulos de concesión respectivos, los concesionarios y permisionarios de estaciones de radio y de televisión abierta tienen la obligación de protección civil de orientar "sus emisiones, en coordinación con las autoridades competentes, con el propósito de prevenir daños mayores a la población y remediar los ya causados".[602] Por su parte los concesionarios y permisionarios de televisión y audio restringidos (p. ej. televisión por cable) están obligados a transmitir oportuna y gratuitamente los mensajes de las autoridades en cuanto a seguridad o defensa del territorio nacional, la conservación del orden público o medidas para prever o remediar emergencias públicas.[603]

600 Cfr. FCC, www.fcc.gov/guides/emergency-video-programming-accessibility-persons-hearing-and-visual-disabilities (fecha de consulta: 17 de octubre de 2011).

601 Artículos 62 de la LFRTV, 29 del Reglamento del Servicio de Televisión y Audio Restringidos, y 25, fracción XXIII del Reglamento Interior de la Secretaría de Gobernación (México).

602 SCT, *Acuerdo por el que se adopta el estándar tecnológico de televisión digital terrestre y se establece la política para la transición a la televisión digital terrestre en México*, publicado en el *DOF* de 11 de abril de 2006, Condiciones Vigésima Primera del título de refrendo de concesión para continuar usando comercialmente un canal de televisión, y Décima Novena del título de refrendo de permiso de un canal de televisión, de los formatos incluidos en dicho Acuerdo; y Cofetel, *Resolución mediante la cual el Pleno de la Comisión Federal de Telecomunicaciones evalúa y tramita las solicitudes de refrendo presentadas por concesionarios de radiodifusión sonora con anterioridad a la entrada en vigor de las reformas a la Ley Federal de Radio y Televisión*, aprobada por el Pleno de Cofetel mediante acuerdo P/110608/190, de 11 de junio de 2008, Condición Vigésima del título de refrendo de concesión para continuar usando comercialmente una frecuencia de radiodifusión, Anexo IV.

603 Artículo 28 del Reglamento del Servicio de Televisión y Audio Restringidos (México).

La Secretaría de Gobernación es la facultada para conocer los boletines y mensajes a transmitirse por los concesionarios y permisionarios salvo cuando exista urgencia, caso en el que las autoridades podrán directamente ordenar la transmisión. Por su parte la Cámara Nacional de la Industria de la Radio y la Televisión (CIRT) difunde información sobre cómo actuar antes, durante y después de un desastre así como a través de sus afiliados difunde mensajes formativos, medidas y recomendaciones para el autocuidado y autoprotección de la población, alerta a la población en caso de emergencia, informa sobre las condiciones de la emergencia o desastre y de las acciones en apoyo a las comunidades afectadas.[604] Asimismo la Federación Mexicana de Radio Experimentadores fomenta el intercambio de información y material técnico y científico en materia de comunicación durante la emergencia.[605] Es importante recordar la labor tan significativa de comunicación que hicieron los radioaficionados enviando y transmitiendo mensajes en toda la República Mexicana para comunicar la situación de las personas a sus seres queridos tras el severo daño que sufrió la red telefónica de larga distancia por el terremoto de 1985, que la inhabilitó varios meses.

6. CIBERSEGURIDAD Y CERT/CSIRT

Con la creciente dependencia a internet y en un mundo interconectado, la seguridad de las redes de telecomunicaciones y la ciberseguridad se han convertido en un tema vital. Recuérdese que internet está formado por las redes de telecomunicaciones, por lo cual su seguridad conlleva la de las redes. La ciberseguridad incluye la prevención, detección y respuesta a vulnerabilidades y ataques. Los riesgos en el ciberespacio incluyen los virus, gusanos, troyanos y otros códigos maliciosos (*malware*) que pueden eliminar la información de las computadoras, acceder sin autorización a éstas y a sus archivos, alterar documentos, atacar a otros sistemas y computadoras, robar la identidad, información de tarjetas de crédito, entre otros muchos riesgos y afectaciones.

La ciberseguridad es responsabilidad de todos los usuarios de internet. Los CERT (*Computer Emergency Response Team*) o CSIRT (*Computer Security Incident Response Team*, que es el término más moderno) son

604 Cfr Acuerdo por el que se emite el Manual de Organización y Operación del Sistema Nacional de Protección Civil, publicado en el DOF de 26 de octubre de 2006 (México).
605 Cfr. *Ibidem.*

equipos de expertos en seguridad de las tecnologías de la información que buscan proteger de manera efectiva y eficiente a los equipos e infraestructuras de información frente a las amenazas, vulnerabilidades y ataques en internet.[606] Los CERT pueden ser públicos o privados. Proporcionan información educativa, alertas sobre incidentes, riesgos y maneras de mitigar éstos y pueden realizar investigación en ciberseguridad. En México los CERT existentes a la fecha de publicación de esta obra son el de la UNAM (UNAM-CERT),[607] el CERT-MX a cargo del gobierno federal y el que el sistema financiero tiene en construcción.

7. GEOLOCALIZACIÓN, BLOQUEADORES Y APOYO A LA JUSTICIA

La situación de seguridad en la República Mexicana desde principios del siglo XXI se ha deteriorado significativa y crecientemente. Pretendiendo buscar formas de combatir la comisión de diversos delitos, el Congreso de la Unión llevó a cabo reformas en 2009, 2010 y 2012 a la LFT, estableciendo ciertas obligaciones a los concesionarios de redes públicas de telecomunicaciones y concesionarios autorizados para el uso de frecuencias del espectro radioeléctrico para usos determinados, así como a las comercializadoras de servicios de telecomunicaciones.[608] La finalidad de estas reformas fue contribuir con la lucha contra diversos delitos, a saber, en cuanto a la reforma de 2009 y 2012 respecto a los delitos de extorsión, amenazas, secuestro, contra la salud, otros delitos graves o los relacionados con delincuencia organizada; la reforma de 2010 sólo es relativa al secuestro. Sin embargo el problema mayor en México es la impunidad y la corrupción, por lo que ninguna cantidad de reformas legislativas puede remediar la ausencia del estado de derecho.

Renaut. En 2009 el Congreso de la Unión estimó que el medio para contribuir a reducir los delitos de extorsión, amenazas, secuestro, otros delitos graves o los relacionados con la delincuencia organizada era

606 Cfr. European Network and Information Security Agency, *Baseline capabilities National / governmental CERTs – v1.0*, diciembre de 2009, p. 8, US-CERT, www.us-cert.gov., y UNAM-CERT, www.cert.org.mx.

607 UNAM-CERT, www.cert.org.mx.

608 Las reformas fueron publicadas en el *DOF* el 9 de febrero de 2009, el 30 de noviembre de 2010 y el 17 de abril de 2012.

crear el Registro Nacional de Usuarios de Telefonía Móvil (Renaut). Estas reformas establecieron obligaciones para concesionarios y, en ciertos casos, a comercializadoras de servicios de telecomunicaciones. Sin embargo, después de casi tres años en que se demostró que esa medida era ineficaz para lo que se pretendía, se derogó el Renaut en 2012.

Bloqueadores. En 2010 el Congreso de la Unión expidió la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro, Reglamentaria de la fracción XXI del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos y reformó nuevamente la LFT en cuanto a las obligaciones de los concesionarios. Mediante esta reforma se adicionó la obligación de los concesionarios de redes públicas de telecomunicaciones de colaborar para que en el ámbito técnico operativo "se restrinja de manera permanente todo tipo de comunicación, ya sea transmisión de voz, datos o imagen en los Centros de Readaptación Social Federales y de las Entidades Federativas".[609] El bloqueo de señales está orientado a comunicaciones sobre cualquier banda de frecuencia y limitada al perímetro de los centros de readaptación social.[610] Asimismo el Consejo Nacional de Seguridad Pública tiene facultades para establecer los casos, condiciones y requisitos para el bloqueo de señales de telefonía celular en instalaciones estratégicas y los centros de readaptación social.[611]

En 2012 se reformó nuevamente lo relativo a bloqueadores de señales de telecomunicaciones en centros penitenciarios proveyendo mayor detalle y señalando que (1) una autoridad distinta a la penitenciaria será la encargada de operar los bloqueadores y lo hará fuera de los centros penitenciarios, (2) si se interrumpe el funcionamiento de los bloqueadores se lanzará una señal de alarma y (3) habrá colaboración entre esta autoridad distinta (la reforma no dice cuál autoridad), los concesionarios de telecomunicaciones y el Sistema Nacional de Seguridad Pública.[612] Esta reforma mejora lo relativo a la operación de bloqueadores, sin embargo faltó incluir la participación de la sociedad civil en el monitoreo de la operación de estos inhibidores de señales. En cualquier caso si las normas prohíben la entrada de teléfonos y equi-

609 Artículo 44, fracción XVI, de la LFT
610 Artículo 44, fracción XVI, párrafo segundo, de la LFT
611 Artículo 149 de la Ley General del Sistema Nacional de Seguridad Pública (México)
612 Artículos 44 de la LFT y 14 ter de la Ley que Establece las Normas Mínimas sobre Readaptación Social de Sentenciados

pos de comunicación, así como se instalan bloqueadores, pero no se combate a la corrupción ni se implementan medidas de supervisión ciudadana, entonces ninguna cantidad de equipos ni leyes serán suficientes para realizar el Estado de Derecho y evitar que se realicen comunicaciones desde y hacia los penales.

Geolocalización. La obligación para ubicar geográficamente un equipo móvil existe en ley desde 2010. Sin embargo en 2012 se incorporó una nueva sección a la LFT respecto a las obligaciones de los concesionarios y permisionarios de telecomunicaciones para que éstos colaboren con la Procuraduría General de la República y con las procuradurías estatales para ubicar geográficamente y en tiempo real los equipos de comunicación móvil vinculados con investigaciones de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas.[613]

Intervención de comunicaciones. La Constitución establece que las comunicaciones privadas son inviolables y sanciona penalmente los actos contra la libertad y privacidad de éstas, salvo que alguno de los particulares que participe en la comunicación privada de que se trate la aporte voluntariamente. Por comunicaciones privadas debe entenderse de manera amplia a todas las comunicaciones electrónicas de voz, video, mensajes de texto y multimedia y mensajes de correo electrónico. La Ley Federal contra la Delincuencia Organizada es más específica al referir a las comunicaciones privadas como aquellas "que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores".[614] Por su parte la LFT establece que será confidencial la información que se transmita a través de redes y servicios de telecomunicaciones, salvo que sea información pública o exista orden de autoridad competente.[615] La Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro obliga a los concesionarios de servicios de telecomunicaciones a prestar auxilio a las autoridades para la intervención de comunicaciones privadas cuando medie orden judicial que así lo determine.[616]

613 Artículos 3 fracción XVII, 40 bis y 44 fracción XVII de la LFT.
614 Artículo 16, párrafo tercero de la Ley Federal contra la Delincuencia Organizada (México).
615 Artículo 49 de la LFT.
616 Artículo 24 de la Ley General para Prevenir y Sancionar los Delitos en Materia de

Las comunicaciones privadas podrán intervenirse previa autorización de los jueces federales competentes, sin que puedan intervenirse comunicaciones para asuntos electorales, fiscales, mercantiles, civiles, laborales, administrativos o cuando se trate de comunicaciones de una persona detenida y su defensor.[617] Cuando una autoridad competente solicite la intervención de comunicaciones privadas al juez federal, deberá expresar el tipo de intervención, las personas cuyas comunicaciones serán intervenidas y la duración de la intervención.[618] En el caso de intervenciones relacionadas con delincuencia organizada, el escrito de solicitud de la autoridad al juez deberá incluir el objeto y la necesidad de la intervención, el procedimiento y los equipos de intervención y en su caso, la identificación de la persona que presta el servicio de comunicación a ser intervenido.[619] Asimismo para el caso de delincuencia organizada, el juez federal podrá otorgar autorización para la intervención de comunicaciones cuando la intervención sea el medio idóneo para obtener pruebas, debiendo en su caso ordenar a las instituciones públicas o privadas (p. ej. concesionarios de telecomunicaciones) modos específicos de colaboración.[620]

La Ley Federal contra la Delincuencia Organizada obliga a los concesionarios, permisionarios y titulares de medios o sistemas que puedan ser sujetos a intervención, a colaborar con las autoridades competentes.[621] La autorización de intervención de comunicaciones en casos de delincuencia organizada podrá ser de hasta seis meses, incluyendo prórrogas, a menos que se acrediten nuevos elementos que justifiquen un tiempo mayor. Las intervenciones hechas sin autorización o fuera de los términos y de ésta, carecerán de valor probatorio.[622]

En México los desafíos en seguridad y atención a emergencias son inmensos por la lacerante corrupción que aqueja al país y la impunidad que la agrava. Finalmente la tecnología y las telecomunicaciones son medios que pueden emplearse positivamente para el desarrollo armónico de la sociedad o utilizarse para el crimen y para una actitud complaciente ante éste. Ninguna cantidad de Renauts o de bloqueado-

---

Secuestro, Reglamentaria de la fracción XXI del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos (México).

617 Artículo 16, párrafo décimo tercero de la Constitución.
618 Artículo 16 de la Constitución
619 Artículo 16 de la Ley Federal contra la Delincuencia Organizada (México)
620 Artículo 16 de la Ley Federal contra la Delincuencia Organizada (México)
621 Artículo 26 de la Ley Federal contra la Delincuencia Organizada (México)
622 Artículo 18 de la Ley Federal contra la Delincuencia Organizada (México)

res en las cárceles remediará la ausencia del Estado de Derecho. Si en las cárceles está prohibida la introducción de equipos celulares o de telecomunicaciones, ¿por qué ingresan? Si el Congreso de la Unión legisla para incorporar equipos bloqueadores de señales de telecomunicaciones dentro de los centros de readaptación social, ¿qué garantiza que la misma corrupción que permitió la entrada de equipos celulares o de telecomunicaciones, esta vez impida apagar los bloqueadores en tanto se realizan llamadas y se generan comunicaciones desde las cárceles? Las telecomunicaciones deben ser pues un facilitador de la prevención y atención a situaciones de seguridad y emergencia, sin olvidar que para ello se requiere de planeación nacional, estratégica e incluyente encabezada por el gobierno mexicano en la cual la ciudadanía participe y se comprometa. ◗