



EL PAPEL DE LA MUNICIPALIDAD EN EL CIBERESPACIO

Lic. Michael DURÁN ARRIETA.¹

Palabras claves: ciberespacio, tecnologías de la información y la comunicación, ciberterritorialidad, gobierno local y ciberseguridad.

Key Words: Cyberspace, Information and communications technology, Ciberterritoriality, Local Government and Cybersecurity.

Presentación. El concepto de territorialidad y de lo local es esencial para la teoría clásica del Derecho municipal. Ante el fenómeno llamado sociedad de la información, misma que está caracterizada por nuevas formas de relación e interacción social, gestión y transferencia de datos, producción de bienes y servicios digitales, los cuales son producto de la interconectividad y de procesos digitales que suceden en el ciberespacio, resulta indispensable que los entes gubernamentales entiendan las concepciones de ciberterritorialidad y ciberseguridad como elementos necesarios para entender su papel y perfilar la forma de desarrollar su actividad como administración pública en esta

nueva realidad, así como utilizar el arte de la guerra para la protección de su ciberterritorio.

Abstract: The concept of territoriality and locality is essential for the classic theory of Municipal Law. Given the phenomenon called Information Society, which is characterized by new forms of relationship and social interaction, management and transfer of data and production of digital goods and services, which are the product of interconnectivity and digital processes that occur in Cyberspace, it is essential for governmental entities to understand the concepts of ciberterritoriality and cybersecurity as elements of cybersecurity. Therefore, it is essential that governmental entities understand the concepts of ciberterritoriality and cybersecurity as necessary elements to understand their role and outline the way to develop their activity as Public Administration in this new reality, as well as to use the art of war for the protection of their cyberterritory.

¹ Socio en BSA CONSULTORES SRL, licenciado en Derecho con énfasis en Tecnología, Comercio Electrónico y Telecomunicaciones, con estudios formales en Auditoría de Tecnologías de la Información y Comunicación en la Escuela de Administración de Negocios de la Universidad de Costa Rica, Analista de Ciberseguridad certificado por Elev8, egresado de la Maestría en Derecho Público del Sistema de Estudios de Posgrado de la Universidad de Costa Rica, asesor en materia de derecho administrativo en diversas instituciones públicas y gobiernos locales del país.

PRELUDIO: EL CIBERESPACIO, LOS GOBIERNOS LOCALES, LA CIBERTERRITORIALIDAD Y LA CIBERSEGURIDAD

Lo primero que resulta conceptualmente útil para empezar a problematizar sobre el tema propuesto es perfilar un concepto operativo para el Derecho del término ciberespacio. Partiendo desde un punto de vista etimológico con motivo de ilustrar la raíz del concepto, se encuentra que el prefijo "ciber" proviene de la palabra *cibernética* que, a su vez, proviene del griego, tal como explica Valencia Giraldo (2016, p.9): “*La palabra cibernética viene del griego Κυβερνήτης (kybernētēs, el timonel que «gobierna» la embarcación) o sea que se refiere a mecanismos precisos de gobierno y control y en ese sentido fue usada por Platón. En el mismo sentido político-social fue utilizada en 1834 por el físico André-Marie Ampère (1775-1836) para referirse a las ciencias de gobierno en su sistema de clasificación de los conocimientos humanos*”.

Según lo anterior, es posible definirla como el arte de gobernar una embarcación (Breton, 2000) y dentro de esta lógica se debe entender a “la embarcación” como un sistema, siendo este como un conjunto de elementos interrelacionados para lograr un objetivo. En este sentido, el internet sería la vía en la cual navega la embarcación, entendida como una red de transporte interconectada y de acceso público, donde la infraestructura de la información es interoperable y globalmente accesible por medio de la conectividad a esta red.

Así se puede ver cómo el prefijo ciber evoca de primera entrada a los conceptos de sistemas, control, gobierno, navegación y, especialmente, al de la comunicación en seres vivos y máquinas; por lo cual, al anteponerlo al término espacio, se encuentra como idea principal el desvincular al concepto de espacio de su contexto más común sea el físico, que se refiere a la extensión tridimensional que contiene todos los objetos

y en el que ocurren los fenómenos físicos, el cual tiene tres dimensiones: largo, ancho y alto; realidad que no existe en ese ciberespacio con esas características particulares.

Es así como, al hacer referencia al ciberespacio, se habla del espacio virtual o digital en el que se lleva a cabo la comunicación, la interacción y el intercambio de información a través de redes de computadoras y sistemas de información. En esencia, el ciberespacio es, entonces, un espacio de datos interconectado que existe especialmente en la infraestructura de internet, que rompe las barreras del espacio y del tiempo físico, donde se almacena, procesa y comunica información; un terreno poco explorado y que escapa a un control central de los Gobiernos.

Este escapa a un control central de los Gobiernos, por cuanto en esencia el ciberespacio como concepto es etéreo e intangible, y no resultan operativos en esa realidad conceptos clásicos del Derecho como el de soberanía, territorialidad, localidad y temporalidad strictu sensu. López de Anda (2011, p. 80) explica que estas discusiones: “*no se agota con la creación de organismos internacionales de regulación, demanda el diálogo abierto, plural y sistemático entre diversas instancias*”.

Antes de alarmarse por esa conclusión adelantada, es necesario ver que la disciplina jurídica no es ajena a este tipo de nociones etéreas y abstractas que logran ser operativas, tales como los conceptos de justicia y el propio concepto de interés público; dado que el derecho como fenómeno también puede ser entendido como una disciplina intangible al menos en su base axiológica y normativa. Nótese que el concepto central de ordenamiento jurídico tampoco puede ser encontrado en el espacio físico, dado que ese universo axiológico de valores, principios y normas es inmaterial y está en un entorno humanamente construido, con sus

respectivas reglas de funcionamiento interno y sus limitaciones en la aplicación de la realidad física, por lo cual conceptualmente no resulta imposible operativizar para ser utilizados en el derecho, conceptos como el de ciberespacio.

Una vez sentadas estas bases, se encuentra la pertinencia de preguntarse: ¿cuál es el papel que debe desarrollar un gobierno local en el ciberespacio?, dado que, en un análisis clásico, se encuentra que estas ejercen sus potestades de imperio y prestan servicios públicos en la limitación de un espacio físico, normalmente ligado a un territorio geográficamente determinado. Esto es parte de la propia esencia del concepto de gobierno local.

El cuestionamiento, entonces, resulta de gran relevancia en el contexto del ejercicio de los municipios como sujetos de Derecho público, en el cual el concepto de territorialidad se erige como un principio que establece los límites dentro de los cuales una autoridad administrativa tiene jurisdicción y competencia para ejercer sus funciones y tomar decisiones.

Esto significa que una entidad administrativa, ya sea a nivel local, regional o nacional, tiene la autoridad y la responsabilidad de administrar y regular asuntos específicos dentro de su territorio designado. Así se han construido conceptos clásicos del derecho como el de soberanía y el de autonomía municipal, cuya concepción resulta entrar en crisis ante esta nueva realidad del ciberespacio, por ejemplo, Peña (2007) afirma: “En el ciberespacio no existen tratados de soberanía y principios de territorialidad, el acceso se desliga de viejos parámetros de nacionalidad” (p. 18).

En este punto, se debe hacer énfasis en el concepto de territorialidad. Velasco Rico (2009) explica la función del territorio como límite del poder de las organizaciones jurídico-públicas de

base territorial, siendo que este ha sido utilizado clásicamente en el Derecho público para definir la extensión de las competencias y responsabilidades de una entidad administrativa y, a su vez, establecer limitaciones al ejercicio del poder para la toma de decisiones y la ejecución de políticas públicas en una determinada área geográfica. Siendo esta la clave en la que el concepto debe ser reevaluado, para comprender el papel que juegan los entes públicos en esta nueva realidad. Así las cosas, para hablar de la municipalidad, en el contexto del ciberespacio, debe reevaluarse el concepto de territorialidad, separando de alguna manera la jurisdicción territorial, del ejercicio de las competencias para el cumplimiento de los fines locales.

Para ejemplificar esta redefinición, resulta útil enfocar la mirada, para ver la legislación a la luz de los avances tecnológicos. Así, es posible empezar por reevaluar el numeral 3 del Código Municipal (1998), mismo que indica:

*“Artículo 3. - La **jurisdicción territorial de la municipalidad es el cantón respectivo**, cuya cabecera es la sede del gobierno municipal. El gobierno y la **administración de los intereses y servicios cantonales estarán a cargo del gobierno municipal**. La municipalidad **podrá ejercer las competencias municipales e invertir fondos públicos con otras municipalidades e instituciones de la Administración Pública para el cumplimiento de fines locales, regionales o nacionales**, o para la construcción de obras públicas de beneficio común, de conformidad con los convenios que al efecto suscriba”.* (El destacado es propio)

En este caso, si se entiende que la jurisdicción de la municipalidad es el cantón respectivo, es incontrovertible que esta se refiere a un espacio físico bajo el concepto clásico de territorialidad antes citado; cuestión que no permite por medio

de interpretación ser extendida o variada.

No obstante, lo que sí puede y en el contexto actual debe ser entendido de forma amplia y comprensiva es el elemento teleológico en la forma de actividad y el ejercicio de las competencias de los gobiernos locales; adaptando entonces el concepto jurídico indeterminado de interés público local o de fines públicos locales, como algo que traspasa y trastoca el concepto de territorialidad, para dejar de estar dirigido solo a un espacio físico geográfico.

Esto es posible, en el tanto el tema del cumplimiento de fines, la protección de los intereses y la prestación de servicios cantonales o locales no están ligados específica y necesariamente al entorno o espacio físico donde se ejerce la jurisdicción, por cuanto cada día más estos intereses y fines están inmersos o relacionados con el ciberespacio, convirtiéndose en una realidad de la cual la municipalidad y sus administrados no pueden escapar. Interpretación que se liga de manera indefectible a lo establecido en el numeral 4 de la Ley General de la Administración Pública (1978) en el tanto indica:

*“Artículo 4º.-La actividad de los entes públicos deberá estar sujeta en su conjunto a los principios fundamentales del servicio público, para asegurar su **continuidad, su eficiencia, su adaptación a todo cambio** en el régimen legal o en **la necesidad social que satisfacen** y la igualdad en el trato de los destinatarios, usuarios o beneficiarios”.* (El destacado es propio)

Esto es así porque, a medida que la tecnología y la digitalización se han vuelto cada vez más prominentes en la sociedad, resulta indispensable la adaptación paulatina de la actividad municipal en esta nueva interacción, para proporcionar servicios a través del entorno digital y proteger el interés público local; sin olvidar la distinción

primaria de la actividad administrativa en actividades de fomento, control o policía y prestacional; más su adaptación complementaria que refuerza su capacidad explicativa, ordenadora y dogmática que incluye la actividad de garante y regulatoria, en las cuales se puede perfilar con alguna facilidad toda la actividad administrativa de una municipalidad en el ciberespacio.

Dentro de estas acciones públicas, se encuentran múltiples ejemplos, tales como la digitalización de trámites y gestiones en línea, la videovigilancia, la creación de plataformas de participación ciudadana con incidencia directa en la toma de decisiones, la instauración del gobierno abierto, plataformas electrónicas para la recepción de mensajes, denuncia o reporte de problemas de índole pública, plataformas para la coordinación interadministrativa de atención centralizada de solicitudes administrativas, entre muchas otras actividades administrativas de carácter público que pueden ser realizadas en línea; las cuales resultan verse reflejadas como un impacto sistemático e inevitable de la disrupción digital, tal como lo explica la Comisión Económica para América Latina y el Caribe (2021, pp. 11-13).

No obstante, es necesario destacar que, para actuar en el ciberespacio, las municipalidades deben considerar como vitales aspectos de seguridad y privacidad de la información, protección de la infraestructura tecnológica, la planificación y diseño especializado y cuidadoso de los servicios tecnológicos basados en experiencia y evidencia. Dado que no se trata solamente de trasladar sus procesos al entorno digital, sino que esta transformación debe suponer una ventaja o valor al momento de su virtualización, por cuanto no son pocos los problemas que se presentan cuando no existe una visión, planificación y gestión correcta del cambio.

Además de lo anterior, desde la perspectiva de los ciudadanos a los que se le prestan los

servicios en línea, el ente local debe asegurar que los servicios en línea sean accesibles, tal como lo referencia la Comisión Económica para América Latina y el Caribe (2021, p.47). Estos deben ser utilizables por una amplia gama de usuarios, incluyendo aquellos con diferentes niveles de habilidades digitales, pero sin perder el control de su infraestructura tecnológica y el gobierno de los datos que debe proteger en el ciberespacio, por lo cual resulta necesaria la introducción del concepto de ciberterritorialidad.

Por lo anterior, la ciberseguridad resulta central para desarrollarse en el ciberespacio, entendida aquella como una disciplina que pone énfasis en la protección de los derechos de las personas en las interacciones, transacciones y comunicaciones que se despliegan a través de redes de comunicación y sistemas de información. Es decir, en el entorno digital donde se almacena, procesa y comunica información, sea el ciberespacio, y específicamente en su ciberterritorio, en protección de la infraestructura crítica, donde las amenazas pueden atentar contra el suministro de servicios públicos, tal como lo indica la Comisión Económica para América Latina y el Caribe (2021, p.83).

Es así como, aplicado al Derecho administrativo, se puede ensayar el concepto de ciberterritorialidad como un término que hace converger las nociones de ciberespacio y territorialidad, y se refiere a la extensión de la autoridad y la influencia de un ente de gobierno a través de su actividad en internet. Implica la capacidad de regular y gobernar las actividades que ocurren en línea con su participación y normalmente en su infraestructura tecnológica, abarcando la prestación de servicios digitales.

Este concepto de ciberterritorialidad, desarrollado por Ruiz, M. (2018) con motivo de su aplicación en el Derecho procesal penal, se ensaya para hacerlo operativo en el Derecho

público y, específicamente, en el Derecho municipal, reconoce que, en la era digital actual, la soberanía estatal y la autonomía municipal en la administración de asuntos locales se expanden más allá del espacio físico, abriendo nuevas posibilidades y desafíos en la relación entre entidades públicas y ciudadanos que sucede en el entorno digital, específicamente, a través de internet.

Es así como la ciberterritorialidad emerge como un concepto crucial para entender la interacción entre los gobiernos locales y los administrados en el espacio virtual, entendiendo la extensión de la competencia local de la municipalidad al ciberespacio, destacando tanto las oportunidades como los retos y provocaciones que surgen al expandir su presencia y servicios hacia el ciberespacio.

De lo dicho, es necesario destacar que, a pesar de la expansión hacia el ciberespacio, es esencial recordar que la territorialidad física sigue siendo fundamental. La ciberterritorialidad no reemplaza la importancia de la administración efectiva de espacios físicos locales ni compite con ella, sino que complementa y enriquece la interacción entre el gobierno y la comunidad en nuevos ámbitos de una realidad atemporal y deslocalizada geográficamente.

Por lo tanto, la ciberterritorialidad representa una evolución en la forma en que los gobiernos locales interactúan con sus ciudadanos y administran sus territorios. Al abrazar la expansión hacia el ciberespacio, los gobiernos locales tienen la oportunidad de ofrecer servicios más eficientes y accesibles, promover la participación ciudadana y mejorar la transparencia. Sin embargo, este avance no está exento de desafíos, particularmente en términos de seguridad y privacidad. En última instancia, una estrategia equilibrada que integre lo digital y lo físico permitirá a los gobiernos locales prosperar en la era de la ciberterritorialidad, para

promover el bienestar y la calidad de vida de la comunidad que sirven, es decir, protegiendo el interés público local.

De esta forma, la municipalidad se convierte en una entidad clave para la gestión de su ciberterritorio y por derivación lógica necesaria, de la implementación de ciberseguridad a nivel local, como primer nivel de defensa contra amenazas cibernéticas que puedan afectar a la comunidad que sirve.

LA NECESIDAD DE INTEGRACIÓN DE LAS CAPAS 8, 9 Y 10 EN EL MODELO OPEN SYSTEMS INTERCONNECTION (OSI) PARA ENTENDER EL PAPEL DE LOS GOBIERNOS LOCALES EN EL CIBERESPACIO

Una vez puestas en crisis las concepciones jurídicas, resulta necesario también poner de manifiesto la crisis en las concepciones técnicas, para poder entender la actividad de las administraciones públicas y el papel regulador del derecho en el internet.

El Modelo de Sistemas de Interconexión Abiertos (por sus siglas en inglés OSI) es una guía o modelo conceptual que describe y desagrega de manera analítica los componentes de la comunicación de datos a través de redes. Asimismo, describe cómo se hace posible la transmisión entre remitentes y destinatarios en este modelo de comunicación, lo que pone de manifiesto un punto de vista del funcionamiento técnico de esta comunicación a través de una división de siete capas.

Cada capa tiene una función específica, se comunica y funciona al interactuar de manera directa con las capas que tiene “encima” y “debajo”. Claramente, el modelo OSI es meramente conceptual en una abstracción técnica, que muestra cómo se posibilitan las comunicaciones en una red, desde sus componentes físicos y virtuales. Por lo cual, se realiza un repaso muy somero de este modelo para proceder a explicar la propuesta del profesor Peter Swire (2018), en torno a la inclusión conceptual de tres capas denominada “capas sociales” al modelo, como propuesta para enseñar los aspectos organizativos, jurídicos y diplomáticos de la ciberseguridad.

Tabla 1: Capas técnicas del modelo OSI

Número de capa	Función en el modelo
Capa 1: La capa física	Esta es la que actúa directamente en la operación de los equipos físicos y la que facilita la transferencia de datos, tales como cableado, conmutadores, enrutadores y puntos de acceso, que realizan su comunicación por medio de estándares, los que hacen posible la comunicación entre dispositivos de diversos fabricantes.
Capa 2: La capa de enlace de datos	La capa de enlace de datos es la responsable de ordenar la transferencia de información en la misma red, donde el enlace de datos convierte los paquetes recibidos en la capa de red en marcos,

	siendo la responsable del control de los errores y el flujo de datos para garantizar una correcta transmisión.
Capa 3: La capa de red	La capa de red es la encargada de adecuar los datos en tránsito entre diversas redes físicas, técnicamente es la que divide los datos en el equipo de quien remite y los recompone en el dispositivo del destinatario.
Capa 4: La capa de transporte	Esta capa es la responsable del control de la velocidad de transmisión de los datos, comunicando la capa de red con la capa de sesión, encargándose de generar una comunicación transparente y segura entre dos sistemas. Puede fragmentar los datos en un paquete de menor tamaño y los segmentos más pequeños contienen información de encabezado que los identifica y permite que estos puedan volver a ser ensamblados en el dispositivo de destino.
Capa 5: La capa de sesión	Para que se dé la comunicación entre dispositivos, se requiere una aplicación responsable de crear una sesión, siendo esta un espacio único para el usuario, que lo identifica en el servidor remoto, siendo la sesión la que se encarga de garantizar que los archivos se transfieran de forma completa, y de que la retransmisión se restablezca si los datos están incompletos, al estar ligada la transmisión a la sesión. Esta transferencia hace más eficiente la comunicación sobre la red.
Capa 6: La capa de presentación	Esta capa es la encargada de preparar los datos con motivo que estos sean mostrados al usuario de manera ordenada, resulta ser la responsable de la codificación y decodificación de los datos para presentarlos a modo de información en texto simple o plano.
Capa 7: La capa de aplicación	Es la capa más familiar para los usuarios no técnicos y la que permite la comunicación directamente con el humano, por medio de la interfaz que se ejecuta utilizando protocolos de comunicación entre servidores web y los navegadores.

Fuente: Elaboración propia.

En la noción de sistema basado en capas, existe el concepto central de unidad de datos del protocolo, que actúa como unidad básica usada en el modelo de interconexión de sistemas abiertos.

Hasta aquí se han abordado las capas técnicas, y por decirlo de alguna manera las consideradas como clásicas, en las cuales no existe una conexión directa entre derecho, administración pública y ciberespacio.

Por lo anterior, en el mundo de lo jurídico, se ha propuesto introducir tres capas que escapan

de los elementos técnicos, dado que se vinculan más al ámbito organizacional, gubernamental e internacional desde una perspectiva jurídica. Cuya propuesta de inclusión en el modelo OSI ha sido desarrollada por el profesor norteamericano experto en Derecho, Ciberseguridad y privacidad, Peter Swire (2018), quien propone la inclusión de las capas 8, 9 y 10 adicionales a las 7 capas técnicas, para entender el ciberespacio y la ciberseguridad fuera de los estándares meramente técnicos, y trasladarlos al ámbito de organización social, así como vincularlas con el Derecho. Tal como se referencia en la tabla 2.

Tabla 2: Propuesta de capas de organización social

Número de capa	Función en el modelo
Capa 8: Organizacional.	Propone entender a la organización misma como una capa del modelo, que tiene la función de gestionar sus riesgos en el ciberespacio, diseñar e implementar acciones y políticas para desarrollar su actividad en el ciberespacio. Incluye la concientización y el dictado de reglas de comportamiento de los individuos que forman parte de la organización respecto a la ciberseguridad, así como la importancia de mantener una actitud vigilante ante posibles amenazas.
Capa 9: Gobierno.	Esta capa se desarrolla a nivel del Gobierno nacional, en la cual se encuentra la creación de leyes y políticas de aplicación general. Esta capa se centra en la regulación de cómo las personas y las organizaciones interactúan con la tecnología y los sistemas de información, fijando derechos y deberes de los usuarios del ciberespacio, con los respectivos efectos jurídicos de su actividad o comportamientos en línea.
Capa 10: Nivel internacional.	Esta capa resulta comprender el nivel de acuerdos y protocolos internacionales de aplicación internacional, tales como el Convenio de Budapest, lo que implica una colaboración internacional para la comprensión profunda de los riesgos cibernéticos y una actitud proactiva para prevenir

	amenazas que desestabilicen la paz y la seguridad internacional.
--	--

Fuente: Elaboración propia.

Claramente, en la inteligencia de entender a estas tres capas adicionales como parte del modelo, se debe fijar al concepto de unidad de datos del protocolo, para mantener la coherencia mediante una unidad básica. El doctor Peter Swire (2018, p.25) propone que estas deben estar regidas o relacionadas directamente con un acuerdo o expresiones de voluntades, en la capa 8 por los contratos, en la capa 9 por las leyes y en la capa 10 por los acuerdos diplomáticos.

Estos acuerdos de voluntades, los cuales son una unidad central para el derecho, resultan operativos en cada una de sus capas, siendo que, para las organizaciones de carácter público, como las municipalidades, se pueden incluir los actos administrativos, como parte de la capa 8. Lo que justamente, a un nivel organizacional del sector público, se vincula con la capa 9 a través de las leyes que los fundamentan a nivel nacional y esta, a su vez, con la capa 10 a través de los acuerdos y protocolos internacionales que podría suscribir el país en materias relacionadas con la actividad en el ciberespacio.

En este punto, es necesario indicar también que, en esta capa 8, hay una condición específica para las organizaciones de carácter público, quienes deben reglar de manera adecuada su interacción en línea, cuando no haga uso de su propia infraestructura tecnológica; dado que es común en la actualidad, ver actividad de entes públicos mediante el uso de plataformas, tales como redes sociales, sobre las cuales la organización en la capa 8 no tiene la condición de autoridad o gobierno.

Siendo que en estas plataformas actúan como

un usuario más con su capacidad de derecho privado, acorde con la facultad dada por el artículo primero de la Ley General de la Administración Pública, aceptando las reglas previstas por la aplicación, a través de contratos tecnológicos. Por lo que se debe tener también regulación interna para poder operar de manera correcta en estos entornos en los que no se comportan o tienen la capacidad de derecho público ni uso de sus potestades de imperio y, por lo tanto, no tiene la capacidad coercitiva de imponer su autoridad; dado que está en un “espacio” ajeno a su competencia como ente público, lo cual sería también parte del ciberespacio, pero no de su ciberterritorio.

En virtud de todo lo dicho, es necesario, entonces, que la municipalidad, como ente de derecho público con capacidad además de derecho privado, establezca su modelo de gobernanza en el ciberespacio, entendiendo su posición y capacidad de acción sobre la capa 8, regulando su actividad a través de procedimientos, reglamentos y políticas.

Es importante destacar que, así entendidas, estas capas resultan cruciales en el entorno de la ciberseguridad, ya que incluso las defensas tecnológicas más avanzadas pueden ser eludidas, si los usuarios, las organizaciones y los Estados no están conscientes de las amenazas o no siguen buenas prácticas de seguridad y no fortalecen su postura de seguridad en línea. Además, resultan operativas en el sistema OSI, para fomentar una cultura de seguridad cibernética que promueva la responsabilidad compartida entre todos los miembros de una organización, una sociedad o la comunidad internacional. Por lo cual, la

introducción de las capas 8, 9 y 10 enfatizan la importancia de los factores humanos y sociales en la protección de la información, además, resultan esenciales para complementar las medidas tecnológicas y construir una defensa integral contra las amenazas en línea, tal como resalta la OEA, BID (2020 p. 39).

APLICAR EL ARTE DE LA GUERRA PARA PROTEGER EL CIBERTERRITORIO DE LOS GOBIERNOS LOCALES

La introducción de los conceptos de ciberterritorialidad y ciberseguridad al ámbito de lo municipal plantea grandes desafíos, los cuales requieren de una capacidad estratégica casi militar en el ciberespacio.

En virtud de lo anterior, es posible que, para abordar el concepto de ciberterritorio, resulte útil echar mano de la obra clásica de estrategia militar el Arte de la Guerra, escrita por Sun Tzu en el siglo V a.C. Dado que el concepto de territorialidad y las estrategias para su defensa ahí expuestas pueden ser adaptadas también, traspasando las fronteras físicas para adentrarse en el ciberespacio.

En este último apartado, se pretende adaptar las enseñanzas sobre la territorialidad expuestas en el Arte de la Guerra, para estudiar cómo estas pueden ser aplicadas y reinterpretadas en el contexto del ciberespacio que, tal como se ha revisado, resulta ser un escenario cada vez más relevante en el ámbito del derecho público, el ordenamiento jurídico, la seguridad y la geopolítica.

El concepto de territorialidad en el *Arte de la Guerra* pone énfasis en la importancia de conocer y controlar el terreno en el que se libra una batalla. Implica la comprensión de la geografía, el clima, los recursos y las ventajas estratégicas de un lugar. Sun Tzu (2022) enfatiza que quien domina el terreno tiene una ventaja crucial en la

confrontación, el artículo X reza en su inicio: “*En la superficie de la tierra, no todos los lugares son equivalentes. Debes huir de algunos y buscar otros; pero tienes que conocerlos todos a la perfección*” (p.77).

Siendo que el ciberespacio resulta ser un nuevo ámbito en el que se libran batallas de información y ciberseguridad, la territorialidad se transforma en el conocimiento y control de la red, los sistemas, la infraestructura y la información digital. Los actores en el ciberespacio buscan obtener ventajas estratégicas a través del acceso y la manipulación de estos elementos, por lo cual una municipalidad debe conocer y controlar su infraestructura tecnológica como parte de su ciberterritorio.

Tal como se ha visto a lo largo de este estudio y lo indica claramente López de Anda M. (2011), la naturaleza virtual, sin fronteras y atemporal del ciberespacio, dificulta la definición clara del territorio digital y, por lo tanto, hace más complicada la atribución de responsabilidades y la fijación de acciones de protección. Además, la constante evolución tecnológica exige una adaptabilidad y actualización constante de las estrategias de ciberseguridad.

Por lo anterior, el concepto de ciberterritorialidad se convierte en un componente crítico de la estrategia de la municipalidad en su actividad en línea, dado que como organización que actúa en la capa 8 del modelo OSI ampliado, debe comprender su conexión con las capas técnicas y con las demás capas sociales, realizando una especie de topografía digital, para poder identificar vulnerabilidades y proteger los activos digitales, así como mantener una ventaja competitiva. Esto incluye la defensa contra ciberataques, la protección de la información sensible, la capacidad de respuesta ante incidentes y las demás obligaciones que sean impuestas por el ordenamiento jurídico nacional e internacional,

lo cual genera un desafío principalmente en adaptación y mejora continua y sostenida de sus capacidades digitales.

Es así como se puede decir que la territorialidad, como principio fundamental en el *Arte de la Guerra*, puede ser reinterpretada para encontrar una nueva dimensión en el ciberespacio. La ciberterritorialidad como concepto puede convertirse en un elemento de sentido crucial en el desarrollo de la estrategia de ciberseguridad, con implicaciones en la protección de la información y la defensa contra ciberamenazas.

Sun Tzu (2022, p.48) también destaca la necesidad de la flexibilidad y la adaptación en la estrategia. En el contexto del ciberespacio, esta premisa se traduce en la capacidad de ajustar continuamente las defensas en función de la evolución de las amenazas y de las tecnologías, así indica el artículo IV: *“El agua, en su movimiento, sigue la situación del terreno en el que corre. Asimismo, tu ejército debe adaptarse al terreno sobre el que se mueve (...) El General hábil sacará partido incluso de las circunstancias más peligrosas y críticas. Sabrá hacer tomar la forma que quiera no solo al ejército que dirige, sino incluso al de su enemigo”*.

No se trata solo de contar con robustas barreras digitales, sino de estar preparados para responder rápidamente a incidentes y de mantenerse actualizado respecto a las últimas tendencias y técnicas utilizadas por ciberdelincuentes; lo que requiere necesariamente la vinculación de las capas técnicas del modelo OSI con las tres capas sociales propuestas por el profesor Swire (2018).

La defensa de un organismo público en el ciberespacio también guarda una estrecha relación con otros principios expuestos por Sun Tzu (2022, p. 28), al indicar en su artículo III: *“Conoce a tu enemigo y concéte a ti mismo. Aunque tuvieras que sostener cien guerras, cien veces obtendrás*

la victoria”. En el contexto cibernético, esto se traduce en comprender las vulnerabilidades propias y las posibles amenazas digitales que enfrenta la institución pública. Es esencial identificar los puntos débiles y anticiparse a las tácticas que un adversario podría emplear para vulnerar la seguridad digital.

Otro punto relevante es la importancia de la información y su manipulación, Sun Tzu (2022, p.47) enfatiza que la información precisa y oportuna es esencial para la toma de decisiones. En el ciberespacio, esto se traduce en la necesidad de garantizar la confidencialidad, disponibilidad e integridad de la información, principios fundamentales de los sistemas de seguridad de la información. Para Sun Tzu, el proteger su información de relevancia y conocer la del adversario es clave para tener el control de las situaciones, en el ciberespacio la información es el activo principal, por lo cual debe ser cuidada con recelo. El principio de la sorpresa es también crucial en la defensa del ciberterritorio. Sun Tzu (2022) sugiere la importancia de mantener ocultas las intenciones y capacidades propias, lo cual se traduce en la necesidad de mantener actualizada y protegida la infraestructura digital, de manera que un atacante potencial no pueda penetrar fácilmente las defensas ni conocer las estrategias de seguridad.

El principio de la economía de recursos también es relevante en la ciberdefensa. Sun Tzu (2022, pp. 20-21) acentúa la importancia de utilizar los recursos de manera eficiente y de evitar el derroche. En el ámbito digital, esto significa priorizar las inversiones en ciberseguridad de acuerdo con la criticidad y el riesgo asociado a los activos digitales y las capacidades financieras de cada entidad.

De esta manera, se ve cómo la aplicación del concepto de ciberterritorialidad en el ámbito del derecho público implica que la administración

pública entienda cómo proteger su "territorio digital", que abarca desde la infraestructura tecnológica hasta los datos y servicios digitales que proporciona. Esto contribuye a fortalecer la seguridad cibernética a nivel local y a crear un entorno digital seguro y confiable para la comunidad, así como convertirse en una primera línea de defensa para garantizar la ciberseguridad, dentro de su papel en la capa 8 del modelo OSI ampliado.

EPÍLOGO: ENSAYANDO LA RESPUESTA AL PAPEL DEL GOBIERNO LOCAL EN EL CIBERESPACIO

Luego de realizar una labor consciente y arriesgada de adaptación de principios jurídicos como el de soberanía, territorialidad, autonomía municipal e interés público local, para operativizar su función en el ciberespacio, exponer la adaptación propuesta para la inclusión de niveles sociales en el modelo OSI propuesta por el profesor Swire (2018), abandonando la concepción de las capas meramente técnicas de dicho modelo, y adaptar una obra clásica al ámbito del ciberespacio y la ciberseguridad, es posible ensayar una respuesta para la pregunta: ¿cuál es el papel que debe desarrollar un gobierno local en el ciberespacio?

Para contestar, se debe recordar someramente lo aquí estudiado e indicar de entrada, que la aplicación efectiva de la autonomía municipal en el ciberespacio es un desafío continuo, debido a la naturaleza global de las redes y sistemas digitales, así como la constante noción que lleva a entender la competencia de la municipalidad como ubicada o limitada a lo local en un espacio físico.

En este sentido, si el ciberespacio rompe los conceptos de tiempo y espacio físico porque las interacciones y amenazas en este entorno operan en una escala y velocidad que superan los límites físicos tradicionales, resulta vital el cambio de

concepción acerca del ejercicio de la competencia municipal en su elemento teleológico, ampliando el margen de actividad al ciberespacio, en aras de garantizar del interés público local. Esto implica entender la necesaria adaptación de la actividad administrativa del municipio en el ciberespacio, dado que, en ese espacio etéreo e intangible, hay intereses públicos locales que deben ser tutelados y protegidos; por lo cual se deben diseñar e implementar procesos y estrategias ágiles, adaptativas y conscientes para hacer frente a los desafíos que presenta ese entorno digital dinámico y complejo, además, garantizar como pilares la protección de la infraestructura tecnológica municipal y el efectivo gobierno de la información y de los datos que utiliza la municipalidad como ente público, implementando acciones para su confidencialidad, disponibilidad e integridad.

Es aquí donde la aplicación del concepto de ciberterritorialidad en el ámbito municipal implica que la administración local debe entender y proteger su "territorio digital", que abarca desde la infraestructura tecnológica hasta los datos y servicios digitales que proporciona; es decir, cubre toda su actividad administrativa en línea. Si se logra comprender y operativizar este concepto, se contribuiría a fortalecer la seguridad cibernética a nivel local y a crear un entorno digital seguro y confiable para la comunidad global (OEA, BID, 2020, p. 26).

El papel de la municipalidad se da en la capa número 8 del modelo OSI, que propone entender al propio ente municipal como una capa del modelo, con la función de gestionar los riesgos en el ciberespacio, diseñar e implementar acciones y políticas para desarrollar su actividad en línea, incluyendo la concientización y el comportamiento de los individuos de la organización respecto a la ciberseguridad, así como poner énfasis en mantener una actitud vigilante ante posibles amenazas, conectando con la regulación nacional e internacional que regula su actividad y la de los

demás usuarios de internet. Lo que demuestra la capacidad para proteger la información y la infraestructura digitales como parte de la defensa de su ciberterritorio.

CONCLUSIONES

En el contexto del ciberespacio, el gobierno local asume un rol crucial como organización que actúa en la capa 8 del modelo OSI ampliado. Su labor implica la protección de elementos vitales para el funcionamiento de la comunidad en línea. Esto incluye la salvaguarda de infraestructura esencial como redes de comunicación y sistemas informáticos, que son fundamentales para la administración y prestación de servicios digitales a los ciudadanos, y la gestión de sus riesgos en el ciberespacio, diseñando e implementando acciones específicas, procesos, políticas y reglamentos para regular su actividad en el ciberespacio.

Sin duda, la noción de ciberterritorialidad añade una dimensión crucial a la labor del gobierno local en el ciberespacio. Al obligarlo a comprender y proteger su "territorio digital", que abarca desde la infraestructura tecnológica hasta los datos y servicios digitales que proporciona, si esto se logra, el gobierno local asegura un entorno en línea seguro y confiable para la comunidad. Esta perspectiva no solo garantiza la integridad de los recursos digitales locales, sino que también facilita la coordinación con otras instituciones y niveles de gobierno en la protección de intereses comunes en el ciberespacio, reforzando así la seguridad cibernética a nivel local y contribuyendo al desarrollo de un espacio digital más seguro a nivel global.

En resumen, el papel del gobierno local en el ciberespacio es multifacético y abarca desde la salvaguarda de infraestructuras críticas hasta la promoción de la innovación segura, pasando por la educación y la colaboración interinstitucional,

la gestión de datos y la respuesta ante emergencias cibernéticas. En última instancia, el gobierno local debe erigirse como un guardián de confianza en su ciberterritorio, velando por el bienestar y la seguridad de sus ciudadanos en este entorno cada vez más interconectado.

BIBLIOGRAFÍA

Libros:

Beah, G., & Yáñez, A. 2017. *Introducción a los Contratos Tecnológicos*. Editorial Tecnológica de Costa Rica.

Breton, P. 2000. *La utopía de la comunicación: el mito de la aldea global*. Buenos Aires: Nueva Visión.

Peña, D. 2007. *Responsabilidad civil en la era digital*. Universidad Externado de Colombia.

Sun Tzu. 2022. *El Arte de la Guerra*. Editorial Alma.

Revistas:

López de Anda M. 2011. M. "Epistemologías del ciberespacio." *Virtualis* No. 4, julio- diciembre 2011. <https://www.revistavirtualis.mx/index.php/virtualis> .ISSN: 2007-2678.

Siles, I. 2007. "Cibernética y sociedad de la información: el retorno de un sueño eterno." *Signo y Pensamiento*, 26(50), 84-99.

Swire, P. 2018. "Privacy and Security: A Pedagogic Cybersecurity Framework." *SRNN*, Georgia Tech Scheller College of Business Research Paper No. 18-42.

Valencia A. 2016. "La ingeniería, la transhumanidad y la posthumanidad" *Revista Ingeniería & Sociedad*, Universidad de Antioquia, No. 11.

Recursos electrónicos:

social. Elaboración propia.

Comisión Económica para América Latina y el Caribe (CEPAL). 2021. *Tecnologías digitales para un nuevo futuro* (LC/TS.2021/43). Santiago. <https://repositorio.cepal.org/server/api/core/bitstreams/879779be-c0a0-4e11-8e08-cf80b41a4fd9/content> (Consultado el 5 de septiembre de 2023).

OEA, BID. 2020. *Ciberseguridad, Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe*, Reporte Ciberseguridad. <https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe> (Consultado el 8 de agosto de 2023).

Ruiz, M. 2018. “Ciberterritorialidad: ¿Un nuevo principio de aplicación espacial de la ley penal?”. Microjuris.com. <https://aldiaargentina.microjuris.com/2018/11/06/ciberterritorialidad-un-nuevo-principio-de-aplicacion-espacial-de-la-ley-penal> (Consultado el 23 de agosto de 2023).

Trabajos Académicos:

Velasco, C. 2009. *Competencias autonómicas y puntos de conexión*. Tesis doctoral, Universitat Pompeu Fabra.

Legislación:

Código Municipal de Costa Rica, 1998. Gaceta N°: 94 del: 18 de mayo de 1998.

Ley General de la Administración Pública de Costa Rica, 1978. N° Gaceta: 102 del: 30 de mayo de 1978, Alcance: 90.

Tablas:

Tabla 1: Capas técnicas del modelo OSI. Elaboración propia.

Tabla 2: Propuesta de capas de organización