La Ley de Ciberseguridad y los límites de legislar contra la incertidumbre

Cuando una sociedad enfrenta una amenaza que percibe como existencial, su primer reflejo institucional suele ser legislar. La idea subyacente es razonable en apariencia: si el problema es nuevo, hace falta una norma nueva. Si el problema es complejo, hace falta una norma extensa. Si el problema es urgente, hace falta una norma inmediata. La Ley Orgánica para el Fortalecimiento de la Ciberseguridad, publicada en el Registro Oficial Suplemento N° 290 del 22 de mayo de 2026, es una manifestación contemporánea de ese reflejo.

El reflejo, sin embargo, merece interrogarse. No porque la ciberseguridad no sea una preocupación legítima del Estado, que evidentemente lo es, sino porque la decisión de legislar de cierta manera, con cierto alcance y bajo cierta arquitectura institucional, tiene consecuencias que exceden el contenido nominal de la norma.

1. Un diagnóstico de fondo antes que un comentario de detalle

La ley aprobada incorpora avances sustantivos que conviene reconocer. La despenalización del hacking ético realizado con consentimiento del titular, contenida en la reforma al artículo 232 del Código Orgánico Integral Penal, resuelve una zona gris que durante años puso en riesgo a profesionales que prestaban un servicio socialmente útil. La articulación institucional entre un CSIRT Nacional y los CSIRT sectoriales reemplaza una arquitectura de respuesta fragmentada por una coordinación más estructurada. La definición de categorías como infraestructura crítica digital, incidente de ciberseguridad y prestador de servicios digitales aporta vocabulario técnico que el ordenamiento ecuatoriano carecía de manera explícita.

Lo que viene a continuación no busca desconocer esos aciertos. Busca examinar, desde la perspectiva de quien acompaña jurídicamente a empresas y proyectos de tecnología, una pregunta más amplia: qué tipo de regulación tecnológica estamos construyendo en el Ecuador, y qué efectos tiene esa elección sobre los actores que viven sus consecuencias.

2. El problema de regular más antes que regular mejor

La ley cubre, en sus treinta y nueve páginas, materias tan diversas como la arquitectura institucional de respuesta a incidentes, las obligaciones de prestadores de servicios digitales, el régimen administrativo sancionador, la reforma a la Ley Orgánica de Educación Intercultural en materia de currículo escolar, la reforma a la Ley Orgánica de Comunicación, la reforma al Código Orgánico Integral Penal, la reforma a la Ley Orgánica de Transporte Terrestre, la reforma a la Ley Orgánica de Telecomunicaciones y la reforma a la Ley Orgánica de Protección de Datos Personales.

Una sola ley que reforma siete cuerpos normativos distintos no es, técnicamente, una ley de ciberseguridad. Es una intervención normativa transversal disfrazada de ley sectorial. La distinción importa, porque cuando una norma intenta resolver demasiado a la vez, suele resolver cada cosa con menos precisión de la que cada una requería por separado. La reforma curricular sobre educación digital, por ejemplo, merecía un debate específico dentro de la Ley Orgánica de Educación Intercultural, con

participación de la comunidad educativa, no su inserción en una ley pensada para infraestructura crítica.

Esta práctica, que la doctrina constitucional ha advertido en otros contextos como leyes ómnibus, erosiona la calidad deliberativa del proceso legislativo. Cada materia merece su tiempo, su debate especializado y su técnica propia. Mezclarlas en un solo paquete legislativo simplifica el trámite político, pero degrada el producto normativo.

3. La indeterminación como diseño regulatorio

Hay un patrón en la ley que merece subrayarse. Las definiciones clave están construidas con la mayor amplitud posible. La categoría de activo digital o informático abarca todo recurso digital, tangible o intangible, incluidos datos, información, sistemas, aplicaciones o plataformas. El catálogo de infraestructura crítica digital queda diferido a una resolución posterior del ente rector. La calificación de quién es responsable administrativamente incluye, en el literal d del artículo 20-Q, a personas jurídicas privadas que participen en la provisión de servicios tecnológicos indispensables para la operación de servicios esenciales, sin que se especifique con criterio objetivo qué empresas entran y cuáles no.

Esta amplitud, defendida en el debate legislativo como flexibilidad regulatoria, tiene un costo concreto para quienes deben cumplir la norma. Las empresas no saben hoy si están dentro del perímetro regulado o fuera de él. Esa información, supuestamente, se sabrá en doce meses, cuando el ente rector expida la normativa secundaria. Mientras tanto, una sanción potencial del uno coma cinco por ciento del volumen de negocios anual queda como espada de Damocles sobre operadores que ni siquiera saben si están sujetos a la ley.

La técnica legislativa contemporánea ha incorporado, con razón, la noción de que las normas demasiado específicas envejecen rápido frente al cambio tecnológico. Esa observación es válida. Pero la respuesta no puede ser legislar con tal vaguedad que el ciudadano regulado dependa, para conocer sus obligaciones, de un acto administrativo posterior expedido por la propia autoridad que lo va a sancionar. Esa arquitectura concentra demasiado poder discrecional en el ente rector y deja al regulado en una posición de indefensión informativa que el principio constitucional de seguridad jurídica no debería tolerar.

4. La superposición de competencias como riesgo subestimado

El derecho administrativo ecuatoriano ha construido, a lo largo de las últimas décadas, una arquitectura de órganos de control especializados. La Superintendencia de Bancos supervisa la banca, la Superintendencia de Compañías, Valores y Seguros supervisa el mercado de valores y las sociedades comerciales, la Superintendencia de Protección de Datos Personales aplica la LOPDP, la Agencia de Regulación y Control de las Telecomunicaciones regula su sector. Cada una de esas autoridades ya cuenta con normativa de gestión de riesgos digitales y con potestad sancionadora dentro de su ámbito.

La nueva ley superpone, encima de esa arquitectura existente, una autoridad rectora en ciberseguridad con potestades de coordinación, fiscalización subsidiaria, sanción

residual y expedición de normativa técnica. La fórmula adoptada por el texto final, tras la objeción presidencial, mitiga el problema al reconocer la especialidad de los órganos sectoriales y limitar al ente rector a una actuación subsidiaria. Pero la mitigación no elimina la zona gris. Una empresa regulada simultáneamente por una superintendencia sectorial y por el ente rector de ciberseguridad puede enfrentar interpretaciones técnicas distintas sobre el mismo hecho, requerimientos de información paralelos y, en el peor escenario, procedimientos sancionatorios concurrentes que el principio de non bis in ídem no siempre alcanza a resolver con claridad.

La pregunta práctica que un abogado debe formularse no es si la ley reconoce la coordinación interinstitucional, que lo hace, sino si esa coordinación funciona efectivamente en la operación cotidiana del aparato regulatorio ecuatoriano. La experiencia comparada sugiere que la coordinación entre superintendencias autónomas y entes rectores nuevos es uno de los puntos más débiles del derecho administrativo, no por mala fe institucional, sino por inercia organizacional natural.

5. Una observación sobre la tendencia regulatoria de fondo

Hay un debate más amplio que esta ley pone sobre la mesa, aunque no lo nombre explícitamente. Cuál es el modelo regulatorio que el Ecuador está construyendo para el sector tecnológico.

Las decisiones acumuladas de los últimos años sugieren una respuesta preocupante. Las normas tienden a ser amplias en su alcance, generales en sus definiciones, severas en sus sanciones y dependientes de normativa secundaria expedida por entes administrativos con discrecionalidad amplia. Esta combinación, observada en el derecho comparado, suele producir efectos que rara vez son los que el legislador buscaba: empresas medianas que evitan operar en sectores regulados, inversión extranjera que prefiere jurisdicciones con marcos más predecibles, y un cuerpo regulatorio cuya aplicación efectiva resulta selectiva, generando arbitrajes regulatorios entre actores comparables.

El Ecuador tiene, en el universo tecnológico, ventajas comparativas interesantes. Una Ley de Modernización a la Ley de Compañías de 2020 que reconoce blockchain como medio idóneo de representación accionaria. Una Ley Fintech de 2022 que crea un sandbox regulatorio coordinado entre tres autoridades. Un ecosistema emergente de proyectos Web3, fintech y servicios digitales que podría posicionar al país regionalmente si las condiciones lo permiten.

La Ley de Ciberseguridad, en su forma actual, agrega una capa de incertidumbre regulatoria a ese ecosistema. No la cancela, no la destruye, pero la encarece. Cada empresa que opera en tecnología tendrá que sumar a su agenda de compliance una nueva variable cuyas reglas concretas se conocerán recién en los próximos meses. Para las grandes empresas, esto es manejable mediante equipos legales internos. Para las medianas y pequeñas, es una barrera adicional que pesa más de lo que la política pública parece considerar.

6. El principio de proporcionalidad regulatoria

El derecho administrativo contemporáneo ha desarrollado el concepto de proporcionalidad regulatoria como criterio rector de la actividad legislativa en sectores complejos. El principio sostiene que una norma debe imponer las cargas mínimas necesarias para alcanzar su objetivo legítimo, evitando exigencias que excedan lo estrictamente requerido.

Aplicado a la ciberseguridad, el principio sugiere que la respuesta regulatoria debe escalar con el riesgo real. Una institución financiera sistémica enfrenta exigencias estrictas, justificadas por el impacto potencial de un incidente sobre el sistema económico. Una pequeña empresa de software que desarrolla aplicaciones de productividad enfrenta exigencias menores, porque su capacidad de generar riesgo sistémico es menor.

La ley adoptada no incorpora suficientemente esta lógica de proporcionalidad ex ante. La aplica solo en la graduación de la sanción ex post, mediante los criterios del artículo 20-X. Pero el costo del cumplimiento, las obligaciones de gestión de riesgos, los protocolos de notificación de incidentes y los requerimientos técnicos no están suficientemente diferenciados según el tamaño y la criticidad real del operador regulado. El resultado es una carga regulatoria que pesa desproporcionadamente sobre los actores más pequeños, que son justamente los que el ecosistema necesita preservar para mantener competencia y diversidad.

7. El camino que viene

La ley está vigente desde el 22 de mayo de 2026. La normativa secundaria llegará en los próximos seis a doce meses. El catálogo de infraestructura crítica digital quedará definido durante el primer año. Los CSIRT sectoriales se formalizarán en plazos variables.

Esa fase reglamentaria es donde se va a decidir, en términos concretos, si la ley se aplica con criterios de proporcionalidad o si se transforma en una nueva capa de fricción regulatoria para el ecosistema digital ecuatoriano. El sector privado, las cámaras especializadas, los gremios profesionales y la academia tienen aquí una ventana de participación cuyo aprovechamiento determinará el carácter práctico del régimen.

Desde la perspectiva del derecho corporativo y tecnológico, nuestra recomendación profesional para las empresas que asesoramos es triple.

- **En primer lugar,** mapear ahora, no después, su exposición potencial a la ley, identificando si su actividad pudiera calificarse como infraestructura crítica digital, prestador de servicios digitales o servicio tecnológico indispensable.
- **En segundo lugar,** comenzar la construcción documental de un programa de cumplimiento básico, aun antes de que la normativa secundaria se expida, porque ese documento será el primer escudo defensivo en una eventual fiscalización.
- **En tercer lugar,** participar institucionalmente, vía gremios o cámaras, en la fase de socialización de la normativa secundaria, porque los detalles que se

decidan ahí pesarán más que la propia ley sobre la operación cotidiana del negocio.

La ciberseguridad es, sin duda, una preocupación legítima del Estado. La pregunta no es si regular, sino cómo hacerlo de manera que el remedio no resulte más costoso que la enfermedad. La sobrerregulación no produce más seguridad: produce cumplimiento formal, costos de transacción más altos, e incentivos para que los actores más sofisticados ejerciten arbitraje regulatorio mientras los menos sofisticados quedan expuestos.

El Ecuador del 2030 se está escribiendo en la normativa secundaria de los próximos meses. Vale la pena pensarla con calma.