Protección de datos en Paraguay: por qué copiar el modelo europeo sería un grave error

Paraguay ha aprobado una nueva Ley de Protección de Datos Personales que moderniza de forma sustancial su marco jurídico. La reforma era necesaria, pero su futura reglamentación plantea una cuestión decisiva: hasta qué punto debe Paraguay acercarse al modelo europeo. La experiencia de la Unión Europea demuestra que una protección razonable de la privacidad puede degenerar fácilmente en una estructura regulatoria costosa, burocrática y de utilidad marginal muy reducida. El problema no es que el modelo europeo sea demasiado caro para Paraguay y asumible para Europa. El problema es más profundo: el modelo europeo es malo también para Europa porque consume recursos, dificulta la innovación y transforma operaciones empresariales normales en problemas jurídicos. En Paraguay esos efectos serían simplemente más graves.

Paraguay aprobó en noviembre de 2025 la Ley n.º 7.593/2025 de Protección de Datos Personales, estableciendo por primera vez un régimen general aplicable al tratamiento de datos personales y creando una autoridad especializada en la materia. La ley prevé un período amplio antes de su plena entrada en vigor y remite numerosas cuestiones a una futura reglamentación, de modo que durante 2026 y 2027 Paraguay conserva un margen importante para decidir cómo funcionará realmente el sistema. (bacn.gov.py)

Ese margen debería utilizarse con prudencia. La ley incorpora elementos razonables que cualquier economía moderna necesita: obligaciones de seguridad, protección frente a determinados usos abusivos, derechos de acceso y rectificación, reglas sobre información sensible, procedimientos ante brechas de seguridad y mecanismos para transferencias internacionales. El problema aparece cuando, partiendo de estos objetivos legítimos, se construye una arquitectura general de compliance semejante a la desarrollada por la Unión Europea alrededor del Reglamento General de Protección de Datos (RGPD).

La experiencia europea demuestra que ese paso es extraordinariamente fácil. Se empieza protegiendo historiales médicos, información financiera o bases de datos sensibles y se termina obligando a cualquier pequeña empresa a justificar jurídicamente por qué conserva el correo electrónico de un antiguo cliente, qué fundamento utiliza para enviar una comunicación comercial o dónde se encuentra físicamente el servidor de su proveedor informático. Ahí está el verdadero riesgo para Paraguay.

Del control de abusos a la regulación de cualquier dato

El modelo europeo parte de una definición extremadamente amplia de dato personal. Un nombre, un correo electrónico, un número de teléfono, una dirección IP, una fotografía, un identificador profesional o cualquier información que permita relacionar determinados datos con una persona pueden quedar dentro del ámbito de la regulación. La consecuencia es que prácticamente cualquier empresa moderna está permanentemente tratando datos personales y, por tanto, queda sometida a obligaciones jurídicas, aunque su actividad no presente ningún riesgo serio para la privacidad.

Una empresa con veinte empleados, una asesoría contable, un restaurante con sistema de reservas, un hotel, una inmobiliaria o un comercio electrónico puede encontrarse ante una sucesión interminable de cuestiones: qué base jurídica justifica cada tratamiento, cuánto tiempo puede conservarse cada dato, si el interesado fue suficientemente informado, si existe una transferencia internacional, si el proveedor tecnológico debe firmar determinadas cláusulas, si el uso posterior del dato es compatible con la finalidad original, si debe documentarse un interés legítimo o si hace falta una evaluación de impacto. El problema no está en ninguna de estas

preguntas considerada aisladamente, sino en su acumulación. Una norma destinada inicialmente a proteger al ciudadano frente a daños reales acaba convirtiendo la utilización de información ordinaria en una actividad permanentemente juridificada.

Este proceso ya se ha producido en Europa y ha creado una situación difícil de justificar desde el análisis económico del derecho. El problema no consiste simplemente en que las empresas europeas soporten costes elevados porque son suficientemente ricas para hacerlo. Esa idea sería equivocada. Los costes regulatorios son costes reales en cualquier economía. Cada euro que una empresa europea destina a abogados, consultores, delegados de protección de datos, plataformas de consentimiento o auditorías es un euro que deja de utilizar en inversión, contratación, innovación o reducción de precios. Europa también es más pobre como consecuencia de esos costes. Lo que ocurre es que una economía con niveles salariales más altos, mayor productividad media y empresas de mayor tamaño puede absorberlos con menos dificultad visible. En Paraguay, donde una parte mucho mayor del tejido empresarial está formada por pequeñas y medianas empresas y donde el capital disponible es más escaso, el mismo tipo de regulación produciría un daño proporcionalmente mayor.

El verdadero coste del RGPD no son las multas

Cuando se habla de protección de datos en Europa suele destacarse el tamaño de determinadas sanciones impuestas a grandes empresas tecnológicas. Sin embargo, desde el punto de vista económico, ese probablemente no sea el principal problema. El coste más importante es cotidiano y mucho menos visible: las horas de abogados, consultores, técnicos, responsables internos y empleados dedicados a demostrar que una empresa cumple.

La propia documentación utilizada por instituciones europeas ha recogido estudios según los cuales una parte relevante de las pequeñas y medianas empresas incurrió en costes superiores a 10.000 euros durante la implantación inicial del RGPD y un porcentaje significativo superó incluso los 50.000 euros. Otros trabajos estimaron miles de horas de preparación interna en organizaciones de cierta dimensión. (eur-lex.europa.eu)

No se trata de trasladar mecánicamente esas cifras a Paraguay, porque los salarios y las estructuras empresariales son diferentes. Lo importante es la lógica económica. Una empresa paraguaya con 25 empleados, unos miles de clientes, cámaras de seguridad, página web, un sistema de nóminas, correo corporativo, almacenamiento en la nube y un proveedor de marketing podría acabar necesitando inventariar tratamientos, documentar bases jurídicas, redactar avisos, revisar contratos, establecer plazos de conservación, preparar protocolos de ejercicio de derechos, formar al personal, gestionar incidentes y comprobar si debe realizar evaluaciones de impacto o designar responsables especializados.

Parte de esas obligaciones tiene sentido cuando existe un riesgo real. No lo tiene necesariamente cuando se aplica de manera indiscriminada. Hay una diferencia enorme entre exigir a una empresa que proteja adecuadamente contraseñas, datos médicos o información financiera y exigirle una extensa documentación jurídica para conservar el email profesional de una persona con la que mantuvo una relación comercial legítima. El modelo europeo tiende a colocar ambos problemas dentro de una misma estructura normativa y ésa es precisamente una de sus mayores debilidades.

La industria de cumplimiento no crea riqueza por el mero hecho de facturar

Otro efecto del RGPD ha sido la creación de un sector económico entero dedicado al cumplimiento: consultores, delegados externos de protección de datos, plataformas para gestionar consentimientos, herramientas para responder solicitudes, auditorías, cursos de formación,

software de inventario y asesoramiento sobre transferencias internacionales. Todo esto genera facturación y empleo, pero sería un error concluir que por ello genera riqueza neta.

Si una regulación obliga a una empresa a contratar un servicio que antes no necesitaba, el gasto aparece en el PIB, pero el coste de oportunidad sigue existiendo. Esos recursos podrían haberse utilizado para producir bienes, prestar servicios, invertir, mejorar salarios o contratar trabajadores. La creación de una burocracia privada alrededor de una burocracia pública no convierte la regulación en productiva.

Esto debe tenerse especialmente en cuenta en Paraguay. Una empresa pequeña que destina varios miles de dólares anuales a cumplimiento puede estar renunciando a una contratación, una máquina, una reforma o una inversión comercial. El problema europeo no desaparece por el hecho de que una gran compañía alemana o francesa pueda asumir ese gasto con mayor facilidad. El gasto continúa siendo improductivo también allí. En Paraguay, simplemente, puede ser más destructivo.

El problema de la utilidad: mucho procedimiento y pocos beneficios demostrables

La privacidad tiene valor y sería absurdo negarlo. Nadie debería poder divulgar libremente historiales médicos, comerciar con contraseñas, utilizar información financiera para cometer fraude o ignorar negligentemente una brecha de seguridad. El problema aparece cuando la regulación se extiende desde esos supuestos claros hacia tratamientos de importancia mínima y pretende resolverlos mediante más información, más consentimiento y más documentación.

El ejemplo más visible es el de los banners de cookies. Millones de europeos reciben diariamente avisos que prácticamente nadie quiere leer y a los que la mayoría responde intentando simplemente eliminar el obstáculo. Se ha creado una industria de plataformas de consentimiento, configuraciones, asesores y auditorías para gestionar una interacción que con frecuencia no aporta una decisión real del usuario. Es cierto que el régimen de cookies procede de la interacción entre el RGPD y la normativa ePrivacy, pero económicamente forma parte de la misma filosofía: suponer que más avisos, más consentimiento y más formalidades equivalen necesariamente a más protección.

El resultado es discutible. Una regulación que obliga a millones de personas a pulsar mecánicamente botones que no leen debería, como mínimo, inducir a cuestionar si la regulación está alcanzando su objetivo. Si el ciudadano no presta atención a la información porque recibe demasiada, la obligación de informar deja de mejorar su capacidad de decisión y se convierte simplemente en un coste más.

La evidencia económica disponible tampoco permite sostener que el enorme esfuerzo europeo haya producido beneficios proporcionales. Un estudio del NBER sobre millones de aplicaciones Android encontró que la implantación del RGPD estuvo asociada a una fuerte reducción del número de aplicaciones disponibles y de la creación de nuevas aplicaciones. (nber.org) Otro estudio identificó, tras la entrada en vigor del RGPD, una caída significativa de la inversión de capital riesgo estadounidense en empresas europeas, especialmente en compañías jóvenes e intensivas en datos. (nber.org) Un tercer trabajo estimó importantes reducciones en almacenamiento y procesamiento de datos por empresas europeas, interpretando el resultado como equivalente a un fuerte incremento del coste económico de utilizar datos como factor productivo. (nber.org)

Estos estudios no demuestran que cualquier protección de datos sea mala. Sí demuestran algo mucho más importante: el modelo europeo tiene un coste económico medible y ese coste afecta precisamente a innovación, inversión y utilización productiva de información.

Paraguay debería regular el daño, no la existencia del dato

La futura reglamentación paraguaya debería partir de una lógica diferente. La intensidad de la regulación debería depender del riesgo real de daño y no simplemente de que exista un "dato personal".

Los historiales médicos, la información financiera, los datos biométricos, las contraseñas, los datos de menores, la prevención del fraude, la suplantación de identidad, las grandes filtraciones y la venta clandestina de bases justifican controles intensos. En estos ámbitos la legislación puede y debe ser exigente. En cambio, el tratamiento normal de nombres, teléfonos, correos electrónicos profesionales, relaciones comerciales y documentación ordinaria debería quedar sometido a reglas sencillas y fácilmente comprensibles.

La diferencia es importante porque el modelo europeo tiende a considerar que todo tratamiento debe ser jurídicamente justificado y documentado y que después la intensidad de las obligaciones puede variar según el riesgo. Paraguay debería invertir el razonamiento: los tratamientos ordinarios y de bajo riesgo deberían presumirse lícitos y quedar sujetos sólo a obligaciones básicas, mientras que la regulación compleja debería reservarse para situaciones verdaderamente peligrosas.

Esa diferencia de enfoque puede determinar si la nueva ley termina protegiendo realmente a las personas o simplemente construyendo una nueva estructura burocrática.

El tratamiento internacional de datos exige todavía más prudencia

El artículo 19 de la Ley 7.593/2025 incorpora un régimen de transferencias internacionales inspirado claramente en la lógica europea. Se parte de la existencia de niveles adecuados de protección y se admiten después garantías contractuales, normas corporativas y otras excepciones. (bacn.gov.py)

Para Paraguay ésta es una cuestión particularmente delicada. La economía paraguaya depende de servicios tecnológicos extranjeros: almacenamiento en la nube, correo electrónico, software contable, CRM, pagos, marketing, inteligencia artificial y plataformas empresariales. Muchos de estos servicios implican necesariamente movimientos internacionales de información. Convertir cada flujo de datos en una cuestión jurídica compleja supone encarecer la digitalización de toda la economía.

La Unión Europea ha utilizado el enorme tamaño de su mercado para proyectar su modelo regulatorio hacia terceros países. Pero que Bruselas tenga capacidad para imponer internacionalmente sus preferencias no significa que esas preferencias sean económicamente correctas. El llamado "*Brussels effect*" puede demostrar poder regulatorio; no demuestra eficiencia.

Paraguay debería hacer exactamente lo contrario: mantener un sistema flexible, abierto y compatible con la tecnología internacional, sin que la adecuación al modelo europeo llegue a ser un objetivo.

La adecuación europea no debería ser un objetivo a cualquier precio

La Comisión Europea puede reconocer que un tercer país ofrece un nivel de protección adecuado conforme al RGPD. Paraguay no dispone actualmente de esa consideración. (commission.europa.eu)

Obtenerla puede tener ventajas para algunas empresas paraguayas que procesen datos de clientes europeos. Pero la falta de adecuación no impide esas transferencias. El sistema europeo admite cláusulas contractuales tipo, normas corporativas vinculantes y otros mecanismos jurídicos.

La cuestión económica consiste por tanto en comparar dos costes. Sin adecuación, las empresas paraguayas que realmente necesiten tratar datos europeos deberán asumir determinadas formalidades contractuales. Con adecuación obtenida al precio de reproducir íntegramente el modelo europeo, todas las empresas paraguayas soportarían permanentemente un aparato regulatorio más costoso, aunque nunca trataran un solo dato procedente de Europa.

La segunda opción puede resultar mucho peor: Desde una perspectiva de análisis económico del derecho, sería perfectamente racional que Paraguay aceptase el coste adicional que soporten determinados exportadores de servicios en sus relaciones con clientes europeos si la alternativa consiste en imponer a toda la economía los costes de un sistema semejante al RGPD.

La adecuación no debería convertirse en un símbolo de modernidad. No existe ninguna razón para considerar mejor una regulación simplemente porque la Comisión Europea la declare equivalente a la suya. El criterio debería ser otro: cuánto protege, cuánto cuesta y qué efectos produce sobre inversión, competencia, innovación y productividad.

Una regulación mala no se vuelve buena porque la economía sea rica. Este punto merece subrayarse porque suele aparecer implícitamente en muchos debates regulatorios. No debe pensarse que Europa puede permitirse una regulación ineficiente mientras Paraguay no puede, pues Europa tampoco puede permitírsela sin coste.

Una regulación mala destruye valor en Alemania exactamente igual que en Paraguay. Reduce productividad, aumenta costes de entrada, favorece a las grandes empresas frente a las pequeñas y desvía recursos hacia actividades de compliance. La diferencia está únicamente en la magnitud relativa del daño.

En Europa, una multinacional puede absorber un departamento de protección de datos y continuar operando. Una startup puede tener más dificultades, y precisamente por eso parte de la evidencia empírica muestra efectos especialmente negativos sobre empresas jóvenes. En Paraguay, donde las empresas son en promedio menores y el capital más escaso, esos mismos costes pueden impedir directamente que una actividad se inicie o se formalice.

Copiar una regulación europea ineficiente no produciría entonces "*protección europea con costes paraguayos*". Produciría los mismos defectos del modelo europeo agravados por las características estructurales de Paraguay.

Cómo debería reglamentarse la ley

La solución no requiere reglamentar la Ley 7.593/2025. con una filosofía diferente de la europea.

Las pequeñas empresas que realicen tratamientos ordinarios deberían disponer de modelos oficiales simples y *safe harbours*. Si utilizan procedimientos básicos de seguridad, información y contratación debería existir una fuerte presunción de cumplimiento.

Las evaluaciones de impacto, oficiales especializados y obligaciones documentales complejas deberían reservarse a tratamientos de gran escala, datos sensibles o riesgos significativos.

Las transferencias internacionales ordinarias vinculadas al uso de servicios tecnológicos deberían ser lo más sencillas posible.

Las sanciones deberían concentrarse en fraude, venta ilegal de información, negligencia grave, filtraciones relevantes y verdaderos abusos, no en errores documentales de escasa importancia.

La autoridad de protección de datos debería medir su éxito por la disminución de daños reales, no por la cantidad de expedientes administrativos, sanciones o nuevas obligaciones que produzca.

Éste es probablemente el aspecto más importante. Toda autoridad reguladora desarrolla con el tiempo incentivos para ampliar su ámbito de actuación. Si Paraguay no introduce desde el principio límites claros, existe el riesgo de que una ley inicialmente razonable evolucione gradualmente hacia el mismo tipo de sistema hiperregulado que hoy existe en Europa.

Conclusión

Paraguay necesitaba actualizar su normativa de protección de datos. Una economía digital no puede funcionar correctamente si las personas carecen de protección frente a fraude, utilización irresponsable de información sensible, filtraciones graves o uso ilícito de sus datos.

Pero proteger esos intereses no exige reproducir el RGPD. La experiencia europea demuestra que un sistema construido sobre definiciones extremadamente amplias, obligaciones generalizadas y documentación permanente puede terminar creando costes superiores a sus beneficios marginales. Europa ya soporta esos costes en forma de menor inversión, menos innovación, mayores barreras de entrada y una gigantesca industria de cumplimiento. No son costes aceptables simplemente porque Europa sea más rica, pero en Paraguay serían todavía peores.

Una economía pequeña, abierta y necesitada de capital debería proteger con intensidad aquello que realmente puede causar daño y dejar el resto de las relaciones económicas sometido a reglas sencillas.

Si para obtener una futura decisión europea de adecuación Paraguay tuviera que adoptar una parte sustancial de la maquinaria burocrática del RGPD, no debería hacerlo. Las empresas que necesiten transferir datos desde Europa pueden utilizar mecanismos contractuales. No tiene sentido imponer permanentemente esos costes a todo el tejido empresarial paraguayo para facilitar las operaciones de una minoría.

La regulación correcta no es la que más se parece a la europea; es la que consigue proteger eficazmente la privacidad con el menor coste económico posible.

Paraguay todavía está a tiempo de construir ese modelo. Debería aprovechar la oportunidad y evitar convertirse, en materia de protección de datos, en una pequeña Bruselas.

Fuentes

- República del Paraguay, Ley n.º 7.593/2025 de Protección de Datos Personales. Biblioteca y Archivo Central del Congreso Nacional. (bacn.gov.py)
- MITIC, información institucional sobre la Ley de Protección de Datos Personales. (mitic.gov.py)
- Comisión Europea, *Second Report on the Application of the General Data Protection Regulation*, 2024. (eur-lex.europa.eu)
- Comisión Europea, régimen de decisiones de adecuación y transferencias internacionales de datos. (commission.europa.eu)
- NBER, Janßen, Kesler, Kummer y Waldfogel, *GDPR and the Lost Generation of Innovative Apps*. (nber.org)
- NBER, Jia, Leccese y Wagman, *How Does Privacy Regulation Affect Transatlantic Venture Investment? Evidence from GDPR*. (nber.org)

- NBER, Demirer, Jiménez Hernández, Li y Peng, *Data, Privacy Laws and Firm Production: Evidence from the GDPR*. (nber.org)

Agosto de 2026