Función de independencia y objetividad: el verdadero desafío del Delegado de Protección de Datos

Por José Lagos, Docente UEjecutivos Facultad de Economía y Negocios Universidad de Chile.

La entrada en vigor de nuevas regulaciones sobre protección de datos está obligando a las empresas a replantear sus estructuras de cumplimiento y gobierno corporativo. En ese escenario, la figura del Delegado de Protección de Datos (DPO) dejó de ser un rol técnico o meramente legal para transformarse en un actor estratégico dentro de las organizaciones. Sin embargo, junto con el crecimiento de su relevancia aparece una discusión cada vez más importante: ¿qué necesita realmente un DPO para cumplir adecuadamente su función, independencia u objetividad? Aunque ambos conceptos suelen tratarse como equivalentes, representan dimensiones distintas del rol. La independencia ha sido históricamente el foco principal de las regulaciones modernas. El Reglamento General de Protección de Datos (GDPR europeo), por ejemplo, establece que el DPO debe actuar sin recibir instrucciones sobre cómo ejercer sus funciones, reportar a los niveles más altos de la organización y mantenerse libre de conflictos de interés. La lógica detrás de esa exigencia es clara: un supervisor subordinado, quien toma decisiones sobre el tratamiento de datos difícilmente podrá fiscalizarlo con verdadera libertad. Por eso, muchas empresas se concentran en resolver aspectos estructurales, tales como dónde reporta el DPO, qué jerarquía tiene o qué nivel de autonomía formal posee dentro de la organización. Pero ahí surge una pregunta incómoda: ¿basta realmente con la independencia? La experiencia demuestra que no. Un DPO puede contar con autonomía formal y aun así transformarse en una figura complaciente, incapaz de cuestionar decisiones estratégicas o comerciales, cuando los riesgos regulatorios o reputacionales lo requieren. Es en este punto donde aparece la objetividad, probablemente el atributo más crítico y menos visible del rol. La objetividad no depende del organigrama, sino que del criterio profesional. Implica evaluar riesgos de manera imparcial, emitir recomendaciones incómodas cuando sea necesario y priorizar el cumplimiento y los derechos de las personas por sobre presiones internas o intereses comerciales. La independencia protege al DPO. La objetividad hace lo mismo con el juicio. Y en un contexto donde los datos personales se han convertido en uno de los activos más valiosos para las compañías, esa diferencia se vuelve especialmente relevante. Hoy, las organizaciones utilizan datos para personalizar servicios, entrenar modelos de inteligencia artificial, automatizar decisiones y optimizar estrategias comerciales. Eso significa que el DPO ya no revisa temas marginales, sino que participa indirectamente en decisiones que impactan en el crecimiento, ingresos y competitividad de la organización. Por lo mismo, el verdadero desafío no es únicamente contar con un DPO independiente “en el papel”, sino con uno capaz de mantener la objetividad, incluso cuando sus conclusiones chocan con intereses económicos relevantes. Las empresas más maduras entienden que el rol del DPO no existe para validar decisiones cómodamente, sino precisamente para introducir límites cuando el entusiasmo tecnológico o comercial comienza a superar los márgenes regulatorios o éticos. Porque, al final, las organizaciones no necesitan solo DPOs independientes. También, requieren de profesionales con la capacidad y la convicción de decir “no”, cuando realmente importa.