RES NON VERBA
Revista Científica

RES NON VERBA 16(2)
Octubre 2026
https://doi.org/10.21855/resnonverba.v16i2.1179

ROLES Y RESPONSABILIDADES EN EL TRATAMIENTO DE DATOS PERSONALES EN ECUADOR: ANÁLISIS DESDE EL MODELO EUROPEO

ROLES AND RESPONSIBILITIES IN THE PROCESSING OF PERSONAL DATA IN ECUADOR: AN ANALYSIS BASED ON THE EUROPEAN MODEL

Hilda Daniela Castro Macías, Mgtr.
Universidad Bolivariana del Ecuador
abg.danielacastro.notificaciones@gmail.com
Guayaquil, Ecuador

María Belén Pincay Benalcazar, Abg.
Universidad Católica Santiago de Guayaquil
bplegal7@gmail.com
Guayaquil, Ecuador

Anderson Josue Terán Arellano, Abg.
Universidad de Guayaquil
anderson.terana@ug.edu.ec
Babahoyo, Ecuador

Inghenborth Nicole Loor Sánchez, Mgtr.
Universidad Complutense de Madrid
iloor@ucm.es
Madrid, España

ARTÍCULO DE INVESTIGACIÓN

Recibido: 30/03/2026
Aceptado: 26/10/2026
Publicado: 30/10/2026

RESUMEN

La transformación digital y la protección de datos personales se ha consolidado como un elemento esencial para la garantía de derechos fundamentales, lo que ha impulsado la adopción de marcos regulatorios en distintos ordenamientos jurídicos, incluido Ecuador con la Ley Orgánica de Protección de Datos Personales. Dicha normativa presenta problemas en la delimitación de los roles y funciones de los actores involucrados en el tratamiento de datos, generando ambigüedad en la atribución de responsabilidades jurídicas. Por ello, el presente trabajo analiza la delimitación de roles, funciones y responsabilidad jurídica en el tratamiento de datos personales en Ecuador, a partir de un enfoque comparado con los estándares del modelo europeo. Para el efecto, se emplea una metodología cualitativa basada en el análisis normativo, doctrinario y comparado de la legislación ecuatoriana frente a otros marcos regulatorios. Los resultados evidencian que, si bien la Ley Orgánica de Protección de Datos Personales reconoce figuras como el responsable, el encargado y el delegado de protección de datos, existen inconsistencias en su delimitación funcional, particularmente en la confusión entre encargado y tercero, la desnaturalización del delegado y las incoherencias en la corresponsabilidad. Tales

deficiencias generan inseguridad jurídica y aumentan el riesgo sancionatorio, por lo que resulta necesario fortalecer la precisión normativa tomando como referencia modelos más desarrollados, a fin de garantizar una protección efectiva de los datos personales.

Palabras Clave: *protección de datos personales, roles, responsabilidad jurídica, gobernanza de datos, transformación digital*

ABSTRACT

Digital transformation and personal data protection have become essential to the safeguarding of fundamental rights, prompting the adoption of regulatory frameworks in various legal systems, including Ecuador through the Organic Law on Personal Data Protection. However, this legislation presents challenges in defining the roles and functions of the actors involved in data processing, resulting in ambiguity in the allocation of legal responsibilities. Accordingly, this study analyzes the delineation of roles, functions, and legal liability in personal data processing in Ecuador through a comparative approach based on European regulatory standards. A qualitative methodology is employed, relying on normative, doctrinal, and comparative analysis of Ecuadorian legislation in relation to other regulatory frameworks. The findings reveal that, although the Organic Law on Personal Data Protection recognizes figures such as the controller, processor, and data protection officer, inconsistencies remain in their functional delineation, particularly regarding the distinction between processors and third parties, the role of the data protection officer, and joint controllership. These shortcomings generate legal uncertainty and increase the risk of sanctions. Therefore, greater regulatory precision is necessary, drawing on comparative legal frameworks to strengthen the effective protection of personal data.

Keywords: *personal data protection, roles, legal responsibility, data governance, digital transformation*

INTRODUCCIÓN

Regular el tratamiento de datos personales exige, además de reconocer el derecho a la privacidad, identificar a quienes intervienen y las obligaciones de cada uno. Esta tarea es especialmente relevante en entornos digitales, donde varias entidades pueden participar en una misma operación con funciones distintas. La delimitación de los roles jurídicos no es, por tanto, una cuestión meramente terminológica: permite atribuir responsabilidades y garantizar el cumplimiento normativo.

En la Unión Europea, el Reglamento General de Protección de Datos (RGPD), aprobado mediante el Reglamento (UE) 2016/679, delimita las funciones de los sujetos que participan en el tratamiento de datos personales. Las obligaciones se atribuyen según su posición y las decisiones que adoptan sobre los fines y medios del tratamiento. Este enfoque ha influido en otros ordenamientos, aunque su incorporación a las legislaciones nacionales no elimina las dificultades interpretativas de su aplicación práctica (Barreno, 2025).

La Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador reconoce, entre otras figuras, al responsable, al encargado y al delegado de protección de datos. Este reconocimiento no resuelve todas las cuestiones sobre sus funciones. Es preciso examinar si la normativa distingue claramente las obligaciones de quienes deciden sobre el tratamiento, de quienes actúan por cuenta de otro y de los terceros que acceden a los datos. La literatura sobre la legislación ecuatoriana también aborda esta problemática (Morales et al., 2024).

La dificultad central radica en las consecuencias jurídicas de una delimitación imprecisa. Si la función de cada interviniente no está clara, resulta difícil determinar sus obligaciones y atribuir un eventual incumplimiento. El problema trasciende la interpretación de conceptos legales y afecta a la seguridad jurídica y al régimen de responsabilidad. La comparación con el modelo europeo permite identificar criterios normativos y funcionales útiles para distinguir los roles y analizar el marco ecuatoriano.

La investigación plantea la siguiente pregunta: ¿en qué medida la indeterminación de los roles y funciones en la LOPDP afecta a la atribución de responsabilidades y cómo se compara con los estándares europeos? Su objetivo principal es analizar críticamente la delimitación de roles, funciones y responsabilidad jurídica en el tratamiento de datos personales en Ecuador mediante un estudio comparado.

La relevancia del estudio reside en identificar los puntos en los que la regulación ecuatoriana puede generar dificultades para asignar obligaciones y responsabilidades. El análisis comparado permite valorar estas dificultades a la luz de otro marco normativo y examinar posibles criterios para mejorar la coherencia de la regulación nacional. No se trata de trasladar automáticamente las soluciones europeas al ordenamiento ecuatoriano, sino de determinar qué elementos de ese modelo pueden resultar útiles para evaluar la precisión normativa y la eficacia de la protección de datos personales en Ecuador.

METODOLOGÍA

La investigación se desarrolló desde un enfoque jurídico cualitativo, mediante un diseño documental y comparado. El análisis se centró en la delimitación de los roles, las funciones y las responsabilidades de los sujetos que intervienen en el tratamiento de datos personales en Ecuador. Para ello, se examinó la LOPDP, su normativa de desarrollo y el RGPD de la Unión Europea. El marco jurídico español se incorporó como referencia complementaria para el estudio comparativo. El material analizado estuvo integrado por 27 fuentes jurídicas y doctrinales, localizadas mediante búsquedas en bases de datos, repositorios académicos y fuentes normativas especializadas. La búsqueda se inició el 15 de enero de 2025 y abarcó publicaciones comprendidas entre 2015 y 2026. Para localizar la documentación se utilizaron los operadores booleanos AND y OR, combinados con términos relacionados con el objeto de estudio, entre ellos protección de datos personales, responsabilidad jurídica, Ecuador, controller, processor, Data Protection Officer, comparative law y accountability.

La selección de las fuentes atendió a su relación directa con la delimitación funcional de los sujetos que participan en el tratamiento de datos personales y con la atribución de responsabilidades jurídicas. Se descartaron los documentos duplicados, aquellos cuya información no pudo verificarse y los que carecían de relevancia para el objeto de investigación. Asimismo, se comparó el marco ecuatoriano con el modelo europeo para identificar coincidencias, diferencias y problemas de coherencia normativa en la distribución de funciones y responsabilidades.

Para examinar la delimitación funcional y la atribución de responsabilidades en el tratamiento de datos personales, se establecieron categorías de análisis vinculadas a los principales sujetos, obligaciones e instituciones del régimen de protección de datos. Estas categorías permitieron comparar el marco ecuatoriano con el modelo europeo e identificar las principales dificultades normativas y funcionales.

Tabla 1

Categorías y procedimiento de análisis documental

Categoría de análisis	Aspecto examinado	Finalidad dentro de la investigación
Responsable del tratamiento	Poder de decisión sobre los fines y medios del tratamiento.	Determinar los criterios para identificar al responsable y atribuirle obligaciones jurídicas.
Encargado del tratamiento	Tratamiento realizado por cuenta del responsable y bajo sus instrucciones.	Examinar sus funciones y distinguirlas de las propias del responsable.
Tercero	Intervención de sujetos distintos del responsable, del encargado y del titular.	Identificar posibles confusiones entre la figura del tercero y la del encargado.
Delegado de protección de datos	Funciones de asesoramiento, supervisión y cooperación con la autoridad de control.	Analizar la naturaleza y los límites de sus funciones.
Corresponsabilidad	Participación conjunta en la determinación de los fines y medios del tratamiento.	Examinar los criterios para distribuir las responsabilidades entre varios sujetos.
Responsabilidad proactiva	Cumplimiento demostrable de las obligaciones de protección de datos.	Valorar el alcance de los deberes preventivos y de cumplimiento.
Evaluación de impacto	Identificación y valoración de riesgos derivados del tratamiento.	Analizar la articulación de la evaluación de impacto en el sistema ecuatoriano.
Registro de actividades de tratamiento	Documentación de las operaciones y responsabilidades vinculadas al tratamiento.	Examinar su utilidad para acreditar el cumplimiento normativo.
Bases de licitud	Fundamento jurídico que legitima el tratamiento de datos personales.	Identificar su relación con la atribución de obligaciones y responsabilidades.

RESULTADOS

Roles en el tratamiento de datos personales

El sistema de protección de datos personales en el Ecuador recoge su base normativa a partir de la LOPDP y su reglamento; no obstante, parte de esta estructura se construye de forma progresiva en el tiempo mediante los pronunciamientos y directrices que la Superintendencia de Protección de Datos Personales incorpora a través de sus resoluciones y absoluciones de consulta.

El artículo 5 de la LOPDP, identifica a los integrantes del sistema de protección de datos personales: (i) Titular; (ii) Responsable del tratamiento; (iii) Encargado del tratamiento; (iv) Destinatario; (v) Autoridad de Protección de Datos Personales; y, (vi) Delegado de Protección de Datos Personales. Dicha categorización constituye el punto de partida para distribuir obligaciones, imputar responsabilidades y contiene las pautas para la operatividad del régimen de protección de datos.

Es fundamental definir conceptualmente cada rol. Como primer punto, el titular constituye el eje central del sistema de protección de datos personales, en tanto se configura como la persona natural a quien corresponde la propiedad de los datos personales que serán objeto de tratamiento, siendo además el sujeto sobre el cual recae el derecho a la autodeterminación informativa.

Otro rol es el del responsable del tratamiento, quien, como sujeto obligado, debe cumplir con las obligaciones de la ley en esta materia y asegurar la protección de los derechos de los titulares. Como siguiente rol a definir, está el encargado del tratamiento, que es la persona natural o jurídica, u otro organismo que trate datos personales por cuenta del responsable del tratamiento, de modo que la base que legitima la actuación del encargado es el mandato conferido por el responsable.

Por consiguiente, el destinatario es una persona natural o jurídica al que se comunican o divulgan datos personales del titular a través del responsable (De Alba Bastarrechea, 2023). En el mismo sentido, la autoridad de Protección de Datos Personales es definida claramente por la ley en esta materia, es una autoridad de carácter público independiente con el fin de supervisar la aplicación de la ley, reglamento y resoluciones que ella dicte, con el objetivo de proteger los derechos y libertades fundamentales de personas naturales en cuanto al tratamiento de sus datos personales (Asamblea Nacional del Ecuador, 2021, art. 4).

Posteriormente, está la figura del Delegado de Protección de Datos Personales, misma que consiste en una figura creada para facilitar el cumplimiento de las obligaciones en materia de protección de datos, rendir cuentas y actuar como intermediario entre las organizaciones, los titulares de los datos y las autoridades de control (Becerra, 2025, p. 118).

Ambigüedad conceptual y estructural de las figuras de encargado y tercero

En este orden de ideas, se aprecia una delimitación conceptual deficiente entre las figuras de encargado y tercero, particularmente en los artículos 34 y 35 de la LOPDP.

El artículo 34 de la antedicha Ley regula el acceso a datos personales por parte del encargado del tratamiento, señalando que no constituye transferencia cuando este accede a los datos para prestar un servicio al responsable, mismo servicio que debe estar formalizado mediante contrato, limitado a las instrucciones del responsable, y que al finalizar el servicio los datos deben ser devueltos o destruidos, por tanto, el encargado responde por cualquier incumplimiento de estas condiciones.

El artículo 35 de la LOPDP regula el acceso a datos personales por parte de terceros, indicando igualmente que no se considera transferencia si el acceso es necesario para prestar un servicio al responsable y se realiza legítimamente. Exige también un contrato que delimite el tratamiento conforme a las instrucciones del responsable, prohíba su uso para fines distintos y establezca la obligación de devolver o destruir los datos al finalizar el servicio. El tercero asume la responsabilidad por las infracciones derivadas del incumplimiento.

Los artículos 34 y 35 de la LOPDP regulan supuestos distintos de acceso a datos personales: el artículo 34 se refiere al encargado del tratamiento, mientras que el artículo 35 contempla el acceso por parte de terceros. Sin embargo, la redacción del artículo 35 puede generar dudas interpretativas, ya que exige regular contractualmente el acceso e incorpora condiciones como la obligación de seguir las instrucciones del responsable y la prohibición de utilizar los datos para fines diferentes de los previstos en el contrato. Estas condiciones son propias de la relación entre ambas figuras, pues no todo tercero que accede a datos personales actúa necesariamente como encargado del tratamiento.

No obstante, el mismo artículo 35 dispone que dicho instrumento debe establecer, de forma clara y precisa, que el encargado del tratamiento actuará exclusivamente conforme a las instrucciones impartidas por el responsable del tratamiento, sin que le esté permitido destinar los datos a finalidades distintas de las expresamente previstas en el contrato.

La redacción de esta disposición plantea dudas sobre la distinción entre el tercero y el encargado del tratamiento. Por una parte, contempla el acceso de terceros a los datos personales bajo determinadas condiciones de legitimidad; por otra, vincula ese acceso a una relación contractual con el responsable. El problema surge cuando las condiciones previstas para regular dicha relación incorporan elementos propios del encargo del tratamiento, lo que dificulta establecer con claridad el alcance de cada figura.

Esta dificultad no implica que ambas categorías sean equivalentes, sino que la forma en que se regula la intervención de terceros puede favorecer una interpretación que las aproxime

indebidamente. La existencia de un vínculo contractual con el responsable no basta, por sí sola, para determinar que un sujeto actúa como encargado del tratamiento. Para distinguir ambas figuras, resulta necesario atender a la función que desempeña cada interviniente y a las condiciones bajo las cuales accede a tratar los datos personales. De ahí que la regulación deba permitir identificar con suficiente precisión las obligaciones correspondientes a cada uno, evitando que la categoría de tercero quede confundida con la de encargado.

Funciones: desnaturalización del Delegado de Protección de Datos

En virtud de las funciones de los demás roles dentro del tratamiento, se debe realizar el examen de las funciones del delegado de protección de datos personales (en adelante, DPD), las cuales implican definir el alcance del entorno del responsable y elaborar un mapa de las actividades de tratamiento de datos de la organización. En particular, Mendoza (2025) manifiesta que:

> En términos generales, solemos denominar un mapeo de datos por tratamientos de datos, que consiste en identificar todas y cada una de las operaciones de tratamiento de datos. Para llegar a esto, primero se requiere un conocimiento completo de la distribución interna, conociendo el organigrama y también la asignación de roles y las responsabilidades relacionadas con el tratamiento de datos, así como los enlaces y acuerdos externos con otras organizaciones y el marco legal aplicable. (p. 253)

La respuesta frente a la definición de responsabilidades comprende, según Martínez (2025), informar y asesorar al responsable y/o encargado del tratamiento sobre sus obligaciones y responsabilidades con relación a las brechas de datos personales, y también cooperar con la Autoridad de Control en las cuestiones relativas a la gestión de la brecha de datos personales.

Primero hay que señalar que los artículos 48 y 49 de la LOPDP, regulan la designación y las funciones del DPD. En cuanto a su designación, esta es obligatoria en los siguientes supuestos: (i) cuando el tratamiento de datos sea realizado por entidades del sector público; (ii) cuando las actividades del responsable o encargado impliquen un control permanente y sistemático por su volumen, naturaleza, alcance o finalidades; (iii) cuando se trate a gran escala categorías especiales de datos; y (iv) cuando el tratamiento no esté relacionado con información reservada o secreta vinculada a la seguridad nacional y defensa del Estado.

A su vez, el delegado de protección de datos personales tiene las siguientes funciones: (i) asesorar al responsable, a su personal y al encargado del tratamiento sobre el cumplimiento de la normativa aplicable; (ii) supervisar el cumplimiento de la ley, el reglamento y demás

disposiciones emitidas por la autoridad competente; (iii) asesorar y supervisar los análisis de riesgo, evaluaciones de impacto y medidas de seguridad; (iv) actuar como punto de contacto y cooperar con la Autoridad de Protección de Datos Personales. En cuanto a la responsabilidad jurídica, como se mencionó anteriormente que este responderá administrativa, civil y penalmente en caso de incumplimiento de sus funciones.

Luego de las definiciones alcanzadas, desde una perspectiva normativa, el DPD está concebido como un órgano técnico e independiente cuya función principal es actuar como nexo entre la autoridad de control y el responsable del tratamiento, limitándose a asesorar sobre el cumplimiento de la normativa, supervisar su observancia y, de ser necesario, reportar incumplimientos a la autoridad competente cuando sus recomendaciones no sean atendidas.

En este apartado corresponde interpretar que en la práctica esta disposición se ve distorsionada, toda vez que la débil cultura de cumplimiento y las limitaciones presupuestarias provocan que el DPD asuma un rol operativo que excede sus funciones atribuidas por la ley, convirtiéndose en un todólogo encargado no solo de supervisar, sino de diseñar, implementar y sostener el sistema integral de protección de datos.

De este modo, pierde su carácter independiente y pasa a ser un asesor interno orientado en vez de un supervisor, por este motivo no hay que confundir al responsable con el DPO, dado que supone un reforzamiento de aquél (Sierra, 2018, p. 245).

En lo que respecta a la tendencia de designar personal interno, ya sea por restricciones económicas o por la necesidad de conocimiento previo de la estructura organizacional y los flujos de datos, se incrementa la problemática identificada, y consecuentemente esta situación se agrava debido a la presión institucional por garantizar servicios eficientes, lo que empeora aún más el cumplimiento estricto de la normativa. Y en función de esta asimilación se debe considerar que la contratación de un DPD externo, si bien podría fortalecer la independencia del rol, suele ser descartada por implicar mayores tiempos de diagnóstico, gastos, levantamiento de información y evaluación de riesgos.

De toda esta argumentación se puede construir una conclusión de que existe una clara desnaturalización del rol del DPD, pues mientras la norma lo determina como un agente de control y supervisión independiente, en la práctica se le impone la carga de construir y ejecutar el sistema de cumplimiento desde cero, comprometiendo su objetividad y eficacia como mecanismo de garantía dentro del régimen de protección de datos personales.

Contradicciones normativas en la responsabilidad de corresponsables

El tratamiento de la figura del responsable conjunto presenta vacíos e inconsistencias relevantes tanto en la LOPDP como en su reglamento. Si bien se reconoce la corresponsabilidad en la determinación conjunta de fines y medios del tratamiento, no se desarrollan adecuadamente los elementos mínimos de los acuerdos entre corresponsables ni los criterios de distribución de responsabilidades.

Particularmente, el artículo 37 del Reglamento introduce una contradicción al establecer simultáneamente la responsabilidad solidaria frente a la autoridad y los titulares, y la responsabilidad individual basada en el acuerdo interno. En concreto, el artículo señala:

> Art. 37.- Responsables conjuntos.- **Si dos o más responsables del tratamiento determinan conjuntamente los mismos fines y los medios del tratamiento de los datos personales, se considerarán responsables conjuntos,** quienes definirán sus respectivas tareas y responsabilidades en materia de protección de datos de forma transparente a través de un contrato, en la medida en que estas no estén ya definidas en disposiciones legales, buscando precautelar los intereses y derechos de los titulares. (...) **En este sentido, cada responsable conjunto es sujeto del régimen sancionador, en forma diferenciada sobre la base de las responsabilidades adquiridas**…". Énfasis propio.

El punto de partida de la atribución de responsabilidad en los supuestos de corresponsabilidad no puede ser entendida de manera indiscriminada, pues ello desconoce el principio de imputación individual, en coherencia aunque los responsables conjuntos determinen fines y medios del tratamiento, sus funciones y obligaciones pueden encontrarse claramente delimitadas mediante acuerdo, por lo que la responsabilidad debe recaer únicamente sobre quien incurre en el incumplimiento dentro de su ámbito de actuación (Sempere Samaniego, 2025).

En lo que se refiere a esta dualidad identificada, en definitiva, supone inseguridad jurídica en la imputación de responsabilidades, riesgo de sanciones desproporcionadas e incertidumbre sobre el alcance real de los acuerdos entre corresponsables.

En esta idea está implícita la viabilidad de plantear una propuesta de reforma que sancione según las responsabilidades incumplidas de cada corresponsable, en otras palabras, que la responsabilidad y el régimen sancionador se determinen de manera individualizada, en función del grado de participación y del incumplimiento específico de las obligaciones asumidas por cada responsable conjunto, conforme al acuerdo celebrado y a la normativa aplicable.

Responsabilidad jurídica en protección de datos

Con lo señalado en líneas anteriores, quedan identificadas las funciones que tiene cada rol en el procedimiento de tratamiento de datos personales conforme a la normativa. De forma consecuente, en caso de que exista incumplimiento de dichas funciones, se establece la responsabilidad jurídica en cada caso respectivamente.

Al referirnos a responsabilidad jurídica, se asemeja a un acto jurídico producto del ejercicio de una potestad, es decir, es un “acto coactivo llevado a cabo por una persona con potestad y competencia para ejecutarlo contra otra, que consiste en la privación parcial o total, temporal o definitiva, de uno o más de sus bienes jurídicos, por la realización de un acto calificado como ilícito” (Vélez, 2015, p. 137).

Con esa definición concretada, la responsabilidad de cada rol en el procedimiento de tratamiento de datos personales provocada por incumplimiento de las funciones señaladas en la ley se determina de forma gradual e independiente. Por un lado, cuando existe incumplimiento de funciones del delegado, éste responde de manera administrativa, civil y penal, de conformidad con la LOPDP, en su artículo 49. Adicionalmente, cuando existe incumplimiento de funciones del encargado y/o responsable, estos tendrán las mismas responsabilidades al tenor del artículo 47 de la Ley previamente mencionada.

Particularmente, el artículo 52 de la Ley citada en párrafos anteriores, señala que los responsables y encargados pueden adherirse a códigos de conducta, certificaciones, sellos y marcas de protección para salvaguardar significativamente el cumplimiento de sus funciones, pero que adherirse a estos códigos no exime la responsabilidad de cumplir con las disposiciones de la LOPDP.

En tal sentido, producto de estos incumplimientos se configuran las infracciones, mismas que se clasifican como leves o graves. En cuanto a las sanciones, se dividen de la siguiente forma, para las sanciones de infracciones leves, el artículo 71 establece que se aplicará una multa de entre el 0,1 % y el 0,7 % calculada sobre el volumen de negocio del ejercicio económico anterior a la fecha de imposición de la multa.

Los porcentajes establecidos del 0,1 % y el 0,7 % se aplicarán bajo el principio de proporcionalidad, donde se establecen los parámetros de: (i) intencionalidad, (ii) si se ha cometido anteriormente la misma conducta; y (iii) las consecuencias lesivas provocadas.

Para las sanciones por infracciones graves se aplicará una multa de entre el 0,7 % y el 1 % calculada sobre su volumen de negocios, en donde también se establecerá el principio de

proporcionalidad como criterio rector para la imposición de multas, y con ello los mismos parámetros de las infracciones leves: (i) intencionalidad, (ii) si se ha cometido anteriormente la misma conducta; y (iii) las consecuencias lesivas provocadas.

De la revisión efectuada de la norma, la responsabilidad jurídica en materia de protección de datos personales garantiza el cumplimiento efectivo de las obligaciones previstas en dicha norma, atribuyéndolas de manera diferenciada y proporcional a cada uno de los roles que intervienen en el tratamiento de datos. Consecuentemente, tanto el delegado como el responsable y el encargado responden por el incumplimiento de sus funciones en los ámbitos administrativo, civil y penal, sin que la adopción de mecanismos voluntarios como códigos de conducta o certificaciones los exima de dicha responsabilidad.

En este contexto, el régimen sancionatorio basado en la clasificación de infracciones leves y graves y en la aplicación del principio de proporcionalidad para la imposición de dichas multas, mantiene un eje sancionador, pero a la vez preventivo de vulneraciones a los derechos de los titulares de datos personales.

Derecho comparado: delimitación funcional entre responsable y encargado en el modelo europeo

En el régimen ecuatoriano de protección de datos personales, una de las cuestiones que merece atención es la delimitación de las funciones de los sujetos que intervienen en el tratamiento. Aunque la normativa reconoce las figuras del responsable y del encargado, la regulación del acceso a los datos por parte de terceros plantea dudas sobre la distinción entre estas categorías. Esta cuestión resulta relevante porque la identificación de cada sujeto condiciona la determinación de las obligaciones que le corresponden y de las responsabilidades que pueden derivarse de su actuación.

El RGPD de la Unión Europea ofrece un marco de referencia para examinar esta cuestión. Su regulación distingue entre el responsable del tratamiento y el encargado atendiendo a las funciones que desempeñan. El responsable determina los fines y los medios del tratamiento, mientras que el encargado trata los datos personales por cuenta del responsable. Por tanto, la diferencia entre ambas figuras se establece a partir de su intervención en el tratamiento y se concreta en las obligaciones previstas para cada una (Agencia Española de Protección de Datos, 2018).

Esta distinción también se refleja en el régimen de obligaciones del RGPD. El artículo 5.2 establece que el responsable debe cumplir los principios aplicables al tratamiento y poder

demostrar dicho cumplimiento. El artículo 28 regula las obligaciones del encargado y las condiciones que deben establecerse para el tratamiento realizado por cuenta del responsable; por tanto, ambos sujetos tienen obligaciones diferenciadas, cuya aplicación depende de las funciones que desempeñan y de las disposiciones que les resulten aplicables (Parlamento Europeo y Consejo de la Unión Europea, 2016).

En la normativa ecuatoriana, el artículo 35 de la LOPDP plantea una cuestión específica respecto del acceso a los datos por parte de terceros. La disposición contempla condiciones contractuales y hace referencia a instrucciones del responsable, elementos que también aparecen en la regulación de la relación entre responsable y encargado. Esta coincidencia puede dificultar la interpretación de ambas figuras y plantea la necesidad de determinar si la regulación permite distinguirlas con suficiente claridad (Serrano, 2019, p. 13).

La delimitación de estas categorías tiene consecuencias prácticas. Si no se identifica con precisión la función que desempeña cada sujeto, pueden surgir dificultades para determinar las obligaciones que le corresponden y atribuir las responsabilidades derivadas de un tratamiento concreto. Por ello, el análisis debe tender a la intervención efectiva de cada actor y al régimen jurídico aplicable, evitando atribuir automáticamente a un tercero las obligaciones propias del encargado o considerar que todas las obligaciones recaen exclusivamente sobre el responsable (Parlamento Europeo y Consejo de la Unión Europea, 2016).

El RGPD incorpora, además, instrumentos que contribuyen a concretar las funciones y obligaciones de los sujetos implicados. El artículo 28 exige que el tratamiento realizado por un encargado se regule mediante un contrato u otro acto jurídico vinculante que establezca, entre otros aspectos, el objeto y la duración del tratamiento, su naturaleza y finalidad, los tipos de datos y las obligaciones de las partes. Respecto al artículo 26 y los supuestos de corresponsabilidad y exigencia hacia los corresponsables, para que determinen de manera transparente sus respectivas obligaciones. Estas disposiciones permiten observar como el modelo europeo aborda la distribución de funciones y responsabilidades mediante reglas específicas (Parlamento Europeo y Consejo de la Unión Europea, 2016).

La comparación deja ver por qué es importante que la normativa ecuatoriana defina con claridad las funciones de quienes intervienen en el tratamiento de datos personales. El modelo europeo ofrece criterios útiles para examinar esta cuestión, especialmente en lo relativo a la distinción entre responsable y encargado y a la regulación de sus obligaciones. Con base en este contraste, corresponde ahora revisar si la regulación ecuatoriana permite identificar de forma

adecuada qué función cumple cada sujeto y atribuirle las responsabilidades que le corresponden (Carrillo, 2021, p. 187).

El principio de *accountability* y su impacto en la delimitación de responsabilidades

El principio de *accountability* o responsabilidad proactiva constituye uno de los elementos relevantes del modelo europeo de protección de datos personales. Recogido en el artículo 5.2 del RGPD, exige que el responsable del tratamiento no solo cumpla los principios establecidos en el Reglamento, sino que también pueda demostrarlo. De este modo, el cumplimiento normativo comprende tanto la observancia de las obligaciones legales como la capacidad de acreditar las medidas adoptadas (Estepa Montero, 2022, p. 72).

Este principio introduce una dimensión preventiva en la gestión de los datos personales. La responsabilidad no se limita a reaccionar ante una infracción, sino que requiere adaptar medidas adecuadas para cumplir las exigencias normativas y poder justificar las decisiones tomadas. A este respecto, la importancia de documentar las actuaciones y gestionar los riesgos asociados al tratamiento, aspectos que permiten evaluar cómo se materializa la responsabilidad proactiva (Kuner et al., 2021).

La aplicación de este principio también permite precisar la relación entre el responsable y el encargado del tratamiento. Al responsable le corresponde garantizar, y estar en condiciones de demostrar, que el tratamiento cumple con el RGPD, mientras que el encargado está sujeto a las obligaciones que le corresponden conforme al Reglamento y a las instrucciones documentadas del responsable. La intervención de un encargado no elimina las obligaciones del responsable, aunque tampoco excluye la responsabilidad propia que pueda corresponder al encargado por el incumplimiento de sus deberes legales (Kuner et al., 2021).

La delimitación de responsabilidades también debe considerar los supuestos en los que varios sujetos participan en la determinación de los fines y medios del tratamiento. En estas situaciones, la calificación jurídica de cada interviniente depende de su participación efectiva y de las funciones que desempeña. Por ello, la existencia de varios actores no implica por sí misma que todos tengan las mismas obligaciones, sino que es necesario examinar el papel de cada uno conforme a la normativa aplicable. La referencia jurisprudencial incluida en la versión original deberá verificarse antes de utilizarse para respaldar esta afirmación (Voigt y Bussche, 2024).

Las directrices del Comité Europeo de Protección de Datos ofrecen criterios adicionales para aplicar el principio de responsabilidad proactiva. Entre las medidas relevantes se encuentran la documentación de las actividades de tratamiento, las evaluaciones de impacto cuando sean

exigibles y la adopción de mecanismos adecuados para supervisar el cumplimiento de las obligaciones. Estas herramientas contribuyen a acreditar las actuaciones realizadas y a delimitar las funciones de los sujetos implicados (Comité Europeo de Protección de Datos, 2018).

En Ecuador, la LOPDP también contempla el principio de responsabilidad proactiva y demostrada. Por ello, la comparación con el modelo europeo no debería plantearse como una ausencia absoluta de este principio en la legislación ecuatoriana, sino como un análisis de su desarrollo normativo de las herramientas previstas para hacerlo efectivo. La cuestión consiste en determinar si las obligaciones establecidas permiten documentar el cumplimiento, gestionar los riesgos y diferenciar adecuadamente las responsabilidades de los sujetos que intervienen en el tratamiento.

A tal efecto, es necesario revisar el alcance de las obligaciones previstas en la normativa ecuatoriana en materia de documentación, evaluación de riesgos y supervisión de los encargados. Comparar estas medidas con las del modelo europeo puede ayudar a identificar semejanzas y diferencias en la regulación de estas medidas, pero cualquier conclusión sobre una menor precisión o eficacia del modelo ecuatoriano debe apoyarse en el análisis de las disposiciones correspondientes. La delimitación de responsabilidades no depende únicamente de que la normativa defina las figuras del responsable, el encargado y los terceros. Hace falta, además, que las obligaciones aplicables a cada sujeto permitan identificar sus funciones y determinar cómo debe acreditar el cumplimiento de sus deberes. Desde esta perspectiva, el análisis de responsabilidad proactiva permite valorar en qué medida el marco ecuatoriano ofrece herramientas suficientes para concretar las responsabilidades derivadas del tratamiento de datos personales (Estepa, 2022).

Desarrollo de las medidas de responsabilidad proactiva

La responsabilidad proactiva concreta mediante medidas que permiten identificar los riesgos del tratamiento de datos personales y acreditar el cumplimiento de las obligaciones legales. Entre ellas se encuentran las evaluaciones de impacto relativas a la protección de datos y los registros de actividades de tratamiento, instrumentos que facilitan la documentación de las decisiones adoptadas y el seguimiento de las operaciones realizadas.

Una de estas medidas es la Evaluación de Impacto Relativa a la Protección de Datos (EIPD), regulada en el artículo 35 del RGPD. Su finalidad es identificar y valorar los riesgos que determinadas operaciones de tratamiento pueden generar para los derechos y libertades de las personas, así como establecer medidas para afrontarlos. Su realización es obligatoria cuando el

tratamiento pueda entrañar un alto riesgo, atendiendo a los criterios previstos en el Reglamento. Por tanto, no basta con que una operación utilice tecnologías emergentes o categorías especiales de datos para concluir automáticamente que la evaluación es obligatoria; debe analizarse el tratamiento y el riesgo que comporta (Kuner et at., 2021)

La utilidad de esta herramienta se aprecia también en la práctica española, en la que el RGPD se aplica junto con la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). La evaluación de impacto permite examinar anticipadamente los riesgos de un tratamiento y determinar qué medidas resultan necesarias para proteger los derechos de las personas afectadas. Para mantener el ejemplo de las sanciones impuestas por sistemas de control horario biométricos, será necesario identificar las resoluciones concretas de la Agencia Española de Protección de Datos y comprobar si la infracción sancionada consistió efectivamente en no realizar una evaluación de impacto obligatoria (Agencia Española de Protección de Datos, 2018).

En Ecuador, la evaluación de impacto también está contemplada en el Reglamento General a la Ley Orgánica de Protección de Datos Personales. Sus artículos 29 a 32 regulan su objeto, los supuestos de obligatoriedad y su contenido. Por ello, la comparación entre ambos ordenamientos no debe partir de que esta herramienta está ausente en la normativa ecuatoriana, sino examinar los criterios que determinan cuándo debe realizarse y las condiciones previstas para su aplicación.

Otra medida importante es el registro de actividades de tratamiento, previsto en el artículo 30 del RGPD. Este registro documenta información sobre las operaciones de tratamiento, incluidos sus fines, las categorías de datos y de interesados, los destinatarios, las transferencias internacionales cuando procedan y las medidas de seguridad. Su función no se limita a reunir información, que permite disponer de una descripción organizada de los tratamientos y facilita la comprobación del cumplimento de las obligaciones aplicables. La obligación de mantener estos registros también se extiende a los encargados del tratamiento en los términos establecidos por el artículo 30.2 del RGPD. De forma paralela, el Reglamento ecuatoriano regula esta cuestión en sus artículos 38 y 39 respecto de los responsables y en el artículo 44 respecto de los encargados. Como estas normas fijan las condiciones en las que corresponde llevar el registro, por lo que la comparación debe considerar los requisitos y supuestos previstos en cada ordenamiento, en lugar de asumir que las obligaciones son idénticas.

El responsable tiene la obligación de seleccionar únicamente encargados que ofrezcan garantías suficientes, lo que implica un deber de diligencia previa que forma parte del principio

de responsabilidad proactiva. La jurisprudencia española refuerza este criterio, ha establecido que la condición de responsable del tratamiento “viene delimitada por la efectiva participación en la determinación de los fines y medios del tratamiento” (Tribunal Supremo, 2016c).

Por su parte, la LOPDP ecuatoriana no establece una obligación equivalente con el mismo nivel de precisión, lo que evidencia una debilidad estructural en la documentación sistemática del tratamiento y en la supervisión efectiva de los encargados. En este sentido, el principio de protección de datos desde el diseño y por defecto, regulado en el artículo 25 del RGPD, obliga a integrar medidas de protección de datos desde la fase inicial de diseño de los sistemas y procesos, así como a garantizar que, por defecto, solo se traten los datos estrictamente necesarios. Este enfoque preventivo refuerza la seguridad jurídica y minimiza riesgos desde el origen del tratamiento. En el caso ecuatoriano, este principio no se encuentra desarrollado de forma expresa, lo que refuerza el carácter reactivo del sistema y limita la incorporación de medidas preventivas en la arquitectura organizacional.

Acuerdos de corresponsabilidad y delimitación de responsabilidades

El RGPD regula de manera expresa la figura de la corresponsabilidad en su artículo 26, estableciendo la obligación de que los corresponsables determinen, de forma transparente, sus respectivas responsabilidades mediante un acuerdo. Este acuerdo debe reflejar la esencia de la relación, incluyendo la distribución de obligaciones en materia de cumplimiento de derechos de los interesados, deberes de información, seguridad del tratamiento y comunicación con la autoridad de control. La jurisprudencia ha precisado que la corresponsabilidad no puede presumirse por la mera existencia de vínculos empresariales, sino que requiere una participación efectiva en la determinación de los fines y medios del tratamiento (Tribunal Supremo, 2016b).

El artículo 26 del RGPD exige que los responsables que determinan conjuntamente los fines y medios del tratamiento establezcan, mediante un acuerdo, como se distribuyen sus respectivas obligaciones. Esta distribución debe contemplar la atención de los derechos de los interesados y el cumplimiento del deber de información. Además, los aspectos esenciales del acuerdo deben estar disponibles para las personas afectadas.

En España, el artículo 74, letras h) e i), de la LOPDGDD contempla como infracciones leves determinados incumplimientos relacionados con este acuerdo, entre ellos su falta de formalización, la determinación inexacta de las obligaciones de las partes y la falta de puesta a disposición de sus aspectos esenciales. La regulación muestra que no basta con que exista un

acuerdo, dado que su contenido debe permitir conocer cómo se distribuyen las responsabilidades entre los corresponsables.

Esta cuestión también resulta relevante para el análisis de la normativa ecuatoriana. Cuando varios sujetos intervienen conjuntamente en un tratamiento, es necesario determinar que obligaciones corresponden a cada uno y como se establece esa distribución. Por ello, para concluir que la regulación ecuatoriana presenta una insuficiencia en este ámbito, debe examinarse si sus disposiciones identifican los criterios aplicables y los elementos que permiten atribuir las responsabilidades en cada caso.

Bases de licitud del tratamiento: una comparación necesaria

El artículo 6 del RGPD reconoce seis bases jurídicas que permiten tratar datos personales, tales como, el consentimiento, la necesidad de ejecutar un contrato o adoptar medidas precontractuales, el cumplimiento de una obligación legal, la protección de intereses vitales, el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos y la satisfacción de intereses legítimos del responsable o de un tercero. Cuál de ellas resulta aplicable depende de las circunstancias del tratamiento y de los requisitos previstos para la base jurídica encovada.

El interés legítimo merece especial atención porque exige valorar las circunstancias concretas en las que se realiza el tratamiento. No es suficiente con que el responsable alegue un interés empresarial o comercial. Este debe justificar que ese interés es legítimo, que el tratamiento resulta necesario para satisfacerlo y que no prevalecen los derechos y libertades fundamentales de las personas afectas. Esta valoración debe atender, entre otros elementos, a las expectativas razonables del interesado y a las consecuencias que el tratamiento puede tener para él. Cuando se utiliza esta base jurídica, el responsable también debe cumplir las obligaciones de información y respetar el derecho de oposición en los términos establecidos por el RGPD.

La Sentencia 1620/2020, de 26 de noviembre del Tribunal Supremo español, resulta pertinente para examinar esta cuestión. El asunto se refiere al tratamiento de datos con fines de mercadotecnia directa y a la posibilidad de fundamentarlo en el interés legítimo sin contar con el consentimiento del interesado (Tribunal Supremo, 2020). La resolución permite apreciar que la invocación de esta base no legitima automáticamente el tratamiento, ya que deben cumplirse las condiciones normativas aplicables y justificarse su concurrencia en el caso concreto. La referencia a la STS 1618/2016 debe reservarse para el análisis de la cuestión que efectivamente aborda, relativa a la identificación del responsable o al establecimiento, una vez comprobado su

contenido, y no emplearse como fundamento directo del régimen de licitud del artículo 6 del RGPD (Tribunal Supremo, 2016a).

En Ecuador, la Ley Orgánica de Protección de Datos Personales también establece bases de legitimación para el tratamiento. Por tanto, la comparación no debe plantearse como una oposición entre un ordenamiento que reconoce estas bases y otro que carece de ellas. La cuestión relevante es determinar cómo se articulan sus requisitos y qué criterios permiten valorar su aplicación en situaciones concretas. Para establecer si existe una diferencia sustancial respecto del modelo europeo, es necesario examinar el contenido de las disposiciones ecuatorianas y su desarrollo normativo, en lugar de atribuir de forma general a la regulación nacional una menor sistematicidad o profundidad.

Régimen sancionador: comparación cuantitativa y cualitativa

El régimen sancionador ecuatoriano diferencia las infracciones leves de las graves y establece las multas en función de la naturaleza del infractor. Cuando se trata de responsables, encargados o terceros, ya sean entidades privadas o empresas públicas, las sanciones económicas oscilan entre el 0,01 % y el 0,7 % del volumen de negocio del ejercicio anterior para las infracciones leves, y entre el 0,7 % y el 1 % para las graves. La ley exige que la determinación de la cuantía respete el principio de proporcionalidad y tenga en cuenta factores como la intencionalidad, la reiteración, el perjuicio ocasionado y la reincidencia (Asamblea Nacional del Ecuador, 2021).

El RGPD establece dos niveles máximos de multas administrativas. El primero alcanza los diez millones de euros o, si se trata de una empresa, el 2 % del volumen de negocio total anual global del ejercicio anterior, aplicándose la cuantía mas elevada. El segundo pude llegar a veinte millones de euros o al 4 % de dicho volumen de negocio, también según cuál de las dos cantidades sea superior. La aplicación de estas sanciones depende de la infracción cometida y debe atender a las circunstancias particulares del caso. El propio Reglamento exige que las multas sean efectivas proporcionadas y disuasorias (Parlamento Europeo y Consejo de la Unión Europea, 2016).

En España, la LOPDGDD contempla el marco europeo mediante disposiciones sobre la tipificación de infracciones y el régimen aplicable a determinados responsables y encargados. Su artículo 77 contempla un régimen específico para las entidades que enumera, entre ellas diversas autoridades y organismo públicos, al que se asocian medidas como el apercibimiento y la adopción de actuaciones correctivas, en lugar de la imposición ordinaria de multas administrativas a esas entidades (Ley Orgánica 3/2018).

Derechos de los interesados: alcance y garantías

El RGPD reconoce un conjunto de derechos que permite a los interesados conocer y controlar el uso de sus datos personales. Entre ellos figuran los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad (Parlamento Europeo y Consejo de la Unión Europea, 2016, arts. 15-22). Su ejercicio se acompaña de obligaciones concretas para el responsable del tratamiento, este debe facilitar los medios para presentar las solicitudes, responder dentro de los plazos establecidos e informar, cuando proceda, de los motivos por los que no atiende una petición. Como regla general, el artículo 12.3 del RGPD fija un plazo de un mes para informar sobre las actuaciones realizadas, con posibilidad de ampliación en los supuestos previstos en el propio Reglamento.

En España, la LOPDGDD contempla el marco europeo mediante disposiciones sobre transparencia, información y ejercicio de los derechos. Su artículo 12 establece reglas generales para la presentación y tramitación de las solicitudes, mientras que los artículos siguientes desarrollan aspectos específicos de su ejercicio, por tanto, las garantías aplicables deben analizarse juntamente con el RGPD, puesto que la ley española lo complementa, no sustituye el catálogo de derechos que establece el RGPD.

Desde una perspectiva comparada, la efectividad de estos derechos depende de que las personas puedan conocer como ejercerlos y obtener una respuesta conforme a la normativa aplicable. La existencia de procedimientos accesibles y de obligaciones claramente definida para los responsables contribuye a que los derechos reconocidos por la ley puedan ejercerse en la práctica. La Ley Orgánica de Protección de Datos Personales de Ecuador también reconoce derechos de acceso, rectificación y actualización, eliminación, oposición, portabilidad, suspensión del tratamiento y otros mecanismos de protección. A este respecto, la comparación entre ambos ordenamientos no debe centralizarse en la existencia formal de estos derechos, sino también en los requisitos para ejercerlos, los plazos de respuesta, las obligaciones de los responsables y las vías de reclamación disponibles para los titulares.

DISCUSIÓN

El análisis comparado muestra que la principal dificultad del régimen ecuatoriano no reside en la ausencia de categorías jurídicas, sino en la necesidad de precisar cómo se relacionan las funciones de cada interviniente con las obligaciones que le corresponden. Esta cuestión se aprecia especialmente en los artículos 34 y 35 de la LOPDP, cuya interpretación conjunta exige

distinguir entre la actuación del encargado y el acceso de terceros a los datos (Asamblea Nacional del Ecuador, 2021).

A este respecto, el RGPD ofrece un marco comparativo útil porque vincula la condición de responsable con la determinación de los fines y medios del tratamiento, mientras que atribuye al encargado funciones realizadas por cuenta del responsable. Además, establece obligaciones específicas para los encargados y los corresponsables. Dicha estructura permite analizar la posición jurídica de cada sujeto atendiendo a su participación efectiva, y no únicamente a la denominación que se le atribuya.

La responsabilidad proactiva también resulta relevante para esta comparación. El RGPD exige que el responsable pueda demostrar el cumplimiento de sus obligaciones mediante instrumentos como los registros de actividades, las evaluaciones de impacto y las medidas de protección desde el diseño. Dado que la normativa ecuatoriana también contempla la responsabilidad proactiva y demostrada, la comparación debe centrarse en cómo se conectan estas herramientas con la identificación de los roles y la atribución de obligaciones.

Esta delimitación repercute, además, en la aplicación de las bases de licitud, el régimen sancionador y los derechos de los titulares. Identificar al sujeto responsable de una decisión permite determinar quién debe justificar la base jurídica del tratamiento, atender las solicitudes de los interesados y responder por los incumplimientos que le sean atribuibles. Con todo, si se afirma que existen dificultades prácticas en estos ámbitos, debe acreditarse mediante el análisis de las normas aplicables y, cuando corresponda, de su aplicación efectiva.

El principal hallazgo del estudio es que la protección de datos no depende únicamente del reconocimiento legal de responsables, encargados y terceros, sino también de la claridad con la que se relacionan su funciones y obligaciones. El RGPD proporciona criterios útiles para examinar esta cuestión, sin que ello implique trasladar automáticamente sus soluciones al ordenamiento ecuatoriano. En el análisis de los artículos 34 y 35 constituye un punto de partida para valorar si la regulación permite distinguir adecuadamente las posiciones jurídicas de los intervinientes y determinar las responsabilidades que corresponden a cada uno.

CONCLUSIONES

En el análisis permite concluir que la principal dificultad para delimitar roles y responsabilidades en la normativa ecuatoriana de protección de datos personales se encuentra en la relación entre las categorías jurídicas que reconoce la ley y las funciones que, en la práctica, cumple cada interviniente. El problema se aprecia especialmente en el artículo 35 de la LOPDP,

cuya regulación reúne elementos propios del encargado del tratamiento y del acceso de terceros a los datos, y dicha mezcla dificulta distinguir ambas figuras, pese a que no todo tercero que accede a datos personales actúa como encargado.

La comparación entre la LOPDP con el Reglamento General de Protección de Datos de la Union Europea, advierte que la posición jurídica de cada sujeto debe definirse a partir de lo que realmente hace en el tratamiento. El modelo europeo tiene criterios específicos para diferenciar al responsable del encargado y regular la corresponsabilidad, incluido el reparto de obligaciones entre quienes determinan conjuntamente los fines y medios del tratamiento, por lo que tales criterios son útiles para revisar la normativa ecuatoriana, sin trasladar automáticamente sus soluciones, teniendo en cuenta las particularidades y realidad de nuestro ordenamiento.

Los resultados también muestran que la delimitación de los roles tiene consecuencias que van más allá de su definición formal. De ella depende saber quién debe cumplir ciertas obligaciones, quién atiende los derechos de los titulares y quién responde por los incumplimientos que le correspondan. Consecuentemente, la atribución de responsabilidad exige vincular la función de cada interviniente con las obligaciones previstas en la ley especialmente cuando participan varios sujetos en una misma operación de tratamiento.

El presente trabajo de investigación pone en evidencia la necesidad de precisar la relación entre las figuras del responsable, el encargado y el tercero en el marco ecuatoriano, y los criterios para distribuir las obligaciones cuando intervienen varios sujetos, de modo que al contar con esa precisión ayudaría a reducir las dudas interpretativas y mejorar la seguridad jurídica en la aplicación de la LOPDP. En ese punto radica el valor de la comparación con el modelo europeo, en proporcionar criterios y herramientas de análisis para estudiar esa delimitación y medir su coherencia con las exigencias de una protección efectiva de los datos personales.

REFERENCIAS BIBLIOGRÁFICAS

Agencia Española de Protección de Datos. (2018). *Guía del Reglamento General de Protección de Datos para responsables de tratamiento*. https://www.aepd.es/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

Asamblea Nacional del Ecuador. *Ley Orgánica de Protección de Datos Personales* [Registro Oficial Suplemento 459 de 26-may.-2021]. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Barreno, M. (2025). El derecho a la privacidad en la era digital: desafíos y garantías frente a la vigilancia masiva desde una perspectiva de derechos humanos*. International Visual Culture Review Revista Internacional De Cultura Visual*, *17*(1), 235-245.

Becerra, C. (2025). El delegado de protección de datos (DPO). *Revista Pensamiento Penal, 2*(3), 116-120.

Carrillo, F. (2021). The central axes of data protection: consent and purpose. criticisms and proposals towards regulation of the protection of personal data in Ecuador. *USFQ Law Review*, *8*(1), 175-204.

Comité Europeo de Protección de Datos. (2018). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.

De Alba Bastarrechea, E. (2023). El derecho de acceso a la información sobre destinatarios concretos de los datos personales: comentario a la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-154/21. *Revista Parlamentaria de la Asamblea de Madrid,* 45, 323-326. *https://doi.org/10.59991/rvam/2023/n.45/96*

Estepa Montero, M. (2022). *El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas*. Anuario Jurídico y Económico Escurialense, LV (2022) 67-90, 1133-3677.

Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L. y Tosoni, L. (Eds.). (2021). The EU General Data Protection Regulation (GDPR): A Commentary - 2021 Update. http://dx.doi.org/10.2139/ssrn.3839645

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE núm. 294, de 06/12/2018. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673&p=20251227&tn=5

Martínez, R. (2025). El rol del delegado de protección de datos en Europa tras la aprobación del Reglamento UE de Inteligencia Artificial. *Revista IUS ET VERITAS*, *71*, 1-16. https://doi.org/10.18800/iusetveritas.202502.004

Mendoza, C. (2025). El rol del delegado de protección de datos en el sector público y el uso de la IA. *Revista Canaria De Administración Pública*, *4*, 243-296. https://doi.org/10.36151/RCAP.4.9

Morales Echeverria, D. A., Morales Alarcón, F. P., Cajamarca Altamirano, E. E. y Intriago Usca, F. J. (2024). La protección de datos personales en Ecuador: evolución legislativa y comparación con modelos regionales en Sudamérica. *Perspectivas Sociales Y Administrativas*, *2*(2), 35–44. https://doi.org/10.61347/psa.v2i2.70

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679 de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.* BOE. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Sempere Samaniego, F. (2025). El régimen sancionador del Reglamento General de Protección de Datos: un enfoque teórico-práctico. https://hdl.handle.net/10637/18644

Serrano, J. (2019). *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia*. vLex. https://vlex.es/source/proteccion-de-datos-y-la-regulacion-de-las-tecnologias-en-la-negociacion-colectiva-y-en-la-jurisprudencia-31055

Sierra, E. (2018). El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico. *Revista Internacional y Comparada de relaciones laborales y derecho del empleo*, *6*(1), 237-260. https://ejcls.adapt.it/index.php/rlde_adapt/article/view/558

Tribunal Supremo. (2016a). *Sentencia 1618/2016*. Sala de lo Contencioso-Administrativo, España. https://www.poderjudicial.es/search/TS/openDocument/b6f677f90f58622d/20160718

Tribunal Supremo. (2016b). *Sentencia 1689/2016*. Sala de lo Contencioso-Administrativo, España. https://www.poderjudicial.es/search/TS/openDocument/426bd95b40f55648/20160726

Tribunal Supremo. (2016c). *Sentencia 1810/2016.* Sala de lo Contencioso-Administrativo, España. https://www.poderjudicial.es/search/TS/openDocument/da9873d5ab4f3034/20160729

Tribunal Supremo. (2020). *Sentencia 1620/2020*. Sala de lo Contencioso-Administrativo, España. https://vlex.es/vid/855089072

Vélez, H. (2015). La responsabilidad jurídica: aproximación al concepto, relación con otros conceptos jurídicos fundamentales y su funcionamiento. *Revista de la Facultad de*

Derecho y Ciencias Políticas, *45*(122), 127-151. http://www.scielo.org.co/scielo.php?pid=S0120-38862015000100006&script=sci_arttext

Voigt, P. y Bussche, A. (2024). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer Nature, 2024.

Agradecimientos

Los autores expresan su agradecimiento a las personas e instituciones que contribuyeron, directa o indirectamente, al desarrollo de esta investigación**.**

Financiamiento

El presente trabajo de investigación no recibió financiamiento de ninguna agencia, institución o empresa.

Conflicto de intereses

Los autores declaran que no existe conflicto de intereses.

Contribución de los autores

HDCM: Conceptualización, análisis formal, investigación, visualización y redacción - borrador original, curación de datos.

MBPB: Conceptualización, análisis formal, investigación, visualización y redacción - borrador original, curación de datos.

AJTA: Conceptualización, análisis formal, investigación, visualización y redacción - borrador original.

INLS: Conceptualización, análisis formal, investigación, visualización y redacción - borrador original, revisión y edición.

Declaraciones éticas

La presente investigación no requirió aprobación de un comité de ética, dado que se trata de un estudio sin riesgo, sin intervención ni identificación de participantes humanos, de conformidad a la normativa local en vigor.