UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ
Colegio de Jurisprudencia

Retos de la sobrevaloración del consentimiento y la autodeterminación informativa en protección de datos personales

Francisco José Almeida De la Cueva
Jurisprudencia

Trabajo de fin de carrera presentado como requisito
para la obtención del título de Abogado

Quito, 23 de noviembre de 2023

© DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en la Ley Orgánica de Educación Superior del Ecuador.

Nombres y apellidos: Francisco José Almeida De la Cueva
Código: 00207339
Cédula de identidad: 1718521345
Lugar y Fecha: Quito, 23 de noviembre de 2023.

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics COPE descritas por Barbour *et al*. (2017) Discussion document on best practice for issues around theses publishing, disponible en http://bit.ly/COPETheses.

UNPUBLISHED DOCUMENT

Note: The following capstone project is available through Universidad San Francisco de Quito USFQ institutional repository. Nonetheless, this project – in whole or in part – should not be considered a publication. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour *et al*. (2017) Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses.

RETOS DE LA SOBREVALORACIÓN DEL CONSENTIMIENTO Y LA AUTODETERMINACIÓN INFORMATIVA EN PROTECCIÓN DE DATOS PERSONALES[1]

CHALLENGES OF THE OVERVALUATION OF CONSENT AND INFORMATIONAL SELF-DETERMINATION IN DATA PROTECTION

Francisco José Almeida De la Cueva[2]
almeidadfrancisco@gmail.com

RESUMEN

La Ley Orgánica de Protección de Datos Personales, publicada en mayo de 2021, se basa en el Reglamento General de Protección de Datos (RGPD) europeo, el cual pone al consentimiento y a la autodeterminación informativa como pilares para la protección del derecho a la privacidad de los individuos. Esto a su vez se encuentra fundamentado en la noción de que el individuo es capaz de entender las implicaciones del procesamiento de sus datos y controlar los mismos. Por otro lado, los avances en la ciencia de datos y tecnología vuelven cada vez más complejos a los flujos de tratamiento de datos personales. Adicionalmente, los espacios físicos han empezado a digitalizarse a través del Internet de las Cosas; y, los individuos se encuentran cada vez más frecuentemente con avisos de privacidad. El propósito de la presente investigación es analizar si la postura actual aún se puede aplicar correctamente a la realidad.

PALABRAS CLAVE

Protección de datos personales, consentimiento, autodeterminación informativa.

ABSTRACT

The Ecuadorian Data Protection Law introduced in May 2021, is based on the European General Data Protection Regulation, (GDPR) which places consent and informational self-determination as pillars for the protection of individuals' rights. This view, in turn, is founded on the notion that individuals are capable of understanding the implications of data processing and controlling it. At the same time, advances in data science and technology make data processes more complex. Additionally, physical spaces are being digitalized through the Internet of Things and individuals are presented with privacy policies much more frequently. The purpose of this investigation is to analyze if the current regulatory strategy can still be effectively applied to reality.

KEY WORDS

Data protection, consent, informational self-determination.

---

[1] Trabajo de titulación presentado como requisito para la obtención del título de Abogado. Colegio de Jurisprudencia de la Universidad San Francisco de Quito. Dirigido por José Sebastián Ponce Rodríguez.

Fecha de lectura: 24 de noviembre de 2023
Fecha de publicación: 11 de diciembre de 2023

SUMARIO

1. Introducción

Una de las mayores constantes del siglo XXI ha sido que, como sociedad, nos encontramos en constante adaptación ante una multiplicidad de nuevos paradigmas. En términos de regulación de protección de datos, Ecuador ha sido un adoptante tardío, pero finalmente las nuevas necesidades provocadas por el desarrollo de nuevas tecnologías lo han obligado a adoptar una norma específica. La Ley Orgánica de Protección de Datos Personales, LOPDP[3], contiene una importante influencia del Reglamento General de Protección de Datos Europeo, "RGPD"[4].

En principio, esto tiene sentido dada la proximidad entre sistemas jurídicos y el mayor avance científico y tecnológico que existe en Europa. Sin embargo, existen tecnologías con un mayor potencial disruptivo que otras. Tal es el caso del *big data*, que se refiere a un grupo de técnicas y tecnologías que permite acceder a enormes conjuntos de datos[5]. Brett Frischmann y Evan Selinger mantienen que a través de su uso se puede practicar ingeniería social, influenciando así la forma en la que las personas piensan, actúan y perciben el mundo[6].

[3] Ley Orgánica de Protección de Datos Personales, [LOPDP], R.O. Suplemento 459 de 26 de mayo de 2021.
[4] Reglamento (UE) 2016/679, Parlamento Europeo Y El Consejo De La Unión Europea [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] [RGPD], L 119/1, de 27 de abril de 2016.
[5] S. Sasikala, Renuka Devi D, "Introduction to Big Data Analytics" *en Research Practitioner's Handbook on Big Data Analytics* (Palm Bay: Apple Academic Press, 2023), 2, (traducción no oficial).
[6] Brett Frischmann, Evan Selinger, "Techno-Social Engineering of Humans through Smart Environments", en *Re-Engineering Humanity* (Cambridge: Cambridge University Press, 2018), 125.

A partir del impacto que la recolección y tratamiento de datos personales puede tener a nivel individual, así como a nivel social, es de gran importancia buscar las mejores formas de regular esta materia de manera efectiva. Actualmente, se toma al consentimiento como pieza fundamental para la regulación de la recolección y tratamiento de datos, con base en los antecedentes del RGPD, que mantienen al consentimiento, y a la autodeterminación informativa como piedra angular en la regulación de esta rama del Derecho.

No obstante, la cada vez más rápida sofisticación de tecnologías que utilizan datos personales genera una gran incógnita acerca de si se pueden mantener los mismos paradigmas; o, si hacerlo podría causar que la realidad tecnológica supere a la regulación y en realidad sea hora de disrumpir desde el campo normativo a través de nuevos enfoques y concepciones.

Este trabajo analizará las potenciales problemáticas que la situación tecnológica actual ocasiona para una regulación que prepondera el consentimiento y la autodeterminación informativa, ¿existe una sobrevaloración del consentimiento al no tomarse en cuenta que la situación tecnológica actual podría volver demasiado complejo tener que continuamente otorgar el mismo? Se partirá desde los antecedentes normativos del Reglamento General de Protección de Datos, norma en la que la Ley Orgánica de Protección de Datos ecuatoriana se encuentra basada. Posteriormente, se revisará si los avances tecnológicos actuales dificultan la aplicación de la regulación en la práctica, principalmente con respecto al uso de *big data* y el Internet de las Cosas. Adicionalmente, se analizarán los retos para la innovación creados a partir de este sistema regulatorio.

2. Estado del Arte

La privacidad y la protección de datos personales son temas actualmente muy discutidos debido a la cada vez más profunda inserción de la tecnología en las vidas de los seres humanos, y las importantes repercusiones que trae consigo este cambio. Este capítulo presentará las posiciones que abordan los problemas creados a partir de una sobrevaloración del consentimiento.

Los problemas derivados de normas que posicionan al consentimiento y la autodeterminación informativa como pilares de la regulación de datos personales ya han sido tratados por algunos académicos. Acerca del consentimiento, Elena Gil señala que, “El

consentimiento informado es el corolario natural de la idea de que privacidad implica control sobre nuestra información. Sin embargo, no siempre está claro cuándo es necesario y cuáles son las condiciones que deben cumplirse para que este consentimiento sea válido"[7]. Según la autora, este es un problema que se ha agudizado, debido a la creciente importancia que el tratamiento de datos personales ha tomado a partir de la introducción del *big data*[8]. Su obra señala importantes retos que la legislación actual no ha podido solucionar a través de una regulación tradicional de esta materia.

Gil plantea que los actuales medios para recabar el consentimiento a través de políticas de privacidad en la web no ofrecen un consentimiento real, dado que la mayoría de los usuarios no las lee[9]. En primer lugar, demuestra que las soluciones planteadas por el legislador en tanto al diseño y simplificación de estas políticas no son totalmente factibles, dada la complejidad que actualmente podría darse en un flujo de tratamiento. Como segundo punto, demuestra que, con cada vez más frecuencia, es posible obtener información de individuos que no han otorgado su consentimiento, a través de un grupo poblacional similar que sí lo ha otorgado. Con respecto a esto Gil señala que, "[e]sto supone que, en realidad, cada individuo no tiene una capacidad real de tomar una decisión que proteja sus intereses […]"[10].

Esto se puede visualizar tomando como ejemplo los mecanismos utilizados en páginas web para que el usuario entregue o no su consentimiento al tratamiento de sus datos personales. Por ejemplo, con respecto a los mecanismos *opt-in* y *opt-out*, Gil hace un análisis entre dos posiciones doctrinarias en materia de protección de datos. Escribe que, por un lado, están quienes manifiestan que todos los datos deben ser considerados 'personales', y por ende regulados por la normativa de protección de datos personales; y, por otro, quienes toman una posición más "pragmática", en palabras de la autora e identifican un riesgo en la "[…] creciente atención por el consentimiento expreso y el principio de minimización de datos, sin tomar en consideración el valor o los usos de dichos datos"[11], estableciendo que hacerlo, podría obstaculizar procesos de innovación y desarrollo social. Luego de analizar

[7] Elena Gil González "El Consentimiento", en *Big Data, Privacidad y Protección de Datos* (Madrid: Agencia Española de Protección de Datos, 2016), 57.
[8] Id., 62.
[9] Id., 71.
[10] Id., 74.
[11] Id., 81.

ambas posiciones, Gil concluye que, a partir de los agudos cambios en el tratamiento de datos personales, guiados por grandes avances tecnológicos "[…] el consentimiento, tal y como está previsto en la actualidad, no soluciona los problemas prácticos que antes venía a solucionar[12]".

Por otro lado, Bert-Jaap Koops sostiene que, el RGPD pone un énfasis importante, pero poco realista en la autodeterminación informativa, sin tomar en cuenta la falta de alternativas a plataformas que recolectan datos, la falta de opciones para modelos de negocios que operan a través de un servicio que a *prima facie* parece gratuito para el usuario (pero en realidad genera réditos a través del tratamiento y venta de sus datos), la limitada capacidad de los seres humanos para tomar decisiones racionales y la dificultad de tener un control real sobre el tratamiento de los datos[13].

Para Hartzog, quien también es crítico de la forma en la que actualmente se regula esta materia, intentar basar la regulación en el control, otorgando a los titulares todas las opciones sobre mucha información, crea simplemente una ilusión de control[14]. Para este autor la regulación basada en el diseño de la tecnología ayuda a generar confianza entre el titular y el responsable, esto a su vez permite que el titular otorgue su consentimiento únicamente en ocasiones donde realmente importa, mitigando así la carga que consentir a todo implicaría[15].

3. **Marco Teórico**

Los retos que podrían presentarse al consentimiento en materia de protección de datos personales, no se encuentran propiamente en su figura o estructura, sino más bien en la supremacía que la regulación plantea sobre este concepto. Existen, a grandes rasgos, dos corrientes importantes. Por un lado, la más tradicional, sostiene que a través del consentimiento y la autodeterminación informativa se protege de una mejor manera la privacidad del individuo; y, por otro, quienes mantienen que la normativa ya no puede mantener al consentimiento como su piedra angular para legitimar el tratamiento de datos

[12] Id., 81.
[13] Bert-Jaap Koops, "The trouble with European data protection law", *International Data Privacy Law* 4(4) (2014), 251-253. Acceso el 10 de septiembre de 2023, https://doi.org/10.1093/idpl/ipu023.
[14] Woodrow Hartzog, "Privacy Values" en *Privacy's Blueprint: the battle to control the design of new technologies* (Cambridge: Harvard University Press, 2018), 57.
[15] Id., 95.

personales debido a los problemas prácticos y técnicos que han surgido en las últimas dos décadas.

En esta primera línea se mantienen posiciones como la planteada en el Reporte Albrecht, realizado por Jann Philipp Albrecht, miembro del Parlamento Europeo y una figura muy importante en el contexto del desarrollo del RGPD de acuerdo a Kuner y Bygrave[16]. Acerca de este reporte, Kuner y Bygrave escriben que:

> El Reporte Albrecht consideró al consentimiento como la Piedra angular de la regulación europea de protección de datos, y como la mejor manera para que los individuos controlen el tratamiento de sus datos … el Reporte respaldaba la idea de que "si quieres mis datos, solicita mi consentimiento". Consecuentemente, la importancia del consentimiento fue elevada en comparación con la propuesta previa del RGPD. El reporte requirió que el consentimiento sea otorgado libremente, específico, informado y explicito, consecuentemente impidiendo a los responsables de apoyarse en el consentimiento implícito y casillas pre-marcadas[17].

Barocas y Nissenbaum también se encuentran dentro de esta primera corriente, ya que si bien admiten que el consentimiento ha sido utilizado como una forma para intentar nivelar al titular con el responsable y que hoy en día esto no es práctico, creen que esta figura aún puede jugar un papel importante cuando este se combina con una carga sobre el responsable de explicar por qué el titular tiene una buena razón para otorgar su consentimiento[18].

Al mismo tiempo, existen posiciones que mantienen una postura aún más escéptica, y consideran que debe reducirse significativamente la importancia del consentimiento y la autodeterminación informativa; o, incluso directamente que ya no son posibles en el siglo XXI. Bert-Jaap Koops argumenta que el problema principal cuando se habla de autodeterminación informativa es el "mito del consentimiento[19]", dado que, en contextos privados o comerciales a pesar de ser la base legitimadora de tratamiento más común, es únicamente teórico y no mantiene importancia práctica[20].

---

[16] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, "Background and Evolution of the GDPR" en *The EU General Data Protection (GDPR): A Commentary* (Oxford: Oxford University Press, 2020), 5, (traducción no official).
[17] Id., 18.
[18] Solon Barocas, Helen Nissenbaum, "Big Data's End Run around Anonymity and Consent" en *Privacy Big Data and the Public Good*, Editado por Julia Lane, et al., (Nueva York: Cambridge University Press, 2014), 64.
[19] Id., 251.
[20] Id., 251-252.

En una posición similar a la de Koops se encuentra Solove, quien esgrime que el consentimiento no tiene ningún tipo de valor a menos que el individuo que otorgue dicho consentimiento tenga suficiente información para analizar el riesgo detrás de su decisión[21]. Solove agrega que, incluso en el caso del RGPD, que mantiene un estándar de consentimiento informado, requerir de los responsables más transparencia, más derechos para los individuos, y en general, más normas que intenten garantizar al individuo un grado más alto de control sobre sus datos va a ser fútil, porque simplemente hay demasiados factores como la falta de conocimiento técnico, sesgos cognitivos, manipulación del consentimiento, falta de sustitutos y una fatiga de consentir varias veces[22].

4. Marco Normativo

Este apartado tiene como propósito contextualizar el estado actual de la regulación en materia de protección de datos en Ecuador y en Europa. Como consecuencia de la ascendente influencia del tratamiento de datos personales, varios países han adoptado una norma de protección de datos personales. Actualmente, se ostenta al RGPD como la norma más robusta y completa en esta materia.

Ecuador fue un adoptante tardío a nivel regional[23]. En el año 2021 se publicó la Ley Orgánica de Protección de Datos Personales, en la que, manteniéndose en línea con la tendencia vista hasta el momento, se optó por un modelo similar al desarrollado en Europa. Este contempla una norma especializada que busca regular la materia de manera extensiva. Se establecen mecanismos para que a través del consentimiento se pueda mantener como

[21] Daniel J. Solove, "Murky Consent: An Approach to the Fictions of Consent in Privacy Law", *104 Boston University Law Review* Forthcoming (2024), 12, Acceso el 18 de septiembre de 2023, https://dx.doi.org/10.2139/ssrn.4333743.
[22] Id., 34.
[23] *Ver*, "Un panorama retrospectivo y futuro de la protección de datos en América Latina y España", Electronic Frontier Foundation, Acceso el 14 de noviembre de 2023, https://www.eff.org/es/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain#:~:text=En%20Am%C3%A9rica%20Latina%2C%20Chile%20fue,)%20y%20Panam%C3%A1%20(2019), (Chile adoptó una norma en 1999, Argentina en 2000, Uruguay en 2008, Perú en 2011, Colombia en 2012, México en 2010 y Brasil en 2018).

pilar a la autodeterminación informativa[24]. Esta es una tendencia que se ha observado en casi la totalidad de ordenamientos jurídicos de la región[25].

Quizás el antecedente más importante para entender la tendencia actual en colocar un papel fundamental sobre el consentimiento y la autodeterminación informativa es la Decisión del Tribunal Constitucional Alemán acerca de la constitucionalidad de la Ley del censo de 1983[26]. Esta sentencia jugó un papel fundamental para consolidar la importancia impuesta sobre la autodeterminación informativa. Según el Tribunal, la información recolectada para propósitos estadísticos que aún no haya sido anonimizada, únicamente puede compartirse a través de una autorización expresa, cuando esta sea recogida por las autoridades. Al mismo tiempo, dichas autoridades deben asegurarse de que los datos sean tratados confidencialmente, ya que no anonimizar estos datos estadísticos recolectados a través de una norma sería una interferencia injustificable al derecho a la autodeterminación informativa[27].

Adicionalmente, en su fallo el Tribunal agrega que, en caso de que una norma quiera tratar datos con fines estadísticos y otros propósitos adicionales, estaría buscando algo incompatible. Esto, debido a que se podría afectar la claridad y comprensibilidad de la norma en cuestión. Consecuentemente, una norma debe ser clara y delimitar estrictamente los propósitos del tratamiento, permitiendo al individuo visibilizar la finalidad y los datos necesarios[28]. Por estos motivos, el Tribunal decide que la ley del censo de 1983 es inconstitucional[29]. Con respecto a la autodeterminación informativa, el Tribunal señaló que, con base en la tecnología actual, el individuo debe contar con la claridad suficiente para

[24] F.N. Roldán Carrillo, "Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador", *USFQ Law Review* 8 (2021), 189, Acceso el 14 de septiembre de 2023, https://doi.org/10.18272/ulr.v8i1.2184.
[25] Luis Enríquez Álvarez, "La Visión de América Latina sobre el Reglamento General de Protección de Datos", *Revista Del Centro Andino De Estudios Internacionales* 19 (2019), 101-102, Acceso el 14 de septiembre de 2023, https://doi.org/10.32719/26312549.2019.19.4.
[26] Ley del Censo, derecho a la personalidad y dignidad humana, Tribunal Constitucional de la República Alemana, Sentencia Constitucional, 15 diciembre 1983.
[27] Ley del Censo, derecho a la personalidad y dignidad humana, Tribunal Constitucional de la República Alemana, Sentencia Constitucional, 15 diciembre 1983, párr. 194.
[28] Ley del Censo, derecho a la personalidad y dignidad humana, Tribunal Constitucional de la República Alemana, Sentencia Constitucional, 15 diciembre 1983, párr. 195.
[29] Ley del Censo, derecho a la personalidad y dignidad humana, Tribunal Constitucional de la República Alemana, Sentencia Constitucional, 15 diciembre 1983, párr. 213.

determinar qué tipo de información es conocida por otras partes de su ambiente social, y si es difícil señalar quiénes pueden acceder a la misma[30].

Dentro de la misma sentencia, se agrega que un orden social y las normas aplicables al mismo no serían compaginables con el derecho a la autodeterminación informativa si los ciudadanos no podrían saber quiénes tienen información sobre ellos, a qué hora y en qué ocasión[31]. Este antecedente jurisprudencial, constituye uno de los fundamentos de la construcción de las posteriores normas de protección de datos. Posteriormente, en el marco de la Unión Europea, se emitió el RGPD, que regula la protección de datos personales a nivel comunitario.

En el caso ecuatoriano, la LOPDP fue expedida el 26 de mayo de 2021. En términos regulatorios, ha sido un importante avance para la regulación de esta materia en Ecuador. Especialmente, porque al ser un adoptante tardío de una norma específica de protección de datos, Ecuador empezó a palpar las consecuencias concretas de no contar con una Ley, principalmente a través de las grandes filtraciones de información[32] y malas prácticas de *call centers*[33] o empresas que inescrupulosamente obtenían datos para comercializar sus productos.

5. Evaluación Normativa

Al existir una importante similitud entre la normativa ecuatoriana, el RGPD y la normativa española de protección de datos, a continuación, se procederá a exponer artículos relevantes de cada regulación relacionadas al consentimiento; y, en un sentido más amplio, a la autodeterminación informativa.

5.1 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016

[30] Ley del Censo, derecho a la personalidad y dignidad humana, Tribunal Constitucional de la República Alemana, Sentencia Constitucional, 15 diciembre 1983, párr. 146.
[31] Ley del Censo, derecho a la personalidad y dignidad humana, Tribunal Constitucional de la República Alemana, Sentencia Constitucional, 15 diciembre 1983, párr. 146.
[32] BBC News Mundo "Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano", British Broadcasting Corporation, 2019, https://www.bbc.com/mundo/noticias-america-latina-49721456.
[33] Primicias, "Acoso telefónico: empresas que llamen sin autorización serán investigadas", Primicias, 2021, https://www.primicias.ec/noticias/economia/superintendencia-investigacion-empresas-llamadas-autorizacion/.

i. **Licitud, lealtad y transparencia:** De acuerdo con este principio, los datos deben ser tratados de una forma legal, es decir, respetando todas las normas vigentes del ordenamiento jurídico; leal, lo cual implica que los datos a ser tratados se han obtenido a través de medios engañosos, poco transparentes o injustos; y, transparente, que se refiere a la forma con la que el responsable se relaciona con el titular. Consecuentemente, establece que se debe informar al titular acerca de la finalidad y las implicaciones del tratamiento de sus datos[34].

ii. **Limitación de finalidad:** El literal b del artículo 5 establece que los datos deben ser recogidos con fines "determinados, explícitos y legítimos"[35]. Agrega que no está permitido tratar datos personales con fines distintos[36]. La importancia de este principio para fines del consentimiento y autodeterminación informativa radica en que el responsable tendría que obtener el consentimiento para cada finalidad. De este modo, se intenta volver más amigable a la aceptación de cada finalidad.

iii. **Minimización de datos:** Con base en este principio, los datos recogidos deben ser "adecuados, pertinentes y necesarios"[37] para las finalidades del tratamiento. Existe una importancia relación con el anterior principio mencionado, dado que la minimización de datos obliga al responsable adicionalmente a recoger únicamente los datos necesarios.

iv. **Exactitud:** El RGPD determina que el responsable debe velar por la precisión e integridad de la información almacenada, así como de los resultados del tratamiento, con especial cuidado cuando este tenga un impacto importante o negativo sobre el titular[38]. En la práctica esto quiere decir que los responsables deberían tener total conocimiento y control del proceso para el tratamiento de datos.

v. **Limitación del plazo de conservación:** El RGPD también obliga a los responsables a establecer un tiempo máximo de la conservación de los datos personales. Esto previene que datos que con el pasar del tiempo se vuelvan inexactos sean utilizados, además de tratamientos ulteriores y en teoría empodera al individuo.

[34] Artículo 5, RGPD.
[35] Artículo 5, RGPD.
[36] Artículo 5, RGPD.
[37] Artículo 5, RGPD.
[38] Artículo 5, RGPD.

vi. **Integridad y confidencialidad:** Con este principio, la norma se refiere a que los datos deben ser tratados de manera ética y manteniendo un nivel adecuado de sigilo y protección sobre la información[39].

vii. **Responsabilidad proactiva:** Este principio obliga al responsable a mantener prácticas adecuadas y tomar decisiones que garanticen los derechos de los titulares dentro de todo el ciclo de tratamiento de datos[40], es decir, recolección, tratamiento o procesamiento, transferencia y destrucción de la información. Adicionalmente, el RGPD indica que el responsable debe ser "capaz de demostrarlo"[41].

Al mismo tiempo, el RGPD establece algunos requisitos relacionados al consentimiento en su artículo 32. Mismos que demuestran la intención de establecer el mayor grado de protección posible para la autodeterminación del titular. La norma determina que el consentimiento debe otorgarse mediante un acto que fielmente refleje una manifestación "[…] libre, específica, informada e inequívoca de la voluntad del individuo"[42]. Acerca de las formas de obtenerlo. El mismo artículo no considera al consentimiento silencioso como válido, de esta manera intenta asegurarse que el titular brinde su consentimiento de forma activa y no tácita. Se determina que la obtención del consentimiento:

> […] podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento[43].

5.2 España

Con respecto a la Ley española de protección de datos, LOPDE[44], cabe mencionar el siguiente principio relacionado al consentimiento:

[39] Artículo 5, RGPD.
[40] Artículo 5, RGPD.
[41] Artículo 5, RGPD.
[42] Artículo 32, RGPD.
[43] Artículo 32, RGPD.
[44] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, BOE N°294, de 06/12/2018.

Tratamiento basado en el consentimiento del afectado: En línea con lo establecido en el RGPD, la LOPDE establece los requisitos de "libre, específico, informado e inequívoco"[45] con relación al consentimiento. Al mismo tiempo, determina que el consentimiento es válido únicamente cuando se otorgue mediante un acto que demuestre una voluntad clara[46].

5.3 Principios Actualizados sobre la Privacidad y Protección de Datos de la Organización de los Estados Americanos

Por su parte, la Organización de los Estados Americanos (OEA) ha establecido en sus Principios Actualizados sobre Privacidad la Privacidad y Protección de Datos algunos criterios para la recolección y tratamiento de datos relacionados al consentimiento. Su primer principio de Finalidades Legítimas y Lealtad, determina que la captura de datos personales debe limitarse y hacerse con el conocimiento o consentimiento del individuo[47].

Respecto de la lealtad, este principio determina que los medios para la recopilación deben ser apropiados para la forma y momento de solicitar el consentimiento, sin engañar al titular[48]. Con este principio es posible identificar nuevamente como la tendencia normativa se ha inclinado a regulación que al menos en papel facilite la vida del titular al momento de otorgar su consentimiento.

El segundo principio, Transparencia y Consentimiento establece que previo a la recopilación se debe especificar la siguiente información:

> i) la identidad y datos de contacto del Responsable; ii) las finalidades del Tratamiento; iii) el fundamento jurídico de su Tratamiento; iv) los destinatarios o categorías de destinatarios a los cuales los Datos Personales serán comunicados; v) la información a serles transmitida, y vi) la existencia, forma y mecanismos o procedimientos a través de los cuales los Titulares de Datos Personales podrán ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad[49].

Al referirse al consentimiento, se indica que es necesario proporcionar al titular con información suficiente en tanto a los datos recopilados, las finalidades, el tratamiento y la

[45] Artículo 6, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, BOE N°294, de 06/12/2018.
[46] Artículo 6, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
[47] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, Publicación aprobada por la asamblea general de la OEA, Organización de los Estados Americanos, OEA/Ser.D/XIX.20, 03 de enero de 2022, párr. 1.
[48] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, párr. 1.
[49] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, párr. 2.

posible divulgación que se pueda dar. Se determina que la recolección de este consentimiento debe ser realizada de forma que se pueda comprobar que éste es libre y claro. Según este principio, la forma de obtener el consentimiento debe variar de acuerdo con la edad y capacidad del titular[50].

Podemos reconocer entonces cómo estos principios, al igual que el RGPD se apoyan en el consentimiento, utilizándolo como base fundamental para la regulación.

5.4 Ecuador

La Ley Orgánica de Protección de Datos establece sus principios en el Art. 10, a continuación, se detallarán los más relevantes:

i. **Juridicidad:** A diferencia del RGPD, donde existe un solo principio de legalidad, lealtad y transparencia, en la LOPDP estos se norman individualmente. Al igual que con el principio de legalidad del RGPD, se crea una obligación para el responsable de cumplir con todo el ordenamiento jurídico ecuatoriano a la hora de tratar datos personales[51].

ii. **Lealtad:** La función del principio de lealtad es principalmente la de proporcionar información al titular. Este principio obliga a que el titular esté en conocimiento constante cuando se estén "recogiendo, utilizando, consultando o tratando de otra manera"[52], así como las implicaciones de estos procesos.

iii. **Transparencia:** Además de buscar que el titular esté en conocimiento de que sus datos son recolectados, la LOPDP busca que la manera en la que se comunica esto permita al titular comprender qué está sucediendo. En este sentido, la LOPDP dispone que "toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro"[53]. Al mismo tiempo, establece que toda relación que nazca a partir del tratamiento de datos personales debe ser transparente[54]. Cabe resaltar que este

[50] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, párr. 2.
[51] Artículo 10, LOPDP.
[52] Artículo 10, LOPDP.
[53] Artículo 10, LOPDP.
[54] Artículo 10, LOPDP.

principio asume que toda la información acerca del tratamiento es simplificable a tal punto que un usuario común de una plataforma logre entender lo que sucede.

iv. **Finalidad:** El principio de finalidad es similar a la normativa europea en tanto obliga a que las finalidades sean "determinadas, explícitas y legítimas"[55]. La LOPDP busca una limitación del ámbito del tratamiento en la misma línea del RGPD.

v. **Pertinencia y minimización de datos personales:** Con relación a la cantidad y tipos de datos que pueden ser tratados, la LOPDP señala que estos deben "ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento"[56]. El objetivo de este principio es crear una obligación para el responsable de establecer los datos estrictamente necesarios previamente a solicitar el consentimiento del titular.

vi. **Proporcionalidad el tratamiento:** Este es un principio que no se encuentra establecido como tal en el RGPD. En el literal f del Art. 10 de la LOPDP se dispone que "[e]l tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos o a la naturaleza misma, de las categorías especiales de datos"[57]. A diferencia del principio anterior, el principio de proporcionalidad señala que el tratamiento debe limitarse a las finalidades para las que estos se obtienen o "a la naturaleza misma, de las categorías especiales de datos"[58].

vii. **Conservación:** De acuerdo con este principio, los datos recopilados deben tener una fecha para su eliminación. La LOPDP indica que el tiempo de conservación no puede ser "mayor al necesario para cumplir con la finalidad de su tratamiento"[59].

viii. **Responsabilidad proactiva y demostrada:** La LOPDP también incluyó este principio que obliga al responsable a "acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley […]"[60]. La norma determina

[55] Artículo 10, LOPDP.
[56] Artículo 10, LOPDP.
[57] Artículo 10, LOPDP.
[58] Artículo 10, LOPDP.
[59] Artículo 10, LOPDP.
[60] Artículo 10, LOPDP.

que, para estos fines, el responsable puede valerse de no solo demostrar su cumplimiento con la ley, sino también a través de sistemas, estándares, mejores prácticas, certificaciones[61].

ix. **Aplicación Favorable al titular:** Este es un principio que no se recoge dentro del Art. 5 del RGPD. De acuerdo con este precepto, cuando existan dudas sobre el alcance de una disposición, esto deberá ser interpretado a favor del titular[62].

Con respecto a los requisitos del consentimiento del titular para el tratamiento de sus datos, al igual que en el caso del RGPD, el legislador optó por un sistema que intente empoderar al titular a través de la creación de requisitos que intenten hacer más sencillo para el mismo entender las implicaciones de otorgar su consentimiento. En este sentido, la LOPDP establece que el consentimiento deber ser libre, específico, informado e inequívoco[63].

Al hablar de regulación del diseño de la tecnología, la LOPDP establece en su Art. 39 regulación acerca de la protección desde el diseño y por defecto[64] De acuerdo con el artículo citado, el desarrollador de soluciones tecnológicas debe tomar en cuenta la potencial incidencia del desarrollo desde la fase inicial del proyecto. Las soluciones creadas deben realizarse con miras a cumplir las disposiciones de la LOPDP. Con respecto a la protección por defecto, el citado artículo dentro de su segundo inciso dispone que se deberá aplicar toda medida pertinente para que el tratamiento se limite a los datos necesarios de acuerdo con las finalidades preestablecidas[65].

Finalmente, también es importante señalar que la normativa ecuatoriana también hace referencia al concepto de la autodeterminación informativa dentro del artículo 23, donde se establece el derecho a la educación digital. En este sentido, se determina que todos los ciudadanos tienen derecho a acceder y disponer de conocimiento de la tecnología[66]. Esto en apego con especial apego según la norma a los principios de:

[61] Artículo 10, LOPDP.
[62] Artículo 10, LOPDP.
[63] Artículo 8, LOPDP.
[64] Artículo 39, LOPDP.
[65] Artículo 39, LOPDP.
[66] Artículo 39, LOPDP.

> […] dignidad e integridad humana; los derechos fundamentales y libertades individuales con especial énfasis en la intimidad, la vida privada, autodeterminación informativa, identidad y reputación en línea, ciudadanía digital y el derecho a la protección de datos personales, así como promover una cultura sensibilizada en el derecho de protección de datos personales[67].

Al comparar la regulación en materia de protección de datos personales con el RGPD, la regulación española y los principios de la OEA, es posible identificar una tendencia regulatoria que ha puesto un importante énfasis sobre el consentimiento del titular para el tratamiento de datos personales. Esto con base en dos antecedentes importantes, el fallo del Tribunal Constitucional alemán acerca de la Ley del Censo del año 1983 y el Reporte Albrecht. Este concepto se encuentra dentro del RGPD y la LOPDP. Adicionalmente, se pudo observar que con respecto a la normativa sobre la privacidad por diseño y por defecto, no existe un desarrollo tan importante como en el caso del consentimiento. De hecho, como ya fue mencionado, se eliminaron ciertas disposiciones del proyecto original del RGPD acerca de la privacidad desde el diseño y por defecto.

6. ¿Cuáles son los retos del consentimiento en el tiempo del *Big Data?*

Hoy por hoy existen varios retos a la hora de aceptar los avisos de privacidad, estos se han generado principalmente a partir de los impactos de nuevas tecnologías y procesos en la sociedad. Tradicionalmente se ha considerado que los acuerdos entre privados son una de las mejores maneras de regular relaciones entre partes. Estas relaciones siempre fueron de distintos grados de complejidad. Sin embargo, la humanidad nunca fue testigo de avances tecnológicos de la magnitud y complejidad con los que vivimos hoy en día.

En un siglo donde se ha logrado hasta cuantificar y manipular emociones por medio de una plataforma de redes sociales[68] y en el cual la tecnología es cada vez más compleja y se vuelve un campo del conocimiento altamente especializado, ¿es real considerar a la autodeterminación informativa y, por lo tanto, al consentimiento como ejes centrales para la regulación de esta materia? Los siguientes capítulos abordarán esta pregunta y desarrollarán acerca de los potenciales retos actualmente presentados para el actual modelo regulatorio.

---

[67] Artículo 39, LOPDP.

[68] New York Times "*Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*", New York Times, 2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Para empezar, es importante conocer el motivo detrás del uso del término *big data,* que proviene de las enormes cantidades de información manipuladas. Para Barocas y Nissenbaum, cuando se habla de *big data* no se hace referencia a una tecnología en concreto, como se haría cuando hablamos de aviones, por ejemplo, sino a un paradigma o forma de pensar acerca de información y conocimiento a través de una cantidad masiva de datos y un marco para justificar decisiones, racionalizar acciones en prácticas a través del análisis de patrones, modelos y estructuras construidos a través de datos[69].

Según Pence, hoy en día estamos acostumbrados a hablar en términos de *gigabytes* o *terabytes* para el almacenamiento de nuestra información personal. No obstante, la medida de almacenamiento base en el mundo del *big data* son los *petabytes* (1.000 *terabytes*). Se estima que Google procesa alrededor de 20 *petabytes* al día[70]. El autor agrega que hoy en día los analistas de datos hablan de *exabytes* (1.000 *petabytes*) y *zettabytes* (1000 *exabytes*)[71]. Para agregar mayor contexto a lo voluminosos que son estos números, se estima que toda la información transmitida por los humanos a través del lenguaje en toda la historia ocuparía apenas 50 *petabytes*[72].

Así, la recolección, procesamiento y estudio de grandes volúmenes de información se pueden lograr importantes avances en distintos campos del conocimiento, más allá de su reconocido uso publicitario. El *big data* tiene aplicaciones de suma importancia para la sociedad como la detección de brotes de enfermedades[73], o el desarrollo de grandes proyectos científicos como el Gran Colisionador de Partículas, que procesa alrededor de 1 *petabyte* diario[74]. A esto hay que sumarle los importantes impactos que el desarrollo que este campo puede aportar en términos económicos. Según un informe del McKinsey Global Institute, se estima que a través de su uso se puede generar ganancias de alrededor de 3 trillones de dólares anualmente en tan solo 7 industrias que fueron estudiadas[75].

---

[69] Solon Barocas, Helen Nissenbaum. "Big Data's End Run around Anonymity and Consent", 46.
[70] H.E. Pence, "What is Big Data and Why is it Important?" *Journal of Educational Technology Systems* 43 (2014), 160, Acceso el 22 de septiembre de 2023, https://doi.org/10.2190/ET.43.2.d.
[71] Id., 160.
[72] Id.,160.
[73] Id., 163.
[74] Id., 165.
[75] James Manyika, *et al*., "Executive Summary" en *Open data: Unlocking innovation and performance with liquid information (*McKinsey Global Institute, 2013), 2, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/open-data-unlocking-innovation-andperformance-with-liquid-information.

Debido a la gran cantidad necesaria de información requerida para el correcto funcionamiento del *big data* y a los importantes incentivos que existen para su uso, su aplicación conlleva importantes riesgos para la privacidad de las personas. Esto a su vez ha creado algunos inconvenientes para la regulación.

En primer lugar, porque existen grandes incentivos económicos detrás de la implementación de esta tecnología, y en segundo lugar porque es complejo para quienes otorgan su consentimiento comprender bien cómo funciona la recolección y tratamiento de sus datos, dónde y cuándo finaliza el proceso y establecer una comunicación efectiva con el responsable del tratamiento. Ante este problema existen a grandes rasgos dos soluciones.

Analizando la línea en la que se mantiene la regulación europea y la LOPDP se ha observado que ambas buscaron igualar la posición del titular y el responsable, con el fin de que el primero, en posición de desventaja, sea capaz de tomar las mejores decisiones para sí mismo con toda la información disponible. A continuación, se abordarán las propuestas de quienes mantienen que nuevos retos tecnológicos requieren de nuevas soluciones, ya que se debe considerar las limitaciones impuestas a la realidad con el advenimiento de nuevas tecnologías.

Bert-Jaap Koops afirma que basarse en la autodeterminación informativa y en normas extensivas ya no es posible en el siglo XXI[76]. Así, el autor considera que el RGPD en la práctica es "letra muerta"[77] debido a los siguientes motivos: En primer lugar, está el modelo de negocio empleado hoy en día en el mundo digital. Las plataformas de servicios en línea como Google, Facebook y Twitter son gratuitas para usar, con la condición de que se entreguen datos personales, a través de los cuales dichas firmas se mantienen rentables, utilizándolos para varios fines, como, por ejemplo, enfocar publicidad para cada usuario o vender información sobre preferencias y hábitos de consumo[78].

La realidad es que el usuario es el producto. Sin embargo, existe una dinámica interesante dentro de esta relación, debido a que para emplear el *big data* se requieren altos volúmenes de información y la capacidad técnica para procesarlos, la información de un individuo tiene por lo general poco valor, y, de hecho, acceder a un servicio en línea tiende

[76] Bert-Jaap Koops, "The trouble with European data protection law", 251
[77] Id., 256.
[78] Id., 252.

a tener un mayor valor para el titular, por lo que el usuario probablemente acepta los términos y condiciones incluso cuando estos son invasivos.

La prevalencia de este modelo a su vez conlleva que a través del rediseño de la tecnología se busque caer fuera de los límites de regulación. Tal es el caso del procesamiento transitorio de datos. George, *et al*., definen a esta práctica como un proceso que "se limita a percibir su ambiente y procesan datos efímeramente, descartándolos de inmediato"[79], los autores analizan un caso de uso impulsado por la cadena de hipermercados alemana *Real*.

Esta creó el programa de publicidad *AdPack*, el cual emplea el reconocimiento facial con ciertas particularidades. El software se construyó alrededor de dos bibliotecas especializadas llamadas *SHORE* y *AVARD*, implementando un modelo de privacidad desde el diseño y con certificaciones de privacidad, limitándose a únicamente recoger el género, rango de edad y estado emocional de cada persona, y a través de esto divide a los clientes en grupos y proyecta publicidad apuntada específicamente a cada grupo.

Sin embargo, esta información no se almacena ni procesa, sino que la cámara detecta características de la persona como un metadato y genera un valor de hash de este, y en base a esto, se escoge la publicidad que se utilizará. Posteriormente, elimina la información en 150 milisegundos, volviendo imposible volver a identificar a un individuo[80]. Lo más interesante de este caso fue que ni la Agencia de Protección de Datos de Bavaria (*BayLDA*) ni la Comisión de Protección de datos de Irlanda pudo enmarcar a esta tecnología como recolectora de datos personales, ya que técnicamente hay una diferencia entre reconocimiento y detección facial, el reconocimiento requiere el almacenamiento para posteriormente volver a identificar los rasgos faciales de una persona, mientras que la detección es inmediata[81].

Esto implicaría que quienes recojan y procesen estos datos ya no requieran del consentimiento del titular, quedando libres de no acatar las normas, principios y sanciones. Un segundo ejemplo de cómo el rediseño permite distorsionar la regulación es el diseño de interfaz en las páginas web, Than Htut Soe, *et al*. encontraron a través del análisis de 300

[79] Damian George, Kento Reutimann, Aurelia Tamò-Larrieux, "GDPR bypass by design? Transient processing of data under the GDPR", *International Data Privacy Law,* 9(4) (2019), 285-286, Acceso el 17 de septiembre de 2023, https://doi.org/10.1093/idpl/ipz017.
[80] Id., 293.
[81] Id., 286-287.

páginas web de medios informativos que, a pesar de que la mayor parte de estas páginas web despliegan ventanas de diálogo que cumplen con los requisitos básicos del RGPD, en la práctica la modificación de la interfaz de estas puede dificultar mucho más otorgar un consentimiento informado[82].

Un segundo problema es la falta de modelos de negocio alternativos. Fundamentalmente esto es consecuencia de que las alternativas de suscripción no podrían atender a la misma cantidad de gente. Es importante considerar que, por lo general, desde la perspectiva de un individuo es más fácil entregar sus datos que pagar por un servicio. Esto se debe a que el valor de los datos recolectados se encuentra en grandes cantidades de volumen. Rostetter también menciona que los efectos de red generados a partir de tener varios usuarios son importantes para que los *startups* tecnológicos generen valor y crecimiento, y justamente son estos efectos de red y escalabilidad los que vuelven a estos servicios rentables y atractivos para los usuarios[83].

En este sentido, en caso de que el usuario no quiera consentir, simplemente no podrá tener acceso a estos servicios. A esto se le ha denominado el problema de "alternativas significantes", el cual según el estudio de Andreotta, *et al*. sitúa al titular en una posición desventajosa al no contar con posibilidades de renegociar las condiciones[84]. Este estudio también describe cómo, debido a la creciente importancia de las redes sociales en nuestras vidas, las personas jóvenes en especial se podrían ver presionadas a aceptar las políticas impuestas por miedo a encontrarse aislados de sus pares[85]. Al mismo tiempo, se menciona que las repercusiones de este problema se pueden agudizar aún más en contextos biomédicos[86].

Más allá de distintos modelos de negocio y alternativas para el usuario, está el problema de leer y comprender los acuerdos de privacidad. Lo mencionado se debe, según

---

[82] Than Htut Soe, *et al*., "Circumvention by design - dark patterns in cookie consent for online news outlets", *NordCHI'20: Proceedings of the Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, 26 de octubre de 2020 5, Acceso el 28 de septiembre de 2023, https://doi.org/10.1145/3419249.3420132.

[83] Carl Pascal Rostetter, "The importance of incentives and the network effect for digital startups to scale" (tesis de maestría, Universidad Católica Portuguesa, 2018), 24, https://repositorio.ucp.pt/handle/10400.14/25426?locale=en.

[84] Adam J. Andreotta, Nin Kirkham, Marco Rizzi, "AI, big data and the future of consent", *AI & Society* 37 (2022), 1721, Acceso el 4 de octubre de 2023, https://doi.org/10.1007/s00146-021-01262-5.

[85] Id., 1721.

[86] Id., 1721.

Koops, a que la mayor parte de personas no leen los términos y condiciones[87]. Ante esto, se podría esgrimir que no hacerlo recae en el titular de los datos.

Se debe considerar que existen importantes argumentos que demuestran que esto no se debe a una falta de cuidado por el titular. La realidad es más compleja debido a que existen factores tecnológicos, económicos, sociales y hasta cognitivos que en la práctica podrían dificultar una correcta implementación del actual sistema.

Por un lado, económicamente no es una decisión económicamente eficiente para el titular ni macroeconómicamente eficiente para la sociedad. McDonald encontró que el costo de leer políticas de privacidad para el ciudadano estadounidense promedio es de aproximadamente 244 horas anuales[88]. Lo que implicaría que, si todos los usuarios leyeran estas políticas, existiría una pérdida económica de unos $3,574 dólares per cápita o $781.000.000 anuales[89]. A esto hay que sumarle la creciente cantidad de servicios digitales, haciendo poco realista esperar que la mayor parte de los titulares pueda leer cada acuerdo de privacidad. Por otro lado, aún se encuentra presente el problema de la complejidad técnica, un reto que se agrava cada vez más con la constante disrupción tecnológica. Adicionalmente, al existir un peso tan importante sobre el consentimiento, el titular al ser presentado con tantas políticas de privacidad podría ver a estas como un simple ritual. A este problema Custers, *et al*. lo denominan como la fatiga del consentimiento, los autores explican que existe una desensibilización por parte del titular que no permite que el mismo realice un análisis objetivo[90].

En este sentido, es importante considerar como los retos planteados por la situación tecnológica actual no eran previsibles para el legislador. Cuando en Suecia se publicó una de las primeras leyes en materia de protección de datos en 1973, aún no existían computadores personales disponibles en el mercado y la información se almacenaba en dispositivos de cintas magnéticas, con pocos *megabytes* de almacenamiento. Hoy en día el desarrollo del *big data* ocasiona que a través de algoritmos altamente complejos y el uso

[87] Bert-Jaap Koops, "The trouble with European data protection law", 252.
[88] Aleecia M. McDonald, Lorrie Faith Cranor, "The Cost of Reading Privacy Policies". I/S: A Journal of Law and Policy for the Information Society 4 (2008), 18-19, Acceso el 5 de octubre de 2023, https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.
[89] Id., 19-20.
[90] Bart H. M. Custers, *et al*., "The role of consent in an algorithmic society. Its evolution, scope, failings and re-conceptualization" en *Research Handbook on EU data protection*, Editado por Eleni Kosta, Ronald Leenes, Irene Kamara (Cheltenham: Edward Elgar Publishing, 2022), 468.

cada vez más común de aprendizaje automático, nos encontremos con *black boxes*, las cuales según el reporte de The Royal Society, son sistemas que producen resultados altamente precisos, pero cuyos métodos para llegar a dichos resultados son realmente difíciles de interpretar[91]. Consecuentemente, no se puede trazar exactamente qué datos está utilizando el sistema y cómo los está interconectando.

Dentro del mismo reporte se consideran cuáles serían las condiciones necesarias para conseguir un correcto funcionamiento de un sistema con un alto grado de dependencia del consentimiento del titular. Según este reporte, se requiere de gente con el tiempo, conocimiento, y energía para poder otorgar este consentimiento[92]. Estos requisitos en ambientes altamente dinámicos hacen que la habilidad de los individuos para consentir se vea cada vez más reducida[93].

Por esto Koops considera que la autodeterminación informativa en el siglo XXI es una utopía, la forma en la que actualmente se realiza el procesamiento de datos vuelve insostenible al sistema actual[94]. El autor plantea que, en una situación simple, en la que un único responsable trata una cantidad relativamente pequeña de datos, con un fin claro, el titular puede entender todo el proceso, desde su inicio a fin[95]. Ahora bien, en la práctica se cuestiona cómo una persona podría ejercer su autodeterminación informativa. Koops plantea este reto ante las técnicas actuales que requieren de varios responsables que comparten datos, con operaciones automáticas cada vez más comunes, utilizando sistemas de perfilamiento y *cloud computing*, mismos que ni siquiera los responsables del tratamiento logran comprender en su totalidad[96].

La respuesta por parte de la LOPDP a estas problemáticas ha sido obligar al responsable a través del principio de transparencia a utilizar un lenguaje "claro y sencillo". Sin embargo, esta simplificación no siempre es posible. De hecho, Barocas y Nissenbaum demuestran que al buscar altos estándares de transparencia se genera una paradoja, ya que simplificar y aclarar los fines con los que se van a utilizar los datos en procesos complejos

[91] The Royal Society, "Chapter Five" en *Machine learning: the power and promise of computers that learn by example* (Londres: The Royal Society, 2017), 93.
[92] Id., 91.
[93] Id., 91.
[94] Bert-Jaap Koops, "The trouble with European data protection law", 252-253.
[95] Id., 252.
[96] Id., 252.

conlleva la perder información valiosa que y necesaria para que el titular tome una decisión informada[97].

Cabe resaltar que la dificultad de describir en términos simples procesos tecnológicos en una sociedad cada vez más compleja y especializada es constantemente más difícil. Por ejemplo, en el caso del *big data*, los autores describen al proceso como "ambientes complejos de *back-end* y redes con diversos componentes"[98]. Agregan que una descripción que permitiría entender lo que sucede sería compleja de entender incluso para personas con un alto grado de conocimiento informático, debido a que estas operaciones son volátiles e impredecibles, debido a que muchas veces es difícil constatar el valor de la información desde la fase inicial[99]. Por ejemplo, según datos del Consejo de Consumidores noruego, a través de únicamente 10 aplicaciones observadas, se transmitió datos a por lo menos 135 terceros dedicados a publicidad o perfilamiento[100].

La problemática del no leer y comprender los acuerdos de privacidad se ha visto también reflejada en los titulares. Según datos del *Pew Research Center*, alrededor de 6 de cada 10 ciudadanos estadounidenses no creen que es posible realizar actividades cotidianas sin que sus datos sean recolectados[101]. También se concluyó que el 59% de la población no sabe lo que las compañías hacen con sus datos personales[102]. Adicionalmente, el 25% de los encuestados respondió que diariamente se les solicita que acepten políticas de privacidad[103].

Al mismo tiempo se descubrió que el 81% de la población siente que los potenciales riesgos que enfrentan debido a la recolección de datos por parte de compañías implican más riesgos que beneficios[104], y apenas el 22% de la población dice que lee completamente las políticas de privacidad antes de aceptarlas[105]. En el caso de Europa, una encuesta del Reporte

---

[97] Solon Barocas, Helen Nissenbaum, "Big Data's End Run around Anonymity and Consent", 58-59.
[98] Id., 58.
[99] Id., 59.
[100] Andreas Claesson, Tor E. Bjørstand. "*Out of Control - A Review of Data by Popular Mobile Apps*", (Oslo: Norwegian Consumer Council, 2020), 83, Acceso el: 9 de octubre de 2023, https://storage02.forbrukerradet.no/media/2020/01/mnemonic-security-test-report-v1.0.pdf.
[101] Brooke Auxier, *et al*., "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*", Pew Research Center*, 2019, 2, Acceso el 9 de octubre de 2023, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
[102] Id., 27.
[103] Id., 37.
[104] Id., 2.
[105] Id., 5.

de Derechos Fundamentales demostró que solo 1 de cada 5 personas afirma que siempre lee las políticas de privacidad, de este grupo el 27% no las entiende[106]. Alrededor del 50% de los encuestados dijo que no era fácil otorgar su consentimiento[107]. Al tratarse de teléfonos móviles, el 72% de los encuestados dijeron que conocían cómo utilizar las configuraciones de privacidad en el dispositivo. Sin embargo, apenas el 41% conoce de las configuraciones para todas sus aplicaciones[108]. Finalmente, otro hallazgo importante en esta encuesta es que alrededor del 41% de la población no quiere compartir sus datos con empresas privadas[109]. Cabe resaltar que de acuerdo a Custers, *et al*. han existido propuestas en Europa para incluir mayor regulación desde el diseño, como opciones preconfiguradas dentro de los navegadores, pero estas nunca fueron incluidas[110]. Esto también se evidencia en la regulación ecuatoriana, debido a que no existe mayor desarrollo con respecto a las normas de privacidad por diseño y por defecto.

Ante todo esto, Barocas y Nissenbaum consideran que existe un problema que no se puede resolver a través del modelo regulatorio actual, debido a que el *big data* creado retos para la tradicional postura enfocada sobre el individuo[111]. En este sentido, para los autores el *big data* crea una "tiranía de la minoría"[112] Con esto se refieren a que "la información provista por pocos puede desbloquear la misma información de muchos"[113]. Los autores citan un estudio de Mislove *et al*. que demuestra que basta con que un 20% de usuarios revele su información para producir información de todo un grupo humano[114]. Los autores mantienen que este punto sumado a la paradoja de la transparencia convierte a la estrategia regulatoria actual en obsoleta[115]. En este sentido, para poder ejemplificar por qué

---

[106] European Union Agency for Fundamental Rights, "*Your Rights Matter: Data Protection and Privacy*" en FRA Fundamental Rights Report 2020 (Luxembourg: European Union Agency for Fundamental Rights, 2020), 9, doi:10.2811/292617.
[107] Id., 9.
[108] Id., 7.
[109] Id., 3.
[110] Bart H. M. Custers, *et al*., "The role of consent in an algorithmic society. Its evolution, scope, failings and re-conceptualization", 470.
[111] Solon Barocas, Helen Nissenbaum. "Big Data's End Run around Anonymity and Consent", 60-61.
[112] Id., 61, (traducción no oficial).
[113] Id., 61, (traducción no oficial).
[114] Mislove, *et al*. "You are who you know: inferring user profiles in online social networks", 251-260 en *WSDM '10: Proceedings of the third ACM international conference on Web search and data mining, 255, https://doi.org/10.1145/1718487.1718519*, citado en Solon Barocas, Helen Nissenbaumm, "Big Data's End Run around Anonymity and Consent", 62.
[115] Solon Barocas, Helen Nissenbaumm, "Big Data's End Run around Anonymity and Consent", 63-64.

el Big Data es un desafío para el consentimiento de mejor manera, podemos tomar al Internet de las Cosas como ejemplo.

6.1 Internet de las Cosas

Durante las primeras olas de la revolución digital, los avances se vieron por lo general constreñidos a un entorno propiamente digital. A través de redes de mejor calidad y poblaciones más conectadas, esta realidad ha ido cambiando. Hanes, *et al.* consideran que el Internet de las cosas, "*IoT",*

> […] se trata de conectar lo no conectado, permitiendo que objetos inteligentes se comuniquen con otros objetos inteligentes, sistemas y personas. El resultado final es una red inteligente que permite tener un mayor control sobre el mundo físico y la habilitación de aplicaciones avanzadas[116].

Existen distintos tipos de conexiones inteligentes, previo al *IoT,* las conexiones más avanzadas eran las experiencias inmersivas: éstas conectan videos, redes sociales, información en la nube e información de movilidad[117]. Por su lado, el *IoT* conecta personas, procesos, datos y objetos físicos[118]. Consecuentemente, sus aplicaciones son diversas, por ejemplo, al poder conectar vías, son fundamentales para el desarrollo e implementación de vehículos sin conductor[119]; Además tiene llamativos beneficios para las fábricas dado que puede mejorar procesos, seguridad y acelerar la introducción de productos en el mercado[120]. Puede incluso conectar animales con el propósito de mejorar procesos en el sector agrícola[121]. Su aplicación en casi todos los aspectos del mundo físico conlleva beneficios económicos importantes. Para el Instituto Global de McKinsey el IoT tiene el potencial de generar entre 3,9-11,1 trillones de dólares en valor económico para el año 2025[122].

---

[116] David Hanes, *et al*., "What is IoT?" en *IoT Fundamentals: Networking Technologies, Protocols and Use Cases for the Internet of Things* (Indianapolis: Cisco Press, 2017), 3.
[117] Id., 5-6.
[118] Id., 6-7.
[119] Id., 8-10.
[120] Id., 12-13.
[121] Id., 78-79.
[122] Mark Patel, Jason Shangkuan, Christopher Thomas, "What's new with the Internet of Things?" en *The Internet of Things: How to capture the value of IoT (Mckinsey&Company, 2018),* 115,

Estos beneficios van de la mano con retos que la regulación en materia de protección de datos tendrá que lidiar con cada vez más frecuencia. Para entender estos riesgos de mejor manera hay que partir desde el funcionamiento. Un objeto inteligente tiene el propósito de recolectar información para enviarla a través del internet para su potencial almacenamiento, procesamiento y análisis. La información recolectada es de importante valor para este campo dado que se utiliza frecuentemente para mejorar o introducir nuevos productos y servicios[123]. Por lo mismo, a la hora de adquirir un dispositivo inteligente, el aparato envía y recibe información constantemente. El *IoT* presenta más retos al consentimiento en tanto es capaz de recolectar información en tiempo real. Por ejemplo, un reloj inteligente es capaz de recolectar datos del titular durante todo el tiempo en el que está siendo usado, desde sus patrones de movimiento hasta información acerca de su salud. Su cada vez más amplia adopción implica una multiplicidad de sensores analizando varios tipos de información en un ambiente. Al mismo tiempo, la extensión de dispositivos y redes a espacios físicos lleva aún más problemas a la hora de informar al titular acerca de todo el procedimiento a realizarse con sus datos. El manejo de estos también se vuelve complicado, especialmente si se considera ambientes que pueden tener varios objetos interconectados.

Dado los pobres resultados evidenciados al momento de leer y comprender los términos y condiciones, es difícil esperar mucho de la autodeterminación informativa a la hora del manejo de los datos y a qué se consiente, más aún cuando no es posible entender los procesos que ocurren con los datos. Al no limitarse a un espacio digital, según Wachter, la interconexión en un mismo espacio de dispositivos de *IoT* permite vincular perfiles de un mismo usuario, incluso cuando su información ha sido anonimizada[124]. Esto podría implicar que el usuario no tenga conocimiento de todas las implicaciones que la recolección y tratamiento de los datos conlleva[125].

Así mismo se debe considerar que dentro de un ambiente estos dispositivos pueden captar información no solo del titular que otorgó su consentimiento, sino de cualquier

https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/the-internet-of-things-how-to-capture-the-value-of-iot.

[123] David Hanes, *et al*., "Chapter 7: Data and Analytics for IoT", 231.

[124] Sandra Wachter, "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR", *Computer Law & Security Review* 34(3) (2018), 10. Acceso el 18 de octubre de 2023. http://dx.doi.org/10.2139/ssrn.3083554.

[125] Id., 10.

persona que se encuentre dentro del rango de detección. En la práctica, podría existir un reto en cómo se informa a las personas que se encuentran cerca del dispositivo acerca de la recolección y tratamiento de sus datos personales, y cómo se les otorga control y acceso a los mismos de acuerdo con los requisitos establecidos. Un punto importante a considerar es la potencial ubicuidad de estos dispositivos. A diferencia de un servicio en línea donde la información se puede vincular a un usuario en particular, varios de estos dispositivos no cuentan con la capacidad de identificar a quién pertenece la información recolectada.

Para procesar dicha información se utilizan técnicas de aprendizaje profundo, algoritmos de IA entrenados para analizar datos y otorgar un resultado deseado[126]. Como se explicó previamente, hoy en día la complejidad que han tomado estos algoritmos es de tal grado que los propios desarrolladores no pueden entender por completo cómo funcionan. Esto también podría levantar una cuestión relacionada al diseño de esta tecnología. La nebulosidad y complejidad técnica de estos campos del conocimiento los vuelven el lugar ideal para aplicar distintas técnicas de diseño que permitan al controlador caer fuera del marco o plenamente evadir la regulación actual.

Existen también grandes desafíos para quienes ofrecen estos productos y servicios. Actualmente en la LOPDP no se prevén normas específicas para la regulación del *IoT*. Se optó por introducir conceptos que regulan la arquitectura de distintas soluciones tecnológicas desde el diseño y por defecto, buscando crear una protección *ex-ante* para el usuario. Así, se intentó crear condiciones más seguras y amigables para el titular. A pesar de esto, la implementación de estos conceptos es una difícil tarea en el campo del *IoT*. Como ya se ha mencionado, existe un problema con la identificación necesaria para el cumplimiento de una finalidad específica y la elaboración de perfiles. Para Wachter, existe una tensión entre la privacidad del usuario y tecnologías para identificar a un usuario y personalizar servicios debido a que los dispositivos de IoT requieren de interconexiones, personalización y sensores[127]. El segundo problema que la autora agrega, es que cuando se comparte información con terceros, los mismos podrían combinar su propia información con la adquirida para procesar estos datos con finalidades distintas a las que consintió el usuario, o

[126] David Hanes, *et al*., "Chapter 7: Data and Analytics for IoT", 212.
[127] Sandra Wachter, "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR", 13.

simplemente sin su consentimiento[128]. Es debido a esto que Eskens mantiene que en el ámbito de *IoT* se requiere de regulación específica, debido a que la tecnología empleada en estos ecosistemas de *IoT* ocasiona que la autodeterminación informativa no pueda funcionar en la práctica[129].

El crecimiento de la tecnología es exponencial, mientras que la regulación tiende a estar un paso atrás. En este sentido, el desarrollo del *big data* y el *IoT*, junto con la capacidad limitada de decisiones de los seres humanos y factores como el tiempo presentan importantes dificultades para el consentimiento y la autodeterminación informativa en la práctica. Adicionalmente a estos retos, un sistema como el actual podría tener consecuencias negativas en la innovación. Dentro del siguiente capítulo, se procederá a analizar las potenciales consecuencias de la regulación actual sobre el desarrollo de nuevas tecnologías, principalmente la Inteligencia Artificial.

7. Impactos de la estrategia regulatoria actual en la innovación tecnológica

La adopción de la LOPDP fue sin duda un importante paso que brindará un mayor nivel de protección al titular del que existía antes. Así mismo es importante considerar que al ser un país en vías de desarrollo, con un menor grado de conexión y avances tecnológicos, los retos que se presentan actualmente en Europa con relación al RGPD no eran previsibles, sin embargo, se ha visto en esta investigación, problemáticas que hace una década tomaron relevancia en Europa y Estados Unidos, hoy en día están creando retos para la regulación en ecuatoriana.

Las nociones tradicionales sobre las cuales se consideró que la autodeterminación informativa aún era posible en el siglo XXI, para bien o para mal ya no soportan el peso de la realidad tecnológica. La autodeterminación informativa, aunque ideal en teoría, ya no existe en la actualidad, o al menos de manera significativa. Debido a esto, Barocas y Nisenbaum consideran que el resultado es desfavorable ya que se mantienen normas que en

[128] Id.,7.
[129] Sarah Eskens, 2016, "*Profiling the European Consumer in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should it* ?", (Tesis de maestría. University of Amsterdam / Instituut voor Informatierecht), 72, https://dev.ivir.nl/publications/profiling-the-european-citizen-in-the-internet-of-things-how-will-the-general-data-protection-regulation-apply-to-this-form-of-personal-data-processing-and-how-should-it/.

la realidad no pueden ser aplicadas, y por lo mismo no son capaces de proteger al titular correctamente[130].

Otra posición que mantiene que la innovación puede verse truncada por normativas de este estilo es la de Janßen, *et al*. ya que demostraron que el RGPD tuvo efectos negativos significativos sobre la innovación posterior a su implementación alrededor de 33% de las aplicaciones salieron del mercado de aplicaciones de Google y los costos de desarrollo incrementaron[131]. Los autores escriben que esto es de especial importancia para el desarrollo de productos como las aplicaciones, debido a la incertidumbre que usualmente existe con respecto a su calidad o recepción en el mercado, haciendo que un incremento en costos de desarrollo tenga efectos importantes[132].

Un ejemplo concreto actualmente se puede observar en Italia con el famoso gran modelo de lenguaje, *LLM*, Chat GPT desarrollado por OpenAI, en marzo de 2023 Chat GPT fue suspendido, ya que existían dudas acerca de si la gran cantidad de datos que está recogiendo de cada usuario es legítima de acuerdo con el RGPD[133]. Al mismo tiempo, la eliminación de los datos recolectados es un reto. La tendencia en el desarrollo de los *LLM* ha sido la utilización de técnicas de recolección masivas de datos como el *web scraping*[134]. Adicionalmente, esto se puede ver en los sistemas de IA que ya interactúan con el usuario, como es el caso Chat GPT, pero con datos que son alimentados al sistema en tiempo real. Uno de los grandes motivos por los que los *startups* tecnológicos podrían tener grandes dificultades con este sistema son los costos. Según Melegati y Kon, los *startups*, al tener usualmente pocos recursos financieros, deben mantener una estructura mínima para mantener a la compañía en pie hasta llegar a su punto de equilibrio[135].

El problema fundamentalmente radica en que estos sistemas no están diseñados para olvidar los datos recolectados en las interacciones con el usuario. Al mismo tiempo,

---

[130] Solon Barocas, Helen Nissenabum, "Big Data's End Run around Anonymity and Consent", 60-61.
[131] Rebecca Janßen, *et al*., "GDPR and the Lost Generation of Innovative Apps*", National Bureau of Economic Research* Working Paper Series 30028 (2022), 36-37, Acceso el 21 de octubre de 2023, doi:10.3386/w30028.
[132] Id., 37.
[133] National Public Radio "ChatGPT is temporarily banned in Italy amid an investigation into data collection", National Public Radio, 2023. Acceso el 21 de octubre de 2023, https://www.npr.org/2023/03/31/1167491843/chatgpt-italy-ban-openai-data-collection-ai.
[134] Rishi Bommasani, *et al*, "On the Opportunities and Risks of Foundation Models" *ArXiv (2021)*, 12, Acceso el 21 de octubre de 2023, doi:10.48550/arXiv.2108.07258.
[135] Jorge Melegati, Fabio Kon, "Early-Stage Software Startups: Main Challenges and Possible Answers" en *Fundamentals of Software Startups: Essential Engineering and Business Aspects*, Editado por Anh Nguyen-Duc, *et al*., (Cham: Springer Nature Switzerland AG, 2020), 133.

debido a que muchos de estos *LLM* contienen *black boxes*, encontrar dicha información para borrarla es casi imposible. Patsakis, *et al*. a través de un estudio concluyeron que el uso de los *LLM* para la desanonimización de documentos puede tener un importante efecto negativo en términos de privacidad[136].

Uno de los retos que más urge considerar es el de las posibles limitaciones a los avances de la inteligencia artificial, dado que existe una tensión importante entre los regímenes que siguen el modelo del RGPD, estos buscan la minimización y pertinencia en la recolección de datos, mientras que los *LLM* requieren de cantidades enormes de información junto a interacciones con el usuario para poder ser entrenados y ofrecer mejores resultados.

A todo esto, se debe agregar que la recolección de datos no siempre puede tener un alto grado de precisión puesto que no se conoce el valor que los datos pueden tener para un fin, y esta es otra potencial limitación a la velocidad con la que se puede desarrollar la tecnología. Debido a la complejidad de sus algoritmos, los mecanismos necesarios para entrenarlos, y las particularidades de sus modelos de negocio, Hacker, *et al*. recomiendan se desarrolle regulación específica para el desarrollo y uso de los *LLM*[137].

Así mismo, Koops propone la creación de regímenes *sui generis* para distintos tipos de datos o regímenes para distintos tipos de problemas como el perfilamiento[138]. El autor agrega que en lugar de considerar qué son y no son datos personales en base a la posibilidad de identificar a una persona, se debería profundizar más sobre categorías de datos que tienen ciertos efectos sobre una persona cuando son procesados[139]. Para Koops otra potencial alternativa es la implementación de tecnología que brinde mayor privacidad al titular, minimizando riesgos para los titulares[140].

Al considerar que es posible delegar una carga tan importante a la autodeterminación informativa, el RGPD se construyó como una regulación neutral que no

---

[136] Constantinos Patsakis, Nikolaos Lykousas, "Man vs the machine in the struggle for effective text anonymisation in the age of large language models", *Scientific Reports* 13 (2023), 14, Acceso el 23 de octubre de 2023, doi:10.1038/s41598-023-42977-3.
[137] Philipp Hacker, Andreas Engel, Marco Mauer, "Regulating ChatGPT and other Large Generative AI Models", *FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, 12 de junio de 2023, 21, Acceso el 2 de noviembre de 2023, doi:10.1145/3593013.3594067.
[138] Bert-Jaap Koops, "The trouble with European data protection law", 260.
[139] Id., 260.
[140] Id., 261.

buscó regular a cada tecnología específicamente sino principalmente la relación con el titular. Esto es contrario a la realidad tecnológica actual. Como ya se mencionó, varios autores que analizan los potenciales retos que la IA y el *IoT* pueden representar para la regulación en esta materia creen que, en vista de las importantes implicaciones de sus particularidades técnicas y prácticas, debe existir una regulación específica.

Para Koops la regulación también debería ser multidisciplinaria, ya que es posible cubrir algunos supuestos con otras ramas del derecho, por ejemplo, regulando el perfilamiento y las decisiones automatizadas a través del derecho de protección del consumidor[141]. Finalmente, dado que las prácticas actuales de procesamiento de datos dejan poco lugar en la práctica para los principios de minimización, finalidad y confidencialidad, Koops afirma que se debería hacer un fuerte énfasis en la transparencia de las decisiones que se toman en base al procesamiento, con respecto a esto, el autor escribe que:

> "Esto implica una estrategia en dos sentidos: en primer lugar, disminuir la transparencia hacia arriba, mediante el blindaje y la ofuscación de los datos, y segundo, mejorar la transparencia hacia abajo con la introducción de mecanismos para la transparencia de resultados y procesos, transparencia retrospectiva en (casi) tiempo real para casos individuales, y, sobre todo, transparencia efectiva (no únicamente nominal). Para esto se requieren receptores que sean capaces de comprender y utilizar la información transparente[142].

Hartzog, por otro lado, afirma que, la normativa debería brindar mayor profundidad con respecto a normas acerca del diseño de la tecnología, ya que las tecnologías que no brindan seguridad al titular limitan la confianza del mismo[143]. Para este autor la regulación basada en el diseño de la tecnología se puede utilizar como una solución para cambiar los incentivos, costos transaccionales y señalizaciones con el fin de crear confianza entre el titular, el responsable y el usuario[144]. Se puede observar entonces que un importante beneficio de estos sistemas es que se encuentran fundamentados en que los seres humanos

---

[141] Id., 260.
[142] Bert-Jaap Koops, "On decision transparency, or How to Enhance Data Protection After the Computational Turn" en *Privacy, Due Process and the Computational Turn: The philosophy of law meets the philosophy of Technology*, Edición de Mireille Hildebrandt, Katja de Vries, 196-220, (Oxford y Nueva York: 2013), 16, Acceso el 3 de noviembre de 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2367510, (traducción no oficial).
[143] Hartzog, "*A Design Agenda for Privacy Law*", 104-105.
[144] Id., 118-119.

no pueden comprender todo a su alrededor, ni tomar decisiones infinitas, pero en que la colaboración entre distintas partes sí es posible cuando existe confianza.

8. Conclusión y recomendaciones

Todo lo expuesto hasta el momento no quiere decir que no existan aspectos positivos detrás de la introducción de la LOPDP. Es sin duda un gran acierto en tiempos en donde terceras partes tienen acceso a cada vez más ámbitos del día a día. Sin embargo, es extremadamente importante alivianar la carga que se ha colocado sobre el individuo con alternativas que ofrezcan un mayor grado de protección. Cabe también mencionar que esto no implica que el consentimiento ya no tiene lugar, ya que correctamente implementado es una buena herramienta para que el titular esté consciente y comprenda lo que implica el tratamiento de sus datos siempre y cuando logre comprender de una manera ajustada a la realidad cómo se tratan sus datos y las implicaciones que esto conlleva.

El sistema regulatorio adoptado por Ecuador se deriva casi en su totalidad del RGPD europeo. Durante esta investigación se ha podido evidenciar que la situación tecnológica actual crea importantes desafíos para regulaciones que colocan a la autodeterminación informativa y al consentimiento como piedra angular para la recolección y tratamiento de datos personales. Cabe mencionar que no se estima un problema con la figura del consentimiento *per se*, sino con la estrategia regulatoria utilizada para los avances tecnológicos del siglo XXI. La enorme carga que la regulación actual impone sobre el titular, hace que el mismo carezca de una protección adecuada y genera el riesgo de que con cada vez más frecuencia se considere a los acuerdos de privacidad como rituales sin sentido, erosionando la importancia que las personas le dan a sus datos y por lo mismo a su privacidad.

En primer lugar, se encuentra la comprensión, control y decisión que el titular puede tener sobre el tratamiento de sus datos. Debido a tecnologías cada vez más complejas y ubicuas, no es posible simplificar las implicaciones del tratamiento de datos a tal punto que la mayor parte de la población pueda comprenderlo. Pero incluso en el hipotético de que se pudiera simplificar a tal punto, la fatiga cognitiva y el tiempo requerido para hacerlo están generando que el consentimiento que el titular otorga se convierta en un acto sin sustento ni sentido, únicamente un "*check in a box*". Al mismo tiempo, existe una falta de regulación

específica para tecnología como el IoT que no puede ser resuelta por la normativa actual acerca de la privacidad desde el diseño y por defecto.

En segundo lugar, si bien se han establecido requisitos en la LOPDP para precautelar la autodeterminación informativa y facilitar el consentimiento del usuario, estos no son completamente aplicables a la realidad operativa de las compañías, ya que incrementan los costos de desarrollo y dificultan la innovación tecnológica. De modo que nos encontramos ante una norma que, al estar enfocada desde una perspectiva desconectada de la realidad tecnológica, no logra cumplir con sus propósitos y relentece los avances tecnológicos, volviendo menos competitivos a países que se han decidido enmarcar dentro de esta tendencia regulatoria.

Como siempre es el caso, existieron limitaciones en el desarrollo de este trabajo. En primer lugar, al no existir aún una autoridad competente en esta materia, el régimen sancionatorio establecido en la Ley y el Reglamento, se encuentra vigente pero no es aplicable; adicionalmente, aspectos como la absolución de consultas en materia de protección de datos personales, funciones de supervisión y control, así como el desarrollo de normativa secundaria, se encuentran pausados hasta la creación de la Superintendencia de Protección de Datos Personales y la designación de su titular. Al mismo tiempo, la extensión del mismo no permitió analizar con mayor profundidad las alternativas ante este modelo regulatorio, especialmente con respecto a la regulación desde el diseño.

Se recomienda abordar la problemática actual permitiendo a las empresas auto regularse a través de códigos de la industria para tecnologías que lo ameriten, como por ejemplo el IoT, especialmente en el caso de regulaciones para tecnologías específicas. Esto se debe a que los proveedores de soluciones tecnológicas tienen mayor información del estado actual de su sector. Fomentar la participación de distintas industrias también permite a los reguladores mantenerse actualizados y conocer las necesidades de cada sector. Por otro lado, la regulación desde el diseño podría eliminar algunos de los retos presentados a los individuos. Por ejemplo, la propuesta de implementar navegadores con políticas de privacidad preconfiguradas para todas las páginas web a las que una persona contrarrestarían el problema del tiempo necesario para leer políticas privacidad, el de la paradoja de la transparencia y el de la fatiga cognitiva. Únicamente tomando en cuenta el estado de la

tecnología actual, y regulando en función de esto es posible brindar una protección adecuada al titular y facilitar el desarrollo tecnológico.