

Sobre el debate relativo al proyecto de ley de protección de datos personales (el “Proyecto”), que se encuentra en consideración de la Comisión de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral y el pleno de la Asamblea Nacional de Ecuador, desde las organizaciones Derechos Digitales, Asociación para el Progreso de las Comunicaciones y Access Now compartimos un análisis actualizado del texto propuesto por la Comisión, conforme a la experiencia internacional en la materia de las organizaciones que representamos. Identificamos las disposiciones respecto de las cuales consideramos que existe necesidad de mejora, en orden a satisfacer mejor el objetivo de la norma propuesta de alcanzar una protección efectiva en el Ecuador del derecho a la autodeterminación de su ciudadanía.

1. **Ámbito de aplicación material: exclusiones**

En el **Artículo 2** (*Ámbito de aplicación material*) se señalan aquellos tratamientos de datos a los cuales la futura ley no aplicaría, entre los cuales se encuentran los datos anonimizados (letra c). Dadas las reiteradas referencias a esta hipótesis de exclusión en el Proyecto y para evitar potenciales futuros conflictos de interpretación respecto de esta hipótesis, se sugiere señalar expresamente que la misma sólo resulta aplicable en la medida que los datos continúen siendo anónimos. En otras palabras, que se aclare que en cualquier caso desde el momento en que se realice una re-identificación del titular de los datos, su tratamiento volverá a estar sujeto al cumplimiento de la ley de protección de datos, incluido el requisito de contar con una base de licitud para continuar tratando los datos de manera no anonimizada.

Otro de los casos que quedaría fuera del ámbito de aplicación del Proyecto sería el de aquellos referidos a *“Datos personales cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado”* (letra e).

Dada la amplitud de los términos utilizados, creemos necesario acotar esta hipótesis agregando la obligación de cumplir con estándares internacionales de derechos humanos y los principios contenidos en la ley en discusión, o a los menos hacer referencia a los criterios de legalidad, proporcionalidad y necesidad, para limitar excepcionalmente la aplicación de la normativa general en la ley propuesta. Al tratarse de una ley que reglamenta el ejercicio de un derecho fundamental, corresponde la aplicación del test tripartito conforme a la jurisprudencia del Sistema Interamericano de Derechos Humanos donde se ha señalado que: “Toda limitación al derecho a la vida privada, incluido el derecho a no ser objeto de injerencias arbitrarias o abusivas en las comunicaciones, debe superar el test de legalidad, proporcionalidad y necesidad establecido por la propia Convención y reafirmado por la Corte.”¹

Por su parte, en relación al literal f) del mismo artículo, el texto actual genera potenciales ambigüedades de interpretación en cuanto a si este se refiere a las bases de datos con los

¹Corte IDH. Caso Fontevecchia y D’Amico vs. Argentina. Sentencia de 29 de noviembre de 2011. Fondo, Reparaciones y Costas. Serie C No. 238, y Corte IDH. Caso Escher vs. Brasil. Sentencia de 6 de Julio de 2009. Fondo, Reparaciones y Costas. Serie C No. 200. Estándares para una Internet libre, abierta e incluyente / Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. (2017) OEA/Ser.LV/II CIDH/RELE/INF.17/17, párrafo 193.

indicados propósitos a cargo de los organismos estatales con competencia legal para “la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales”, o si bases de datos que privados pudieran establecer para tales objetivos pudieran quedar amparadas en la excepción, con lo cual creemos recomendable agregar una oración que delimite su sentido y alcance a los organismos estatales con competencia legal para las funciones enumeradas.

Los problemas respecto de las limitaciones del ámbito de aplicación consideradas se repiten luego, en el Capítulo III del proyecto (*Derechos*), en el cual encontramos otros dos Artículos referidos a determinados ámbitos que quedarían excluidos de la aplicación del Proyecto:

El **Artículo 11** (*Normativa especializada*), que pese a su título, **también se refiere a determinados tratamientos que quedarían excluidos** de la aplicación de la ley de datos personales, extendiendo la hipótesis de exclusión de aplicación de la ley. Sin embargo, a diferencia del artículo anterior, ahora no en razón de sus “tratamientos” sino en razón a la categoría de “datos” - *cuyo tratamiento se encuentre regulado en normativa especializada*. En relación a este artículo resultan pertinentes las siguientes observaciones de mejora:

- a. Como correctamente se establece en el Artículo 2, el Proyecto, la norma en discusión tiene por objetivo regular el tratamiento de datos personales, con lo cual para proveer de claridad en técnica legislativa utilizada, ello debiera mantenerse en forma consistente a lo largo del proyecto, y así enfocarse en las excepciones pertinentes a determinados tratamientos, más que a excepciones aplicables a categorías completas de datos.
- b. Este artículo no sólo repite algunas de las hipótesis que ya se encontrarían excluidas del ámbito de aplicación de la ley en virtud del Artículo 2, sino que además agrega otras adicionalmente problemáticas, entre ellas la de “*los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes*

amparadas en competencias atribuidas en la normativa vigente”. En relación a esto último, resulta preocupante que la normativa y principios propuestos en el Proyecto no sea aplicable a los datos que deban proporcionarse a *autoridades administrativas* en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente, especialmente considerando la experiencia comparada (v.gr.: Chile) en que autoridades administrativas han terminado haciendo un tratamiento intensivo de datos personales en virtud de normas reglamentarias sin control de ningún tipo, incluso amparadas en disposiciones más restrictivas que la que aquí se propone.

- c. Por último, no se explica por qué los datos *cuyo tratamiento se encuentre regulado en normativa especializada* quedarían sujetos sólo a algunos de los principios del Proyecto y no necesariamente a los principios de pertinencia y minimización; proporcionalidad; calidad y exactitud; aplicación favorable al titular; e independencia del control.

Resulta imperioso que la disposición sea enmendada para eliminar tal excepción amplia otorgada a las autoridades administrativas, o alternatively se exija que esas excepciones satisfagan al menos los principios de la ley en comento y sean compatibles con el estándar de legalidad, proporcionalidad y necesidad enunciado por el Sistema Interamericano de Derechos Humanos citado anteriormente.

Por su parte, el **Artículo 27 (Excepción por normativa especializada)**, se refiere más específicamente a la improcedencia de los derechos establecidos en el Proyecto, *para los datos personales cuyo tratamiento se encuentre regulado en (la) normativa especializada que el mismo artículo detalla.*

Al respecto cabe señalar que aún cuando las reglas de tratamiento no fueren aplicables, no parece lógico limitar la exigibilidad de los derechos que son manifestación del derecho fundamental a la protección de datos personales.

Por último, por motivos de coherencia legislativa, lo recomendable sería que el contenido de los tres artículos señalados quede regulado en el Capítulo I, especialmente considerando que los tres se refieren directa o indirectamente a las exclusiones del Proyecto, y que el Artículo 11 en ningún caso se refiere a los derechos de los titulares.

En virtud de lo anterior sugerimos las siguientes modificaciones:

1. Agregar al final de la letra c) del Artículo 2, una coma, seguida del siguiente texto: *“en tanto no sea posible identificar a su titular. Tan pronto los datos dejen de estar disociados o de ser anónimos, su tratamiento estará sujeto al cumplimiento de las obligaciones de esta ley, especialmente la de contar con una base de licitud para continuar tratando los datos de manera no anonimizada o disociada.”*
2. Agregar al final de la letra e) del Artículo 2, un punto seguido del siguiente texto: *“en cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad.”*
3. Agregar al final de la letra f) del Artículo 2, una coma seguida del siguiente texto: *“llevado a cabo por los organismos estatales competentes en cumplimiento de sus funciones legales. En cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad.”*
4. *Eliminar Artículos 11 y 27.*

2. **Ámbito de aplicación territorial**

En relación al **Artículo 3 (Ámbito de aplicación territorial)** del Proyecto, el texto de su numeral (3) resulta bastante confuso dada la sobre referencia a “personas residentes en el territorio nacional”, no quedando claro cuál sería, en definitiva, el ámbito de aplicación territorial. Es por esto que sugerimos la siguiente redacción alternativa:

5. Reemplácese el numeral (3) del Artículo 3, por el siguiente:
“El responsable o encargado del tratamiento de datos personales, que no se encuentre domiciliado en Ecuador, oferte bienes o servicios dentro de Ecuador; o realice actividades relativas a la recolección de datos personales de personas residentes en el territorio nacional; y”

3. Fuente accesible al público

En el **Artículo 4 (Términos y definiciones)** se definen las **fuentes accesibles al público** de manera excesivamente amplia y ambigua, cuestión que en otros países (v.gr.: Chile) ha generado un problema interpretativo relevante respecto a bajo qué circunstancias una fuente de datos que puede ser consultada libremente, puede ser legítimamente considerada una fuente accesible al público, o no, para los efectos de la protección de datos personales. Al no estar delimitado el concepto, se puede dar como ejemplo el caso de que la base de datos sea publicada ya sea por error o de forma ilícita en un lugar público, por ejemplo una filtración de datos personales obtenidos ilícitamente que se pone a disposición en Internet sin consentimiento de los titulares de los datos, dando pie a que exista un tratamiento masivo de dichos datos sin que ellos hayan sido obtenidos legítimamente a través de consentimiento de sus titulares o satisfagan el principio de finalidad conforme al cual ellos pudieron haber sido entregados originalmente.

Como antecedente adicional, debe tenerse en consideración que en el **numeral 7 del Artículo 7 (Tratamiento legítimo de datos personales)** se establece que el *tratamiento de datos personales que consten en bases de datos de acceso público*, será considerado legítimo y lícito, sin importar la finalidad con que el dato sea tratado, en circunstancias que el tratamiento de datos personales contenidos en este tipo de fuentes siempre debiese estar condicionado al hecho que dicho tratamiento respete la finalidad con que los datos de dicha fuente fueron recogidos.

Por último, cabe señalar que el **Artículo 32** del Proyecto (*Datos relativos a la salud*) establece un deber de confidencialidad respecto de los datos de salud “Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos de salud, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales relativos a la salud, *están obligadas a guardar confidencialidad sobre éstos, cuando hayan sido recogidos de*

fuentes no accesibles al público”. En otras palabras, si los datos de salud fueran recogidos de fuentes accesibles al público no habría tal deber de confidencialidad, cuestión que sólo tendría sentido en caso de un concepto acotado de fuentes accesibles al público, que evitara, por ejemplo, una mala utilización de datos de salud filtrados y puestos a disposición públicamente de forma ilícita (sin consentimiento de su titular u otra disposición legal habilitante).

En virtud de lo anterior, resulta imprescindible acotar la definición de “fuentes accesibles al público” para prevenir serios inconveniente interpretativos. Al efecto, proponemos la siguiente redacción alternativa:

6. Reemplazar la definición de fuentes accesibles al público contenida en el Artículo 2 del Proyecto actual, por la siguiente:

“todas aquellas bases de datos o conjuntos de datos personales, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, siempre que no existan restricciones y/o impedimentos legales para su acceso o utilización, entre ellos infracción al principio de finalidad, tales como listas de colegios profesionales, diario oficial, medios de comunicación, los registros públicos que disponga la ley, entre otros.”

4. Bases de licitud para el tratamiento de datos personales

En el **Artículo 7 (Tratamiento legítimo de datos personales)** se establecen las bases de licitud en virtud de las cuales el tratamiento de datos personales será considerado legítimo y lícito.

Si bien el tratamiento de datos personales sobre otras bases de legitimidad distintas del consentimiento es reconocido ampliamente en el derecho comparado, asimismo se ha establecido la necesidad de que ellas sean precisa y adecuadamente definidas para evitar su abuso, y con ello vaciar de contenido al principio del consentimiento para el tratamiento de datos personales como regla general.

Es por ello que en relación a dos de los numerales contemplados en esta disposición creemos necesario acotar su alcance mediante las siguientes complementaciones a la redacción:

7. Agregar al final del numeral (4) del artículo 7 del Proyecto, el siguiente texto: “*y en todo caso sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad;*”
8. Agregar al final del numeral (8) del artículo 7 del Proyecto, el siguiente texto: “*cuestión esta última que, en caso de disputa, corresponderá al Responsable acreditar*”.

Por último, hacemos presente que en caso que no se modifique la actual definición de “fuentes accesibles al público” contenida en la versión actual del Proyecto, como hemos propuesto anteriormente, sería necesario modificar también el numeral (7) del artículo en comento, que establece como base de licitud el tratarse de datos personales que consten en bases de datos

de acceso público, sin condicionar dicho tratamiento al respecto al cumplimiento del principio de finalidad para el cual fueron recogidos dichos datos.

5. Consentimiento

El **Artículo 8** dispone que el consentimiento será válido cuando el mismo reúna las condiciones de libre, específico, informado e inequívoco mientras que el **Artículo 29** referido al consentimiento relativo a categorías especiales de datos estipula la necesidad de que el consentimiento sea expreso. De esta forma podría interpretarse la existencia de dos tipos de consentimiento lo cual es incorrecto dado que el requisito de expreso subyace a las condiciones de libre, específico, informado e inequívoco.

Esta forma de consentimiento es la adoptada por los modernos estándares en materia de protección de datos, por ejemplo en el Reglamento General de Protección de Datos Personales de la Unión Europea el cual dispone: “*El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal.*”

Por lo expuesto sugerimos la siguiente modificación:

9. *Eliminar Artículo 29.*

6. Derechos

En el **Artículo 12 (Derecho a la información)** se enumera aquella información que el titular de datos personales tiene derecho a conocer de parte del responsable, entre ellas, la siguiente:

7) *Otras finalidades y tratamientos ulteriores;*

11) *El carácter imprescindible o facultativo de las respuestas y consecuencias de proporcionar o no sus datos personales;*

En relación al número 7, no queda suficientemente clara la redacción propuesta en función de los objetivos que parece pretender alcanzar, dado que conforme a las disposiciones anteriores de la misma ley, todas las finalidades con que se contempla tratar los datos personales deben ser informadas al momento de solicitar el consentimiento, con lo que la hipótesis quedaría repetitiva respecto de la incluida en el numeral 1. En caso de que se tratara de una finalidad que se agrega posteriormente, y que no fue contemplada al momento de la recolección de los datos, tendría que haber sido solicitado un complemento del consentimiento original, o tratarse de un tratamiento amparado en el tratamiento legítimo del artículo 7, que tiene reglamentación de información específica en el inciso tercero del mismo artículo, de manera que el numeral 7) estaría de más.

Por su parte, la redacción del numeral 11 podría inducir a equívocos respecto de la obligación de entrega de determinados datos, cuando aquello que se busca es información precisa

respecto a las consecuencias de la entrega o no, siempre voluntaria, de datos personales específicos.

En virtud de lo anterior se proponen las siguientes modificaciones:

10. Eliminar el actual numeral 7 del Artículo 12 del Proyecto.

11. Reemplazar el actual numeral 11 del Artículo 12 del Proyecto, por el siguiente: “Las consecuencias para el titular de los datos personales de su entrega o negativa a ello;”

12. Sustituir el inciso tercero por el siguiente:

“Cuando los datos personales no se obtuvieren de forma directa del titular o fueren obtenidos de una fuente accesible al público el titular deberá ser informado dentro de los siguientes treinta (30) días o al momento de la primera comunicación con el titular, cualquiera de las dos circunstancias que ocurra primero. Se le deberá proporcionar información expresa, inequívoca, transparente, inteligible, concisa, precisa y sin barreras técnicas”

En el **Artículo 13** se establece el **derecho de acceso** que tienen los titulares, esto es, el derecho de acceder, de forma gratuita, a su información que está siendo tratada.

Este es sin duda un derecho esencial del derecho a la autodeterminación informativa, constituyéndose en parte de su núcleo esencial. Es imposible ejercer cualquiera de los demás derechos que suelen otorgar las leyes de protección de datos personales sin el derecho a confirmar si los datos personales están siendo tratados o no, y en caso afirmativo qué datos están siendo tratados.

Sin embargo, el inciso final del artículo en comento limita este derecho al establecer en su inciso final que *“El derecho de acceso no podrá ejercerse de forma tal que constituya abuso del derecho.”*

Dicha limitación podría terminar por vaciar de contenido a este derecho, afectando su aplicación al prestarse como potencial excusa a ser utilizada por los responsables para negarse ante solicitudes de acceso de los titulares, bajo el pretexto de estar ejerciendo de forma abusiva.

Para superar el problema anterior, existen distintas soluciones posibles, por ejemplo, que sea la autoridad de datos la encargada de calificar si una solicitud de acceso constituye o no abuso de derecho; establecer cobros para las solicitudes de acceso que sean ejercidas dentro de un período inferior a un determinado período de tiempo; o dejar que sean los responsables quienes determinen si negar el acceso o cobrar por él cuando consideren que las solicitudes son infundadas o excesivas, pero obligando a este último a demostrar que la solicitud es infundada o excesiva. En cualquier evento, sugerimos eliminar la limitación por abuso del derecho contemplada actualmente en el proyecto, y evaluar la procedencia de alguna de las soluciones alternativas aquí propuestas.

El **Artículo 16**, referido al **derecho al olvido digital**, constituye una institución de suyo problemática en el mundo, y cuya compatibilidad con el sistema interamericano de protección de derechos humanos que proscribía la censura previa en el Artículo 13 de la Convención

Americana de Derechos Humanos, no resulta clara. Es por ello que nuestra recomendación es la eliminación de este artículo de la ley en discusión para mantener su coherencia y consistencia con los compromisos internacionales de derechos humanos adoptados por el Ecuador.

Ahora bien, en caso que la disposición se mantenga, creemos imprescindibles al menos las modificaciones de la misma que se sugieren a continuación. La redacción propuesta en el Proyecto, correctamente somete la cuestión de su aplicación a una decisión judicial sin embargo, no señala cual sería el tribunal competente para resolver estas solicitudes. Considerando que la protección de datos personales es un derecho fundamental reconocido por la Constitución Política de Ecuador y tratados internacionales de derechos humanos, creemos recomendable que el mismo tribunal con competencia para conocer de asuntos relacionados con derechos fundamentales sea el que conozca esta clase de solicitudes, especialmente considerando la necesaria ponderación de conflictos entre derechos fundamentales implícitas en una regulación de este tipo.

Ahora bien, por otra parte otro problema concreto que se aprecia en el artículo 16 es que este hace referencia a “**datos personales que estén siendo tratados en el entorno digital**”. Dicha expresión es extremadamente amplia, pudiendo incluir información contenida en un blog, un post en Facebook o Instagram, una opinión en Twitter, medios independientes, publicaciones académicas, etc. Dado lo anterior, lo más lógico pareciera ser acotar esta materia a la desindexación, que es aquello que se ha contemplado en los casos que se ha regulado este derecho como es el caso más saliente por la Unión Europea.

Por otra parte, en concordancia con lo antes señalado, dada la dudosa compatibilidad de la consagración de este derecho con el artículo 13 de la Convención Americana de Derechos Humanos, si en definitiva se opta por mantener este derecho dentro de la ley propuesta, este debiera quedar condicionado como criterios de procedencia conjunta a que: (i) el titular de los datos que busca ejercerlo acredite que existe una grave afectación en el ejercicio de sus derechos fundamentales, y (ii) que la eliminación del contenido de que se trate no afecte derechos fundamentales de terceros.

Por último, en el último inciso se señala que un reglamento establecerá los parámetros de aplicación, por los fundamentos antes expresados, no parece conveniente considerando que aquí se está regulando el ejercicio de un derecho fundamental, cuestión que no debiese ser objeto de regulación por una norma de rango infralegal.

13. Eliminar el Artículo 16 del Proyecto, o alternatively, reemplazar el texto actual del Artículo 16 del Proyecto, por el siguiente:

Cuando exista una grave afectación en el ejercicio de sus derechos fundamentales causado por la publicación de datos personales, el titular tiene el derecho a solicitar al juez competente, obtener sin dilación indebida del responsable de un motor de búsqueda en internet la desindexación de las publicaciones que contengan sus datos personales en el entorno digital, cuando concorra alguna de las circunstancias siguientes:

- 1) *Los datos personales sean de carácter obsoleto;*
- 2) *Los datos personales no tengan valor histórico o científico;*
- 3) *Los datos personales no sean de relevancia pública; o,*
- 4) *Los datos personales sean inadecuados, impertinentes o excesivos con relación a los fines y al tiempo transcurrido.*

La desindexación no procederá cuando ella afecte el ejercicio de derechos fundamentales de terceros.

Por último, en relación al **Artículo 19 (Derecho a la portabilidad)**, la redacción de la parte final de su numeral 1) no es del todo clara en cuanto a si el hecho de no ser técnicamente posible una transferencia o comunicación de datos implica que la misma podría no ser realizada por parte del responsable, o sólo que no podría ser realizada de un responsable a otro responsable. Entendemos que el sentido auténtico de esta norma es el último, pero para evitar futuros problemas interpretativos se sugiere la siguiente complementación:

14. Agregar al final del numeral 1) del Artículo 19, lo siguiente: “*en caso contrario los datos deberán ser transmitidos directamente al titular*”.

Finalmente, solo para los casos del derecho al acceso, a la eliminación y de consulta se consagra la **gratuidad** de su ejercicio. Sugerimos la incorporación de un artículo especial que disponga tal condición para el ejercicio de todos los derechos o que sea incluido específicamente en el derecho a la oposición, a la rectificación y actualización, nulidad y portabilidad.

7. Excepciones a los derechos de los titulares

En el **Artículo 20** se enumeran los casos en que no serían procedentes los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad.

Un primer problema de esta norma es que se agrupan la mayoría de los derechos (con la sola excepción del derecho de acceso) haciendo aplicable a todos ellos las mismas excepciones, siendo que difieren entre sí tanto desde el punto de vista de su naturaleza como de sus objetivos, y por lo tanto lo lógico sería que tuvieran causales de excepción distintas.

Sin perjuicio de lo anterior nos limitaremos a señalar las principales observaciones que merece este artículo, según el numeral de que se trate:

En relación al **numeral 5)**, que señala como caso de excepción “*Cuando se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros;*” surgen varias dudas, entre ellas las siguientes: ¿Cómo se acredita la concurrencia de esta circunstancia? ¿En quien descansa la carga de la prueba? ¿Es posible aplicar esta misma hipótesis como excepción a todos los derechos?).

En relación al **numeral 9)**, que señala como caso de excepción “*En los casos en los que medie el interés público;*” se vacía completamente el contenido de las disposiciones que establecen los derechos respecto de organismos públicos, que resultan propensos de acuerdo a la legislación comparada a invocar el interés público para restringir el ejercicio de derechos de la ciudadanía.

Para evitar futuros problemas interpretativos de esta disposición que vacíen de contenido el ejercicio de derechos por los titulares de datos personales, se sugieren las siguientes complementaciones:

11. Agregar en el numeral 9), luego del punto y coma, lo siguiente: “y ello sea acreditado por el Responsable de la base de datos al momento de dar respuesta al titular a su solicitud de ejercicio del derecho respectivo;”.
12. Agregar en el numeral 9), luego del punto y coma, lo siguiente: “y *en todo caso sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad;*”.

8. Decisiones basadas en valoraciones automatizadas

Los Artículos 22 y 23 del Proyecto abordan la regulación del derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas, el primero para todo tipo de datos

personales y el segundo, para el caso de categorías especiales de datos. En ambos casos debe incorporarse las valoraciones parcialmente automatizadas de forma de evitar que una mínima intervención humana evite que las normas se apliquen.

En relación al **Artículo 22** consideramos que en materia de informaciones que pueden ser demandadas por el titular de los datos, debiera agregarse la especificación de los tipos de datos y fuente de la cual han sido obtenidos los mismos, y no tan solo los criterios de valoración del sistema mismo, ya que los resultados pueden variar grandemente atendida la calidad de los datos utilizados al efecto.

Por otra parte, atendidas las exclusiones amplias consideradas en la disposición al ejercicio del derecho en el numeral 1 (relación contractual) y 3 (consentimiento del titular) del inciso segundo del artículo, a fin de evitar que la disposición se vacíe de contenido y aplicación práctica, sería adecuado incluir en este artículo la exigencia de que el consentimiento sea explícito además de una prohibición de exigencia de renuncia en contratos de adhesión masivos. Adicionalmente, resultaría conveniente reforzar la obligación de información al titular de los datos sobre la implementación de toma de decisiones por el Responsable basadas únicamente en valoraciones automatizadas.

En cuanto al **Artículo 23**, creemos que al tratarse de categorías de datos sensibles y de datos de niñas, niños y adolescentes, debiera excluirse por regla general su uso para la realización de valoraciones automatizadas, con la sola excepción de concurrencia de un interés público, definido en forma más completa y alineada a los estándares internacionales de derechos humanos, que aquella redacción actualmente contemplada.

13. Modificar el título y el cuerpo del Artículo 22 de la siguiente forma: “Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas. - El titular tiene derecho a no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de procesos automatizados..”

14. Intercalar, en el Artículo 22 a continuación del literal c), el siguiente literal:

d) Solicitar al responsable información sobre los tipos de datos utilizados y la fuente de la cual han sido obtenidos los mismos; o”

15. Agregar al Artículo 22 numeral 3 a continuación de la palabra consentimiento:

“explícito.”

16. Agregar el siguiente inciso final al Artículo 22:

“No se podrá exigir la renuncia a este derecho en forma adelantada a través de contratos de adhesión masivos”. A más tardar en el momento de la primera comunicación con el titular de los datos personales para informar una decisión basada únicamente en valoraciones automatizadas, este derecho le será informado explícitamente por cualquier medio idóneo.”

17. Reemplazar el Artículo 23 por el siguiente:

“Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas en categorías especiales de datos. No se podrán tratar datos sensibles o datos de niñas, niños y adolescentes, a menos que dicho tratamiento esté destinado a

salvaguardar un interés público esencial, el cual se evalúe en atención a los estándares internacionales de derechos humanos, y como mínimo satisfaga los criterios de legalidad, proporcionalidad y necesidad, y además incluya salvaguardas específicas para proteger los derechos fundamentales de los interesados.”.

9. Categorías especiales de datos

Datos crediticios

El **Artículo 31** se refiere a la posibilidad de comunicar este tipo de datos, pero no establece un límite para ello, aún cuando los mismos puedan referirse a deudas pagadas o extinguidas por otros medios. En virtud de lo anterior se sugiere la siguiente complementación:

18. Agregar el siguiente inciso final al Artículo 31:

“Sin perjuicio de lo anterior, en ningún caso podrán comunicarse los datos crediticios relativos a obligaciones de carácter económico, financiero, bancario o comercial después de haber sido pagadas o extinguidas por otro modo legal, ni una vez transcurridos cinco años desde que la obligación a la que se refieran se haya hecho exigible”.

Datos relativos a la salud

En relación al **Artículo 32**, se sugiere limitar el alcance de la excepción que permite prescindir del consentimiento del titular para el tratamiento de sus datos de salud cuando este sea realizado por razones de interés público en el ámbito de la salud, establecida en su inciso final,

dado que la amplitud del término “razones de interés público” no otorga un marco legal lo suficientemente delimitado como para prevenir tratamiento indebido de esta particular clase de datos. En virtud de lo anterior, se sugiere la siguiente redacción alternativa:

19. Reemplazar el inciso final del actual Artículo 32 del Proyecto, por el siguiente:

*“No se requerirá el consentimiento del titular para el tratamiento de datos de salud cuando ello sea necesario por **razones de interés público esencial** en el ámbito de la salud, el que en todo caso deberá ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular;*
*Asimismo, tampoco se requerirá el consentimiento del titular cuando el tratamiento sea necesario por **razones de interés público en el ámbito de la salud pública**, como en el caso de amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, siempre y cuando se establezcan medidas adecuadas y específicas para proteger los derechos y libertades del titular y, en particular, el secreto profesional.”*

Por su parte, el **Artículo 33**, establece tres parámetros mínimos que han de ser considerados para el tratamiento de los datos relativos a la salud. En relación al primero de estos parámetros es posible hacer los siguientes reparos:

Considerando que el mismo se refiere a los datos de salud generados en establecimientos de salud, una excepción que permita prescindir del consentimiento del titular de esta clase de datos para su tratamiento cuando este sea requerido *para fines de prevención, diagnóstico o tratamiento*, vacía completamente de contenido la disposición, toda vez que estas son precisamente todas las finalidades con que, por regla general, son tratados los datos personales dentro de esta clase de establecimientos, pasando así el consentimiento informado a ser la excepción.

En virtud de lo anterior se sugiere la siguiente redacción alternativa:

20. Eliminar la parte final del numeral 1) del Artículo 33, donde dice “*salvo el caso de tratamiento para fines de prevención, diagnóstico o tratamiento.*” y reemplazarla por el siguiente texto:

”salvo en los casos en que el tratamiento sea necesario para proteger intereses vitales del interesado, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; o sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base de la legislación especializada sobre la materia o en virtud de un contrato con un profesional sanitario. En este último caso el tratamiento sólo podrá ser realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con la legislación especializada sobre la materia o con las demás normas que al respecto pueda establecer la Autoridad.”

Respecto del **Artículo 34** del Proyecto, este resulta bastante confuso respecto de sus objetivos. Creemos que tal disposición puede aprovecharse para abordar en forma más sistemática la cuestión del acceso a datos relativos a la salud para fines de investigación pública y privada, pero excluir otro tipo de usos amplios por parte de privados de esos mismos datos (ejemplo con fines de empleo o determinación de asegurabilidad).

En virtud de lo anterior proponemos la siguiente redacción:

21. Sustituir el actual Artículo 34 por el siguiente:

“Artículo 34.- Tratamiento de datos de salud por entes privados y públicos con fines de investigación.- Los datos relativos a salud que consten en las instituciones que conforman el Sistema Nacional de Salud, podrán ser tratados por personas naturales y jurídicas privadas y públicas con fines de investigación científica, siempre que según el caso encuentren agregados o anonimizados, o dicho tratamiento sea autorizado por la Autoridad de Protección de Datos Personales, previo informe de la autoridad sanitaria nacional”.

10. Comunicación de datos a terceros

El segundo párrafo del **Artículo 35** puede generar incongruencias interpretativas respecto a los requisitos necesarios para obtener el consentimiento, por lo que sugerimos la siguiente redacción:

22. Reformular el segundo párrafo del Artículo 35 de la siguiente forma:
“Se entenderá que el consentimiento es informado cuando para la transferencia o comunicación de datos personales el Responsable del tratamiento haya entregado información suficiente al titular que le permita conocer la finalidad a que se destinarán sus datos y el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos”.

El **Artículo 38** recoge en forma miscelánea una serie de hipótesis bastante amplias en que no es necesario contar con el consentimiento del titular para la transferencia o comunicación de datos personales. Particularmente problemáticas se presentan la hipótesis de los numerales 1, 3 y 4.

Respecto del numeral 1), la redacción de la disposición no resulta suficientemente clara, cubriendo dos hipótesis distintas de la legitimidad del procesamiento de los datos: por una parte la fuente accesible al público (que ha sido criticada y sugerida enmendar antes), y por otra el consentimiento como base de una relación jurídica. Con ello esta disposición estaría en forma general autorizando a la transferencia o comunicación de datos personales sin necesidad de un consentimiento específico al respecto como dispone el inciso primero frase final del Artículo 35. Esta excepción por su amplitud contradice y vacía de contenido la regla general establecida en el Artículo 35, con lo cual debiera ser eliminada.

Respecto del numeral 3), la referencia a datos disociados debiera armonizarse con la nomenclatura utilizada en el proyecto, refiriendo a datos agregados, o al menos anonimizados.

Respecto del numeral 4), la calificación de “urgencia” parece un concepto demasiado abierto que requerirá de bastante interpretación para prevenir su abuso. En el derecho comparado, por ejemplo en la Unión Europea, ello se acota a urgencias que impliquen intereses vitales. En la misma línea, debiera contemplarse específicamente una regla para el tratamiento de datos con fines epidemiológicos, sujeta a tratamiento agregado, o al menos anonimizado una vez pasada la urgencia que implique intereses vitales, y siempre que el interés público en este tratamiento resulte acorde estándares de derechos humanos.

En virtud de lo anterior, se sugieren las siguientes complementaciones:

23. Eliminar el numeral 1 del Artículo 38.
24. Eliminar en el numeral 3 del Artículo 38 la palabra “disociados”, y agregar a continuación de “debidamente” lo siguiente: “agregados, o a lo menos anonimizados;”.
25. Sustituir el numeral 4 del Artículo 38 por el siguiente:
“Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que implique intereses vitales de su titular y este se encuentre impedido de otorgar su consentimiento.”
Agregar un nuevo numeral al Artículo 38:

“Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para realizar los estudios epidemiológicos de interés público, dando cumplimiento a los estándares internacionales en la materia de derechos humanos, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad. El tratamiento deberá ser de preferencia anonimizado, y en todo caso agregado, una vez pasada la urgencia de interés público”.

11. Seguridad de datos personales

El **Artículo 45 (Notificación de vulneración de seguridad)** establece la obligación del responsable de notificar a la autoridad competente en caso de sufrir una vulneración de seguridad, otorgándole un plazo máximo de 5 días para ello.

Este plazo parece demasiado amplio en orden a precaver adecuadamente los posibles daños causados por un quiebre de seguridad que tenga como consecuencia la filtración de datos personales. Ello particularmente en atención a que dicho plazo no dice relación con la solución del problema de seguridad, sino con advertir a la autoridad sobre la existencia de riesgos, para que ésta pueda disponer medidas de resguardo o supervisar las que se estén tomando para evaluar su suficiencia y pertinencia. En virtud de lo anterior, se recomienda realizar la siguiente modificación:

26. Reemplazar la parte final del inciso primero, desde “*dentro del término de cinco (5) días...*” en adelante, por lo siguiente:
“tan pronto sea posible, y a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.”
27. Reemplazar la parte final del inciso segundo, desde “*dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella.*” por lo siguiente:
“tan pronto sea posible, y a más tardar dentro del término de veinticuatro (24) horas contadas desde que tenga conocimiento de ella”.

En línea con lo anterior, el **Artículo 47** obliga a la Notificación de vulneración de seguridad al titular, pero también establece excepciones a este deber. En relación con estas últimas, consideramos que las exclusiones de los numerales 1 y 2 vacían de contenido la obligación de notificación, desproveyendo al titular de su derecho de saber cómo están siendo tratados sus datos y de la posibilidad de tomar medidas de resguardo en caso de una brecha de seguridad que afecta sus datos personales. En la alternativa se decida mantener tales excepciones, ellas debieran ser calificadas por la evaluación de la Autoridad de Protección, y no dejarse al mero arbitrio del Responsable la determinación de si concurren.

En virtud de lo anterior, se recomienda realizar la siguiente modificación:

28. Eliminar los numerales 1 y 2 del Artículo 47, o alternativamente, agregar el siguiente inciso a continuación del numeral 3:

“La procedencia de las excepciones de los numerales 1 y 2 deberá ser calificada por la Autoridad de Protección una vez informada esta tan pronto sea posible, y en cualquier caso dentro de los plazos contemplados en el Artículo 45”.

12. Delegado de protección de datos personales

En el **Artículo 51** se establecen algunas consideraciones especiales para el delegado de protección de datos personales, entre las cuales se establece que *“No podrán destituir o sancionar al delegado de protección de datos personales por el desempeño de sus funciones”*.

Entendemos que la finalidad de dicha norma es proteger al Delegado de eventuales represalias por cumplir sus funciones, para que este pueda realizar su trabajo de la manera más objetivamente posible y no presionado por expectativas ajenas que sean contrarias a las labores que él debe ejercer. Pero de la manera en como está redactado el artículo, podría terminar provocando la consecuencia contraria, pues en su texto actual se entiende que el Delegado no podría ser destituido de su cargo *aun cuando no cumpliera con sus funciones*. Es por esto que recomendamos lo siguiente:

Intercalar en el Artículo 51 numeral 4) *entre “el y desempeño” la palabra correcto*.

13. Régimen sancionatorio

El **Artículo 65** que abarca los casos en que resultan aplicables las medidas correctivas para resolver en primera instancia infracciones de carácter leve presenta en su actual formulación un problema de técnica legislativa, ya que a su vez el Artículo 66, referido a las infracciones leves, contempla en su numeral 5 como una de aquellas el incumplimiento de una medida correctiva. En el juego de estas dos disposiciones se produciría un bucle infinito, en que el no cumplimiento de medidas correctivas daría lugar nuevamente a medidas correctivas. Adicionalmente genera un incentivo incorrecto respecto del cumplimiento de las órdenes de la Autoridad de Protección,

es por ello que proponemos que el incumplimiento de las medidas correctivas sea calificado de infracción grave de acuerdo a lo indicado en el numeral 15 del Artículo 67.

En general, el catálogo de infracciones leves contemplado en el **Artículo 66** nos parece apropiado, con la sola excepción de dos hipótesis (numerales 2 y 3) que creemos más propias de una infracción grave, por el vínculo directo que tienen con la afectación del ejercicio de derechos fundamentales de los titulares.

Resulta preocupante la señal de política pública que se entrega al calificar el incumplimiento de la obligación de notificación de una brecha de seguridad que impacta en el ejercicio de derechos fundamentales como una infracción leve, pues se trata de una situación que podría acarrear consecuencias desastrosas para las ciudadanas y ciudadanos.

Como contrapartida, las circunstancias descritas en los numerales 9 y 11 del **Artículo 67** sobre infracciones graves, de naturaleza más bien administrativa no parecieran ser constitutivas de infracciones graves, ya que bajo la lógica del mismo proyecto de ley, son infracciones que son fácilmente solucionables mediante la aplicación de medidas correctivas como las señaladas en el artículo 64.

Adicionalmente, creemos conveniente modificar el numeral 15 del Artículo 67 incluyendo como falta grave la reincidencia en la comisión de faltas leves, por ejemplo, el negar reiteradamente las peticiones o quejas realizadas por los titulares de los datos.

Es por ello que proponemos las siguiente modificaciones:

29. En el Artículo 66, eliminar el numeral 5, y sustituir los actuales numerales 2 y 4 por los numerales 9 y 11 del Artículo 67.
30. En el Artículo 67 sustituir los actuales numerales 9 y 11 por los numerales 2 y 4 del Artículo 66.
31. Incluir al final del numeral 15 del artículo 67 la siguiente fórmula: “; o incurrir de forma reiterada en faltas leves.”

La participación de las organizaciones de sociedad civil especializadas en derechos digitales, con el espíritu de colaboración entre múltiples partes interesadas, puede enriquecer sustancialmente el proceso de debate y el resultado en la perspectiva de contar con una ley general de protección de datos personales que permita el desarrollo económico y el pleno ejercicio de los derechos de los ciudadanos y las ciudadanas del Ecuador.