Miraflores, 04 de abril de 2022

OFICIO N° 763 -2022-JUS/SG

Señor
ALEJANDRO SOTO REYES
Presidente de la Comisión de Transportes y Comunicaciones
Congreso de la República
Presente. -

Asunto: Opinión técnica del Proyecto de Ley Nº 878/2021-CR, Ley General de Internet

Referencia: a) Oficio Múltiple N° D001857-2021-PCM-SC
b) Oficio N° 0483-2021-2022-CTC/CR

De mi mayor consideración:

Es grato dirigirme a usted para saludarlo cordialmente y, por especial encargo del Señor Ministro de Justicia y Derechos Humanos, Félix Inocente Chero Medina, dar respuesta al documento a) de la referencia, a través del cual la Secretaría de Coordinación de la Presidencia del Consejo de Ministros traslada la solicitud de su Despacho de emitir opinión técnica sobre el Proyecto de Ley Nº 878/2021-CR, Ley General de Internet.

Al respecto, se remite copia del Informe Jurídico N° 03-2022-JUS/DGTAIPD, de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, con la finalidad de dar atención a lo requerido.

Aprovecho la oportunidad para expresarle los sentimientos de mi más alta consideración y estima.

Atentamente,

RAMÓN FERNANDO ALCALDE POMA
Secretario General
Ministerio de Justicia y Derechos Humanos

cc: Secretaría de Coordinación de la Presidencia del Consejo de Ministros

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

INFORME JURÍDICO N° 03-2022-JUS/DGTAIPD

A : **Juan Manuel Carrasco Millones**
Viceministro de Justicia

DE : **Eduardo Luna Cervantes**
Director General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales

ASUNTO : Opinión sobre Proyecto de Ley N° 878/2021-CR que propone la Ley General de Internet

REFERENCIA: a) Oficio Múltiple N° D001857-2021-PCM-SC
b) Proyecto de Ley N° 878/2021-CR
c) Informe Técnico N° 007-2022-DFI-ORQR

FECHA : 24 de febrero de 2022

I. ANTECEDENTES:

1. Mediante Oficio Múltiple N° D001857-2021-PCM-SC de fecha 16 de diciembre de 2021, la Secretaría de Coordinación de la Presidencia del Consejo de Ministros solicitó opinión legal al Ministerio de Justicia y Derechos Humanos sobre el Proyecto de Ley N° 878/2021-CR, que propone la dación de la Ley General de Internet, atendiendo a que dicho texto contiene materias que se encuentran dentro del ámbito de sus competencias. Dicho documento fue derivado a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIPD) mediante Proveído N° 005566-2021-VMJ, y este a su vez fue derivado a la Dirección de Protección de Datos Personales (DPDP) mediante Proveído N° 001754-2021-DGTAIPD.

2. En ese contexto, considerando que el referido proyecto de ley contiene aspectos técnicos relacionados con las tecnologías de la información y comunicación, mediante Memorándum N° 002-2022-JUS/DGTAIPD-DPDP de fecha 06 de enero de 2022, se solicitó a la Dirección de Fiscalización e Instrucción (DFI) la emisión de un informe técnico con el fin de emitir una opinión integral sobre el citado proyecto.

3. De esa forma, la DFI, mediante Memorándum N° 005-2022-JUS/DGTAIPD-DFI de fecha 17 de enero de 2022, remitió el Informe Técnico N° 007-2022-DFI-ORQR de fecha 14 de enero de 2022, a través del cual se emitió opinión técnica conforme a lo solicitado.

II. MARCO NORMATIVO DE ACTUACIÓN

4. De conformidad a lo establecido por los artículos 70 y 71 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N° 013-2017-JUS, corresponde a la DGTAIPD ejercer la Autoridad Nacional de Transparencia y Acceso a la Información Pública (ANTAIP) y la Autoridad Nacional de Protección de Datos Personales (ANPD); por ende, en su calidad de tal, tiene entre sus funciones emitir informes respecto de los proyectos de normas que se refieran total o parcialmente a los ámbitos de su competencia.

5. En esa medida, esta Dirección General emite el presente Informe Jurídico en el ámbito de la interpretación de las normas en materia de acceso a la información pública y protección de datos personales contenidas en el Proyecto de Ley N° 878/2021-CR.

III. ANÁLISIS

6. El proyecto de Ley tiene como objeto, de acuerdo al artículo 1, "establecer el marco general sobre diversos aspectos de internet, tales como el reconocimiento del acceso a internet como un derecho a la persona, su declaratoria como servicio público esencial, la creación de reglas de favorecimiento de la ampliación y mejora en materia de infraestructura para el acceso a internet, el establecimiento de las reglas básicas para la provisión de servicios en internet, la regulación de aspectos básicos de la contratación electrónica, así como de los nombres de dominio y la publicidad comercial por correo electrónico no deseado".

7. En esa línea, el artículo IV del Título Preliminar del citado proyecto, hace mención a la gratuidad del acceso a Internet en instituciones y espacios públicos.

8. En ese contexto, se aprecia que uno de los objetivos del mencionado proyecto de ley es reconocer como un derecho de la persona humana el acceso a Internet, declarándola inclusive como un servicio público esencial, lo cual se condice con el pronunciamiento realizado por el Consejo de Derechos Humanos de las Naciones Unidas[1] respecto a la reducción de las brechas digitales en la población.

9. Sin embargo, de la revisión de la propuesta consideramos necesario observar dos temas que ponen en riesgo la protección de datos personales:

   - El tratamiento no autorizado del correo electrónico con fines publicitarios.
   - El acceso o derecho a solicitar la contraseña de una red wifi de titularidad pública.

[1] El Consejo de Derechos Humanos de las Naciones Unidas mediante Resolución A/HRC/38/L.10 de fecha 02 de julio de 2018, exhorta a todos los Estados a cerrar las brechas digitales, especialmente la existente entre los géneros, y a aumentar el uso de la tecnología de la información y las comunicaciones, para promover el pleno disfrute de los derechos humanos para todos. [Recuperado el 01 de febrero de 2022 de: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L10.pdf].

Sobre el tratamiento no autorizado del correo electrónico con fines publicitarios

10. La Ley Nº 29733, Ley de Protección de Datos Personales (en adelante la LPDP) tiene como objeto garantizar el derecho fundamental a la protección de datos personales, previsto en el numeral 6 del artículo 2° de la Constitución Política del Perú, que señala que toda persona tiene derecho "*a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.*"

11. La LPDP define a los datos personales en el artículo 2, numeral 4, como "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados".

12. Complementariamente, el Reglamento la LPDP, aprobado por Decreto Supremo Nº 003-2017-JUS, en su artículo 2, numeral 4, define a los datos personales como "aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados".

13. La dirección de correo electrónico es un dato personal, puesto que identifica o hace identificable a la persona. Identifica a la persona en aquellos casos en los que la dirección de correo electrónico lleva el nombre de la persona o el nombre bajo el cual se hace llamar, y será identificable en aquellos casos en los que, aun no llevando el nombre de la persona, unido a otro dato, se puede identificar fácilmente a la misma. Respecto a este segundo supuesto, puede ocurrir que el propio titular del dato personal[2] haya brindado su correo junto con su nombre para determinadas finalidades, o que, si bien no se tiene identificado en un primer momento al titular del dato personal, una vez que este conteste el correo electrónico, ya se le habrá identificado como dicho titular.

14. Para el tratamiento[3] de los datos personales, la LPDP establece principios rectores para la protección de los mismos, entre ellos se encuentra el principio de consentimiento[4], el cual establece que solo se puede realizar tratamiento de datos personales con el consentimiento del titular del dato personal. El consentimiento, de acuerdo a la LPDP, artículo 13, inciso 13.5, debe ser previo, informado, expreso e inequívoco.

---

[2] La LPDP, artículo 2, numeral 16, define al Titular del dato personal como "Persona natural a quien corresponde los datos personales."

[3] La LPDP, artículo 2, numeral 19, define como tratamiento de datos personales a "cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales, comprende tratamiento de datos personales".

[4] LPDP, artículo 5.

15. Sin embargo, la LPDP establece excepciones a la obligación de solicitar el consentimiento de forma previa cuando se presenten los supuestos establecidos en el artículo 14 de la LPDP, entre ellos, *"cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento."*[5]

16. Por lo tanto, para utilizar o dar tratamiento al titular del dato personal, se debe contar previamente con el consentimiento del titular del dato personal.[6]

17. El tratamiento de datos personales sin el consentimiento del titular del dato constituye una infracción grave a la LPDP conforme el artículo 132, numeral 2, literal b)[7], la cual puede ser sancionada con una multa entre más de 5 a 50 UIT, conforme el artículo 39 de la LPDP, por parte de la Autoridad Nacional de Protección de Datos Personales.[8]

18. Sin embargo, en el proyecto, específicamente en el artículo 75, se permite el uso de correo electrónico para envío de publicidad sin consentimiento previo, siempre que de forma posterior se pueda solicitar no recibir dichos mensajes. Dicha propuesta es contraria al principio de consentimiento establecido en el artículo 5 de la LPDP.

19. Asimismo, en el artículo 76, inciso 76.3, se señala que es el Instituto de Defensa de la

[6] Ver: Opinión Consultiva N° 12-2019-JUS/DGTAIPD-Remisión de correos publicitarios no solicitados. Disponible en: https://www.gob.pe/institucion/anpd/informes-publicaciones/1373460-oc-n-12-2019-jus-dgtaipd-sobre-remision-de-correos-publicitarios-no-solicitados

[7] LPDP
"Artículo 38.- Tipificación de infracciones
Las infracciones se clasifican en leves, graves y muy graves, las cuales son tipificadas vía reglamentaria, de acuerdo a lo establecido en el numeral 4) del artículo 230 de la Ley Nº 27444, Ley del Procedimiento Administrativo General, mediante Decreto Supremo con el voto aprobatorio del Consejo de Ministros.
(…)."
Reglamento de la LPDP
"Artículo 132.- Infracciones
Las infracciones a la Ley Nº 29733, Ley de Protección de Datos Personales, o su Reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada Ley.
(…).
2.Son infracciones graves:
(…).
b) Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la Ley Nº 29733 y su Reglamento.
(…)."

[8] Al respecto, de acuerdo al artículo 33 de la LPDP, la Autoridad Nacional de Protección de Datos Personales ejerce funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras, y en ese marco, de acuerdo al numeral 20 del artículo mencionado, tiene entre sus funciones *"iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento."*

Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), la institución encargada de conocer las infracciones al mal uso del correo electrónico con fines publicitarios, no teniendo en cuenta que el correo electrónico es un dato personal que debe ser utilizado cumpliendo tanto la LPDP como las normas referidas a comercio electrónico.

20. El proyecto no ha tenido en cuenta que la Autoridad Nacional de Protección de Datos Personales tiene a cargo la fiscalización y sanción del mal uso de datos personales.

21. Es necesario que la Ley General de Internet este acorde con la protección del derecho fundamental a la protección de datos personales y con los principios que lo garantizan.

Sobre el acceso a la contraseña de una red wifi

22. El artículo IV del Título Preliminar del citado proyecto, referido a la gratuidad del acceso a Internet en instituciones y espacios públicos, prescribe lo siguiente: "*Las distintas instituciones del Estado y los espacios públicos gestionados por el mismo deben contar con mecanismos que hagan posible el acceso a Internet a todos los ciudadanos, salvo medien razones de orden público y seguridad nacional. Los ciudadanos tienen el derecho de solicitar la contraseña de acceso de forma gratuita en caso encuentren una red wifi de titularidad pública, a menos que se trate de una red protegida por razones de orden público y seguridad nacional."* (Subrayado nuestro).

23. Si bien se aprecia que uno de los objetivos del mencionado proyecto de ley es reconocer como un derecho de la persona humana el acceso a Internet, declarándola inclusive como un servicio público esencial, proyectar dentro del mismo dispositivo legal como un derecho ciudadano el *"solicitar la contraseña de acceso de forma gratuita en caso encuentren una red wifi de titularidad pública",* resultaría atentatorio contra el marco de confianza digital que debe existir en las interacciones digitales entre el Estado y la ciudadanía, conforme a las disposiciones establecidas por el Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento[9].

24. Y es que no es lo mismo reconocer el derecho de acceso a Internet que deben tener todas las personas en un mundo cada vez más digitalizado, que el derecho de cada individuo de solicitar la contraseña de acceso a una red inalámbrica de una entidad pública, debido a que esto último puede poner en riesgo el entorno digital en que se desenvuelven dichas entidades, así no sean instituciones que tengan por finalidad el

[9] El literal a) del artículo 3 del D.U. N° 007-2020, define como confianza digital al "estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la trasformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital".

orden público o la seguridad nacional, dado que todas las entidades del Estado de algún modo poseen activos críticos que deben de proteger, como son: información de carácter secreta, reservada y confidencial según las disposiciones del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado por Decreto Supremo N° 021-2019-JUS, así como realizar un adecuado tratamiento de datos personales conforme a la Ley N° 29733, Ley de Protección de Datos Personales (LPDP).

25. Sobre todo, si el artículo 9 de la LPDP establece como un principio rector para el tratamiento de datos personales **el principio de seguridad**, a través del cual se establece que *"el titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate".*

26. Igualmente, el artículo 16 de la LPDP, sobre la seguridad en el tratamiento de datos personales, señala que para *"fines de tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado. (…). Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo";* tratamiento que no se garantizaría al divulgarse la contraseña de una red inalámbrica de Internet de una entidad pública a la ciudadanía.

27. Lo antes expuesto tiene sustento en el Informe Técnico N° 007-2022-DFI-ORQR de fecha 14 de enero de 2021, formulado por el Analista de Fiscalización en Seguridad de la Información de la DFI, en donde se señala que la red de internet "wifi" es uno de los componentes de arquitectura más vulnerables de cualquier institución, debido a que permite el acceso de dispositivos desconocidos a la red, con implicaciones y fines desconocidos, por lo que se debe contar con una protección comprobada y robusta.

28. También, en dicho Informe, se indica que la propuesta legislativa consistente en reconocerle a los ciudadanos el derecho de solicitar la contraseña de acceso de forma gratuita, en caso encuentren una red *wifi* de titularidad pública, no se encuentra alineada con las buenas prácticas establecidas en la gestión de los controles de acceso, conforme a la norma ISO 27001[10] (sección A9 del Anexo A). En la parte concerniente a controles de acceso, señala que: "Los usuarios sólo deben tener acceso a la red y a los servicios

[10] La norma ISO 27001, es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El estándar ISO 27001:2013 para los Sistemas de Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. [Recuperado el 01de febrero de 2022 de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/#:~:text=ISO%2027001%20es%20una%20norma,los%20sistemas%20que%20la%20procesan.&text=La%20Gesti%C3%B3n%20de%20la%20Seguridad,en%20la%20norma%20ISO%2027002.]

para los que se les ha autorizado específicamente. El acceso debe ser controlado por un procedimiento de inicio seguro y restringido, de acuerdo con la política de control de acceso".

29. Además, la acción de compartir las credenciales de acceso, clave de usuario y/o contraseña de acceso a redes "wifi" de titularidad pública con múltiples usuarios desconocidos y sin tener en cuenta un esquema de control y registro, imposibilita tener certeza respecto a la trazabilidad de las acciones realizadas en el entorno de red correspondiente, ya que ante un posible escenario de vulneración de la confidencialidad de la información o tratamiento inadecuado, no sería posible identificar a los usuarios u operadores cuyas acciones han vulnerado la red, y esa falta de información tampoco podría fortalecer una base de conocimiento necesaria para disminuir la ocurrencia de dichos escenarios.

30. El informe técnico advierte también que compartir el acceso de una red de forma pública, sin contemplar lo indicado en la norma internacional ISO 27001, presenta potenciales riesgos, tales como el robo de información transmitida, el robo de información almacenada, la infección por malware y el uso ilegal de la red.

31. Por último, es necesario señalar que disponer mediante ley la entrega de una contraseña de acceso a una red inalámbrica de titularidad pública, vulneraría la confidencialidad que posee cualquier contraseña como característica inherente; así incluso se ha remarcado en la Directiva de Seguridad de la Información[11] emitida por la Autoridad Nacional de Protección de Datos Personales, en cuyo numeral 2.3.1.1 del artículo 2, al referirse a las medidas de seguridad técnicas, sobre la gestión y uso de contraseñas cuando el tratamiento se realice con medios informáticos, señala lo que *"se debe controlar la asignación y el uso de las contraseñas de los usuarios de los sistemas de información que realizan tratamiento de datos personales mediante la adopción de las siguientes medidas: a) Solicitar a los usuarios que mantengan en secreto las contraseñas asignadas. (…)".* (Subrayado nuestro).

IV. CONCLUSIONES

1. El Proyecto de Ley N° 878/2021-CR, denominado Ley General de Internet, propone considerar como un derecho de la persona humana "solicitar la contraseña de acceso de forma gratuita en caso encuentren una red wifi de titularidad pública"; no obstante, dicha propuesta resultaría atentatoria del marco de confianza digital que debe existir entre el Estado y la ciudadanía, según las disposiciones establecidas por el Decreto de Urgencia N° 007-2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento, así como las disposiciones sobre medidas de seguridad en el tratamiento de datos personales establecidas en la Ley N° 29733, Ley de Protección de Datos Personales.

[11] Directiva de Seguridad, Primera Edición 2013, p. 22. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf.

2. La propuesta legislativa bajo examen, en su versión actual, no se condice con el principio de seguridad establecido en el artículo 9 de la Ley de Protección de Datos Personales, el cual garantiza que el titular del banco de datos personales y el encargado de su tratamiento adopten las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales, disponiendo además que dichas medidas de seguridad deban ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

3. La posibilidad de reconocer como un derecho el solicitar la contraseña de acceso en caso se encuentre una red wifi de titularidad pública, resulta contrario a las buenas prácticas y estándares establecidos en la gestión de los controles de acceso, conforme a la norma internacional de seguridad de la información ISO 27001, lo cual derivaría en la generación de potenciales riesgos en el entorno digital de las entidades públicas, como son: riesgos de robo de información transmitida, robo de información almacenada, infección por malware y uso ilegal de la red.

4. El Proyecto de Ley N° 878/2021-CR no ha considerado el correo electrónico como un dato personal, ni las funciones de la Autoridad Nacional de Protección de Datos Personales; por lo que se ha omitido un análisis de la evaluación de impacto que este tratamiento podría acarrear sobre el derecho constitucional reconocido en el artículo 2, inciso 6 de la Constitución.

Por las consideraciones expuestas, y hasta no superar las observaciones planteadas, no consideramos viable para aprobación el proyecto bajo examen.

Eduardo Luna Cervantes
Director General
Dirección General de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales