CONGRESO DE LA REPÚBLICA
Área de Trámite Documentario
13 DIC. 2023
RECIBIDO
Firma: Hora: 16:16

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la unidad, la paz y el desarrollo"

Lima, 13 de diciembre de 2023

OFICIO Nº 385 -2023 -PR

Señor
ALEJANDRO SOTO REYES
Presidente del Congreso de la República
Presente. -

Tenemos el agrado de dirigirnos a usted, de conformidad con lo dispuesto por el artículo 104º de la Constitución Política del Perú, con la finalidad de comunicarle que, al amparo de las facultades legislativas delegadas al Poder Ejecutivo mediante Ley N° 31880, y con el voto aprobatorio del Consejo de Ministros, se ha promulgado el Decreto Legislativo N° 1591, que modifica la Ley N° 30096, Ley de Delitos Informáticos para promover el uso seguro y responsable de las tecnologías digitales por niñas, niños y adolescentes.

Sin otro particular, hacemos propicia la oportunidad para renovarle los sentimientos de nuestra consideración.

DINA ERCILIA BOLUARTE ZEGARRA
Presidenta de la República

LUIS ALBERTO OTÁROLA PEÑARANDA
Presidente del Consejo de Ministros

REPUBLICA DEL PERU

ES COPIA FIEL DEL ORIGINAL

TERESA GUADALUPE RAMIREZ PEQUEÑO
SECRETARIA DEL CONSEJO DE MINISTROS

Decreto Legislativo Nº 1591

LA PRESIDENTA DE LA REPÚBLICA

POR CUANTO:

Que, el Congreso de la República, mediante Ley N° 31880, ha delegado en el Poder Ejecutivo la facultad de legislar en materia de seguridad ciudadana, gestión del riesgo de desastres-niño global, infraestructura social, calidad de proyectos y meritocracia, por un plazo de noventa (90) días calendario;

Que, el literal f) del numeral 2.3 del artículo 2 de la Ley N° 31880, dispone que el Poder Ejecutivo está facultado para legislar en el marco de la promoción del uso seguro y responsable de las tecnologías digitales por niños, niñas y adolescentes, de acuerdo con las siguientes consideraciones: 1) La modificación de la Ley 30096, Ley de delitos informáticos, se encuentra delimitada a la precisión de los delitos de grooming, fraude informático y suplantación de identidad; 2) Las modificaciones de la Ley 30096, Ley de delitos informáticos, y del Decreto Legislativo 957, Código Procesal Penal, en cuanto a la figura del agente encubierto, se limitan a la mención expresa de la posibilidad de su actuación en entornos digitales, así como al deber de coordinación con la Secretaría de Gobierno y Transformación Digital en la elaboración de protocolos referidos a dicha actuación; y, 3) La modificación del Decreto Legislativo 1267 se limita a incorporar el deber de coordinación con la Secretaría de Gobierno y Transformación Digital en la elaboración de protocolos referidos al empleo de sistemas tecnológicos y registros previstos en el artículo 43 de dicha norma;

Que, en los últimos años, la comisión de delitos informáticos y los delitos cometidos a través de las tecnologías digitales se ha incrementado significativamente en el Perú, aspecto que supone un especial riesgo para las niñas, niños y adolescentes, cuya interacción en el ámbito digital también va en aumento. Esta situación requiere de una respuesta integral y eficiente del Estado que, entre diversos aspectos, incluye el fortalecimiento de la persecución penal, a través de la tipificación de delitos, precisión de actos de investigación y articulación entre las instancias competentes en materia penal y en materia de gobierno y transformación digital; con el propósito de contribuir a brindar una mayor protección a las víctimas de tales delitos, especialmente si se trata de niñas, niños y adolescentes, así como para evitar la impunidad respecto a tales delitos;

Que, en virtud a la excepción establecida en el numeral 18) del inciso 28.1 del artículo 28 del Reglamento que desarrolla el Marco Institucional que rige el Proceso de Mejora de la Calidad Regulatoria y establece los Lineamientos Generales para la aplicación del Análisis de Impacto Regulatorio Ex Ante, aprobado mediante Decreto

OFICINA DE LA DIRECCIÓN GENERAL DE ASESORÍA JURÍDICA · PRESIDENCIA DEL CONSEJO DE MINISTROS

ES COPIA FIEL DEL ORIGINAL
TERESA GUADALUPE RAMIREZ PEQUEÑO
SECRETARIA DEL CONSEJO DE MINISTROS

Supremo Nº 063-2021-PCM, no corresponde que se realice el Análisis de Impacto Regulatorio Ex Ante debido a que las disposiciones contenidas no establecen, incorporan o modifican reglas, prohibiciones, limitaciones, obligaciones, condiciones, requisitos, responsabilidades o exigencias que generen o impliquen variación de costos en su cumplimiento por parte de las empresas, ciudadanos o sociedad civil que limite el otorgamiento o reconocimiento de derechos; sino modificaciones a la Ley N° 30096, Ley de Delitos Informáticos; asimismo, en la medida que el presente Decreto Legislativo no desarrolla procedimientos administrativos bajo el alcance del Análisis de Calidad Regulatoria (ACR), no se requiere realizar el ACR Ex Ante previo a su aprobación;

De conformidad con lo establecido por el artículo 104 de la Constitución Política del Perú, y en ejercicio de las facultades delegadas según lo dispuesto en literal f) del numeral 2.3 del artículo 2 de la Ley N° 31880;

Con el voto aprobatorio del Consejo de Ministros; y,

Con cargo a dar cuenta al Congreso de la República;

Ha dado el Decreto Legislativo siguiente:

DECRETO LEGISLATIVO QUE MODIFICA LA LEY N° 30096, LEY DE DELITOS INFORMÁTICOS PARA PROMOVER EL USO SEGURO Y RESPONSABLE DE LAS TECNOLOGÍAS DIGITALES POR NIÑAS, NIÑOS Y ADOLESCENTES.

Artículo 1.- Objeto

El presente decreto legislativo tiene por objeto modificar la Ley N° 30096, Ley de Delitos Informáticos, para promover el uso seguro y responsable de las tecnologías digitales por niñas, niños y adolescentes.

Artículo 2.- Modificación de los artículos 5 y 9, así como de la Segunda y Tercera Disposiciones Complementarias Finales de la Ley N° 30096, Ley de Delitos Informáticos

Se modifican los artículos 5 y 9, así como la Segunda y Tercera Disposiciones Complementarias Finales de la Ley N° 30096, Ley de Delitos Informáticos, en los siguientes términos:

> **"Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos**
> El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad **no menor de seis ni mayor de nueve años**.
>
> Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años.

PRESIDENCIA DEL CONSEJO DE MINISTROS · OFICINA GENERAL DE ASESORÍA JURÍDICA · V°B°

ES COPIA FIEL DEL ORIGINAL
TERESA GUADALUPE RAMIREZ PEQUEÑO
SECRETARIA DEL CONSEJO DE MINISTROS

Decreto Legislativo

En todos los casos se impone, además, la pena de inhabilitación conforme a los numerales 1, 2, 3, 4, 5, 6, 8, 9, 10 y 11 del artículo 36 del Código Penal."

"Artículo 9. Suplantación de identidad
El que, mediante las tecnologías **digitales** suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material, moral **o de cualquier otra índole**, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

La pena privativa de libertad es no menor de seis ni mayor de nueve años cuando se suplante la identidad de una persona menor de 18 años de edad y resulte algún perjuicio, material, moral o de cualquier otra índole."

"DISPOSICIONES COMPLEMENTARIAS FINALES

(...)

SEGUNDA.- Agente encubierto en delitos informáticos
El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, **incluso si estas acciones deben realizarse en entornos digitales,** y con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

Los protocolos para la actuación del agente encubierto en entornos digitales, tanto en el marco de la presente Ley, como en el marco del artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957, son coordinados, en cuanto corresponda, con la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en concordancia con las normas vigentes que regulan el Sistema Nacional de Transformación Digital."

"TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados
La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del

ES COPIA FIEL DEL ORIGINAL

TERESA GUADALUPE RAMÍREZ PEQUEÑO
SECRETARÍA DEL CONSEJO DE MINISTROS

Ministerio Público, la **Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros** y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad."

Artículo 3.- Financiamiento

La implementación de lo dispuesto en el presente Decreto Legislativo se financia con cargo a los presupuestos institucionales de los pliegos involucrados, sin demandar recursos adicionales al Tesoro Público.

Artículo 4.- Refrendo

El presente Decreto Legislativo es refrendado por el Presidente del Consejo de Ministros, el Ministro del Interior, el Ministro de Justicia y Derechos Humanos y la Ministra de la Mujer y Poblaciones Vulnerables.

DISPOSICIÓN COMPLEMENTARIA FINAL

ÚNICA. Las improcedencias a las que hacen referencia los artículos 161, 372 y 471 del Código Procesal Penal, aprobado con Decreto Legislativo N° 957 y los artículos 51 y 55 del Texto Único Ordenado del Código de Ejecución Penal, aprobado con Decreto Supremo N° 003-2021-JUS, respecto al artículo 183-B del Código Penal, aprobado por el Decreto Legislativo Nº 635, son también aplicables a la comisión del delito establecido en el artículo 5 de la Ley N°30096, Ley de Delitos Informáticos.

POR TANTO:

Mando se publique y cumpla, dando cuenta al Congreso de la República.

Dado en la Casa de Gobierno, en Lima, a los doce días del mes de diciembre del año dos mil veintitrés.

PRESIDENCIA DEL CONSEJO DE MINISTROS
OFICINA GENERAL DE ASESORÍA JURÍDICA
V°B°

LUIS ALBERTO OTÁROLA PEÑARANDA
Presidente del Consejo de Ministros

DINA ERCILIA BOLUARTE ZEGARRA
Presidenta de la República

VÍCTOR MANUEL TORRES FALCÓN
Ministro del Interior

NANCY TOLENTINO GAMARRA
Ministra de la Mujer y Poblaciones Vulnerables

EDUARDO MELCHOR ARANA YSA
Ministro de Justicia y Derechos Humanos

CONGRESO DE LA REPÚBLICA

Lima, **14** de **diciembre** de **2023**

En aplicación de lo dispuesto en el Inc. b) del artículo 90° del Reglamento del Congreso de la República; para su estudio pase el expediente del Decreto Legislativo **N° 1591** a la Comisión de:

- **CONSTITUCIÓN Y REGLAMENTO.**

GIOVANNI FORNO FLOREZ
Oficial Mayor
CONGRESO DE LA REPÚBLICA

EXPOSICIÓN DE MOTIVOS

DECRETO LEGISLATIVO QUE MODIFICA LA LEY N° 30096, LEY DE DELITOS INFORMÁTICOS PARA PROMOVER EL USO SEGURO Y RESPONSABLE DE LAS TECNOLOGÍAS DIGITALES POR NIÑAS, NIÑOS Y ADOLESCENTES.

I. ANTECEDENTES

Mediante Ley N° 31880, el Congreso de la República delegó en el Poder Ejecutivo la facultad de legislar en materias de seguridad ciudadana, gestión del riesgo de desastres-niño global, infraestructura social, calidad de proyectos y meritocracia por un término de noventa (90) días calendario, contados a partir de la entrada en vigor de la referida Ley.

El literal f) del numeral 2.3 del artículo 2 de la precitada ley, dispone que el Poder Ejecutivo está facultado para legislar en el marco de la promoción del uso seguro y responsable de las tecnologías digitales por niños, niñas y adolescentes, de acuerdo con las siguientes consideraciones: 1) La modificación de la Ley 30096, Ley de delitos informáticos, se encuentra delimitada a la precisión de los delitos de grooming, fraude informático y suplantación de identidad; 2) Las modificaciones de la Ley 30096, Ley de delitos informáticos, y del Decreto Legislativo 957, Código Procesal Penal, en cuanto a la figura del agente encubierto, se limitan a la mención expresa de la posibilidad de su actuación en entornos digitales, así como al deber de coordinación con la Secretaría de Gobierno y Transformación Digital en la elaboración de protocolos referidos a dicha actuación; y, 3) La modificación del Decreto Legislativo 1267 se limita a incorporar el deber de coordinación con la Secretaría de Gobierno y Transformación Digital en la elaboración de protocolos referidos al empleo de sistemas tecnológicos y registros previstos en el artículo 43 de dicha norma.

Una de las herramientas que posee el Estado para proteger el libre ejercicio y respeto de los derechos es la regulación positiva que, en la mayoría de casos, asume la forma de normas jurídicas, de corte general y específico. En el caso de la Ley 30096, Ley de delitos informáticos, que regulan diferentes situaciones jurídicas que se encuentran directamente relacionadas con la promoción del uso de las tecnologías de la información y comunicación, la protección del derecho a la paz, tranquilidad y el entorno seguro, incluyendo cuando se encuentran involucrados niñas, niños o adolescentes.

Ahora bien, un problema común de la regulación es que muchas veces no se encuentra organizada, por diferentes motivos; la existencia de competencias compartidas, rectorías superpuestas, nivel de especificidad. Esta falta de organización resta eficiencia a la aplicación de la regulación y en muchos casos hace que sea incoherente o quede desfasada en un período de tiempo más corto, con pocas expectativas de ser actualizada de forma razonable frente al desarrollo de nuevos escenarios.

A propósito de este problema, durante la última década y como parte del proceso de modernización del Estado Peruano, se han creado los Sistemas Funcionales. Estos sistemas son conjuntos de principios, normas, procedimientos, técnicas e instrumentos mediante los cuales se organizan las actividades de la Administración Pública, que requieren ser realizadas por todas o varias entidades. En ese orden de ideas, los Sistemas Funcionales

tienen por objetivo asegurar el cumplimiento de políticas públicas que requieren la participación de todas o varias entidades del Estado.

En el caso de las tecnologías de comunicación e información, desde 2020 existe el Sistema Nacional de Transformación Digital, un sistema funcional del Estado establecido por el Decreto de Urgencia N° 006-2020 y cuyo ente rector es la Secretaría de Gobierno y Transformación Digital. En el artículo 4, numeral 2 de dicha norma se define este sistema como el que "(...) se sustenta en la articulación de los diversos actores públicos y privados de la sociedad y abarca, de manera no limitativa, las materias de gobierno digital, economía digital, conectividad digital, educación digital, tecnologías digitales, innovación digital, servicios digitales, sociedad digital, ciudadanía e inclusión digital y confianza digital; sin afectar las autonomías y atribuciones propias de cada sector, y en coordinación con estos en lo que corresponda en el marco de sus competencias".

Varias de las materias a las que hace referencia el Decreto de Urgencia N° 006-2020, ya habían sido desarrolladas de forma previa en otros dispositivos normativos, que establecen las rectorías, atribuciones y niveles de coordinación entre entidades del sector público. Por ejemplo, el Decreto Legislativo N° 1412, Ley de Gobierno Digital, dispone en su artículo 8 que la Secretaría de Gobierno Digital dicta las normas, establece los procedimientos y es responsable de la operación y correcto funcionamiento del gobierno digital, lo que incluye las materias antes mencionadas. De manera aún más específica, el Reglamento del Decreto Legislativo N° 1412, aprobado por Decreto Supremo N°029-2021-PCM, desarrolla las formas de articulación. Así, en materia de confianza y seguridad digital, el artículo 100 del citado reglamento señala que la Secretaría de Gobierno y Transformación Digital coordina las acciones contra la ciberdelincuencia y la creación de protocolos de actuación cuando las víctimas son menores de edad, en conjunto con la Policía Nacional y el Ministerio Público.

Así pues, es claro señalar que las competencias de la Secretaría de Gobierno y Transformación Digital, en tanto ente rector del Sistema Nacional de Transformación Digital, la habilita para proponer modificaciones a aquellas normas que inciden en las materias sobre las que tiene rectoría, siendo estas la confianza digital, la seguridad digital y las tecnologías digitales.

II. FUNDAMENTO TÈCNICO DE LA PROPUESTA NORMATIVA

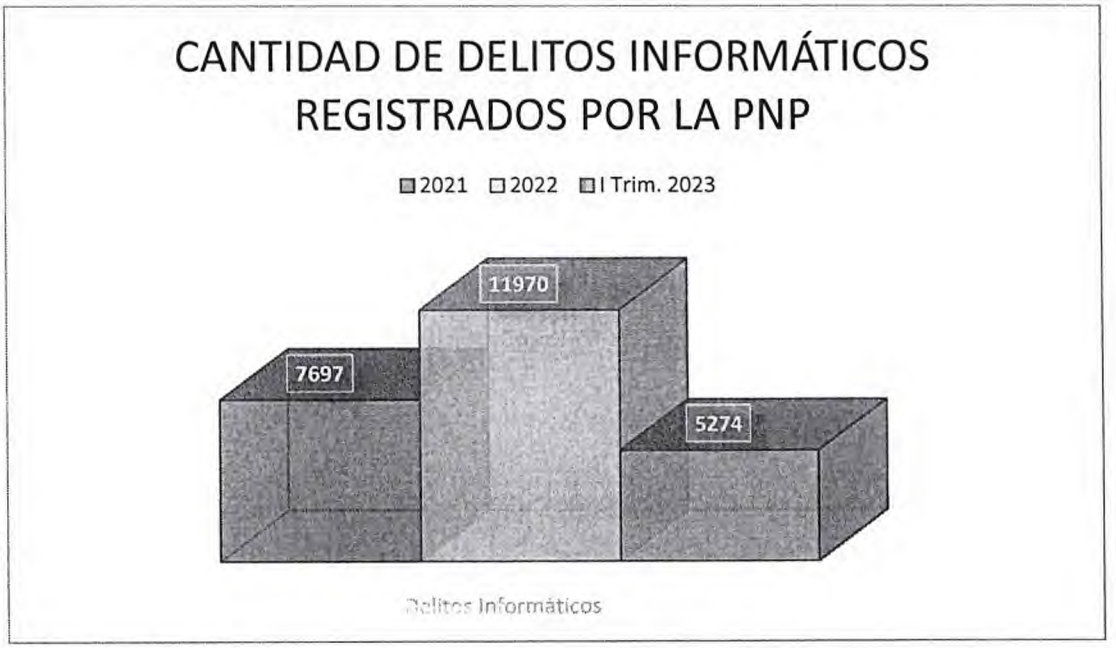
2.1. Análisis del estado situacional

A medida que aumenta la influencia de las tecnologías digitales, especialmente de Internet, el debate sobre si su impacto en la sociedad es mayormente positivo o negativo se torna cada vez más complejo. Por un lado, están quienes defienden las posibilidades casi ilimitadas que ofrece, desde la comunicación en tiempo real, hasta el ejercicio de derechos como la libertad de expresión e información. Por el otro, quienes resaltan sus peligros, como la aparición de nuevas adicciones, la cibercriminalidad y la diseminación de contenidos que promueven el odio y el extremismo.

De acuerdo con el Informe Defensorial N° 001-2023-DP/ADHPD "La ciberdelincuencia en el Perú: estrategias y retos del Estado" el Perú no ha sido ajeno al crecimiento global de este fenómeno criminal, pues desde octubre del 2013 hasta julio del 2020, las fiscalías penales comunes y mixtas del Ministerio Público de todo el país registraron 21,687 denuncias por delitos

informáticos, lo que demuestra un aumento significativo de la ciberdelincuencia, especialmente durante la emergencia sanitaria.

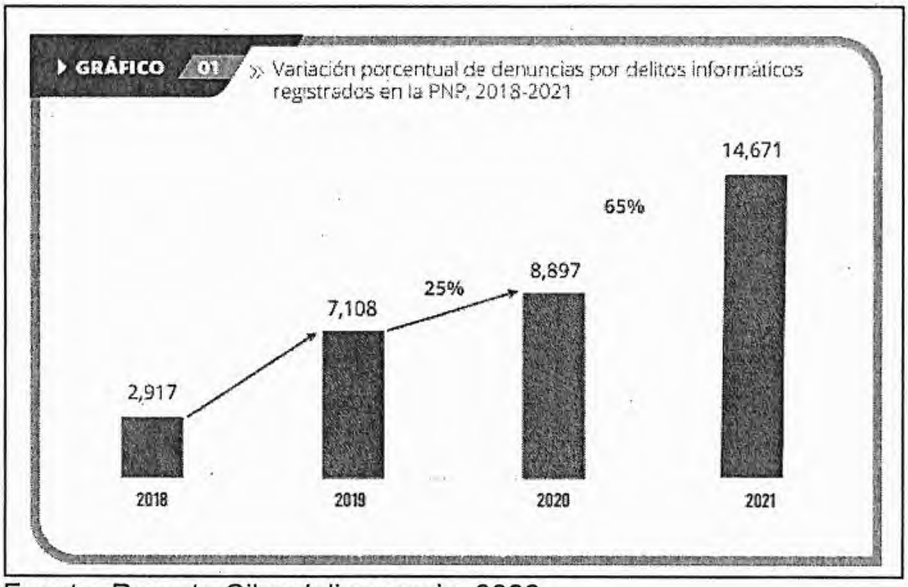
En efecto, conforme con los boletines estadísticos de la Policía Nacional del Perú, entre el año 2021 y el primer trimestre de 2023, se registraron 24,941 denuncias por delitos informáticos[1], siendo además que esta cifra que representa sólo aquellos delitos que son denunciados formalmente por las víctimas o su entorno:



Elaboración propia
Fuente: Boletines estadísticos PNP

Del mismo modo, el documento de trabajo denominado *Reporte de Ciberdelincuencia*, elaborado por el Ministerio de Justicia y Derechos Humanos y publicado en 2022, revela que la incidencia de los ciberdelitos viene creciendo de manera alarmante en el país, pasando de una incidencia de 2,917 delitos en 2018 a 14,671 en 2021. Siendo además que esta cifra solo representa aquellos delitos que son denunciados formalmente por las víctimas o su entorno.

[1] https://www.policia.gob.pe/estadisticopnp/documentos/anuario-2021/anuario-estadistico-policial-2021.pdf Pág. 32
https://www.policia.gob.pe/estadisticopnp/documentos/anuario-2022/anuario-estadistico-policial-2022.pdf Pág. 27
https://www.policia.gob.pe/estadisticopnp/documentos/boletin-2023/Boletin%20I%20Trimestre%202023.pdf Pág. 6



Fuente: Reporte Ciberdelincuencia, 2022

La situación anterior supone la necesidad de adoptar acciones desde el Estado, así como desde otros ámbitos como la sociedad civil y la academia, orientadas tanto a prevenir, como a investigar, perseguir y sancionar este tipo de delitos.

Ahora bien, resulta necesario distinguir entre los ciberdelitos puros, que en nuestro ordenamiento jurídico se denominan delitos informáticos, y los delitos facilitados por las tecnologías. Así, la Defensoría del Pueblo señala que mientras los primeros son los actos delictivos que tienen a las TIC como su objetivo o blanco específico, por cuanto son dependientes de las tecnologías[2] y donde la información es uno de los principales bienes jurídicos protegidos, al ser delitos de carácter pluriofensivo[3]; los segundos son delitos tradicionales facilitados por el uso de las TICS que se constituyen como herramientas que aumentan su volumen y alcance[4].

En ese contexto, precisa la Defensoría del Pueblo que la sola intervención o utilización de una tecnología no convierte a un delito tradicional en ciberdelito, por lo que es necesario reconocer aquellos tipos penales tradicionales o clásicos perfeccionados por el uso de las tecnologías para comprender los desafíos de cada uno, y así poder luchar contra ellos de manera efectiva. Algunos de estos retos son: el anonimato, la inmediatez, la masividad, la internacionalidad y las dificultades para la obtención de la evidencia digital, entre otros, aspectos que cobran relevancia en el ámbito de la investigación del delito.

2.2. Identificación del problema público

Ante el problema del incremento de ciberdelitos y delitos tradicionales cometidos a través de medios digitales, resulta importante fortalecer la persecución penal de los mismos, a través de precisiones en la tipificación de los delitos, las acciones de investigación y articulación entre entidades.

---

[2] Interpol (2021). Guía sobre la Estrategia Nacional contra la Ciberdelincuencia. Lyon, página 38.

[3] Delitos Informáticos, en Revista Ius et veritas, 49, diciembre del 2014, Lima, páginas 288-289

[4] Interpol (2021). Guía sobre la Estrategia Nacional contra la Ciberdelincuencia. Lyon, página 10.

Así, a continuación, se detallará la problemática actual en relación a cada propuesta de modificación que plantea el presente proyecto:

a) Problemática respecto al delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El artículo 5 de la Ley Nº 30096, Ley de Delitos Informáticos tipifica el delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos en los siguientes términos:

> ***"Artículo 5.- Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos***
>
> *El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal.*
>
> *Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal".*

PRESIDENCIA DEL CONSEJO DE MINISTROS
Secretaría de Gobierno y Transformación Digital

Cabe señalar que el tipo vigente data de la última modificación que se realizó a través de la Ley Nº 30838, en agosto del año 2018. En ese sentido, a continuación, se presenta una línea del tiempo que contiene las sucesivas modificaciones que se han efectuado a este tipo penal:

Tabla Nº 1: Desarrollo del delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

Ley 30096 "Ley de delitos informáticos" 22.10.2013	LEY Nº 30171, "Ley que modifica la Ley 30096, Ley de Delitos Informáticos" 10.03.2014	LEY Nº 30838, "Ley que modifica el Código Penal y el Código de Ejecución Penal para fortalecer la prevención y sanción de los delitos contra la libertad e indemnidad sexuales" 04.08.2018
Art. 5.- El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal	Art. 5.- El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.	Art. 5.- El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal"

Elaboración: Ministerio de la Mujer y Poblaciones Vulnerables

No obstante, de forma casi paralela, se tipificó el delito de proposiciones a niños, niñas y adolescentes con fines sexuales en el artículo 183-B del Código Penal, desde 2014 y hasta su última modificación en junio de 2019, conforme se puede apreciar a continuación:

Tabla N° 2: Desarrollo del delito de Proposiciones a niños, niñas y adolescentes con fines sexuales

Modificación del Código Penal LEY N° 30171, "Ley que modifica la Ley 30096, Ley de Delitos Informáticos" 10.03.2014	Modificación del Código Penal LEY N° 30838, "Ley que modifica el Código Penal y el Código de Ejecución Penal para fortalecer la prevención y sanción de los delitos contra la libertad e indemnidad sexuales" 04.08.2018	Modificación del Código Penal Ley 30963 Ley que modifica el Código Penal respecto a las sanciones del delito de explotación sexual en sus diversas modalidades y delitos conexos, para proteger con especial énfasis a las niñas, niños, adolescentes y mujeres 18.06.2019
Art. 183-B CP.- El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación de conforme a los numerales 1, 2 y 4 del artículo 36. Cuando la víctima tiene entre catorce y menos de dieciocho de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36.	Art. 183-B CP.-El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con pena privativa de libertad no menor de 6 ni mayor de 9 años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36. Cuando la víctima tiene entre 14 y menos de 18 años, y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36°.	Artículo 183-B El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con pena privativa de libertad no menor de seis ni mayor de nueve años. Cuando la víctima tiene entre catorce y menos de dieciocho años, y medie engaño, la pena será no menor de tres ni mayor de seis años. En todos los casos se impone, además, la pena de inhabilitación conforme al artículo 36, incisos 1, 2, 3, 4, 5, 6, 8, 9, 10 y 11

Elaboración: Ministerio de la Mujer y Poblaciones Vulnerables

Como se puede apreciar, la conducta típica del delito tipificado en el artículo 5 de la Ley de Delitos Informáticos únicamente difiere de la conducta típica del delito tipificado en el artículo 183-B del Código Penal en cuanto al medio empleado para contactar a una persona menor de edad, esto es por Internet u otro medio tecnológico. Esta es una situación atípica en nuestro ordenamiento jurídico. Acertadamente, un estudio temprano de 2014 apunta al hecho de que actualmente una misma conducta está tipificada en dos variantes; cuando ocurre a través de tecnologías digitales y cuando el contacto se realiza por medios no digitales, algo que no se da en otros países de la región que recogen esta figura.[5]

Otra diferencia importante entre el delito tipificado en el artículo 5 de la Ley de Delitos Informáticos y el artículo 183-B del Código Penal, es la pena privativa de libertad y la inhabilitación con la que son sancionados. Así, mientras el primero de ellos, en su tipo base, es sancionado con una pena privativa de la libertad conminada de 4 a 8 años e inhabilitación conforme a

[5] Hiperderecho (2014). Luces y sombras en la lucha contra la delincuencia informática en el Perú. Lima, página 18.

los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal, el segundo es sancionado, en su tipo base, con una pena privativa de libertad conminada de 6 a 9 años e inhabilitación conforme al artículo 36, incisos 1, 2, 3, 4, 5, 6, 8, 9, 10 y 11, conforme se puede apreciar en el siguiente cuadro:

Tabla Nº 3: Diferencias en cuanto a la pena entre el delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos y el delito de delito de Proposiciones a niños, niñas y adolescentes con fines sexuales

	Art. 5 Ley de Delitos Informáticos	Art. 183-B Código Penal
Pena privativa de la libertad Persona menor de 14 años	4 – 8 años	6 - 9 años
Pena privativa de la libertad Persona de entre 14 y menos de 18 años.	3 – 6 años	3 – 6 años
Pena limitativa de derechos	Inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal	Inhabilitación conforme al artículo 36, incisos 1, 2, 3, 4, 5, 6, 8, 9, 10 y 11 del Código Penal

Elaboración propia

PRESIDENCIA DEL CONSEJO DE MINISTROS
Secretaría de Gobierno y Transformación Digital

Una diferencia adicional en cuanto al proceso penal respecto a ambos tipos penales, radica en la disminución de la pena por confesión sincera, terminación anticipada o conclusión anticipada, en el marco del Código Procesal Penal – CPP, conforme se puede observar a continuación:

Tabla Nº 4: Diferencias en cuanto al beneficio de confesión sincera entre el delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos y el delito de delito de Proposiciones a niños, niñas y adolescentes con fines sexuales

	Art. 5 Ley de Delitos Informáticos	Art. 183-B Código Penal
Confesión sincera Disminución de la pena hasta en una tercera parte por debajo del mínimo legal (Art. 161 CPP)	Sí aplica, salvo excepciones del propio Art. 161 del CPP	Su aplicación está expresamente prohibida por el Art. 161 del CPP.
Conclusión anticipada Reducción de la pena (Art. 372 CPP)	Sí aplica	Su aplicación está expresamente prohibida por el Art. 372 del CPP

Reducción adicional acumulable **Reducción de la pena en una sexta parte** (Art. 471 CPP)	Sí aplica	Su aplicación está expresamente prohibida por el Art. 471 del CPP

Elaboración propia

Finalmente, con respecto a los beneficios penitenciarios, tenemos que el beneficio de redención de pena por trabajo, semi-libertad o libertad condicional no son procedentes para personas sentenciadas por la comisión del delito tipificado en el artículo 183-B del Código Penal, pero sí para las que lo son por la comisión del delito tipificado en el artículo 5 de la Ley de Delitos Informáticos:

Tabla N° 5: Diferencias en cuanto a beneficios penitenciarios entre el delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos y el delito de delito de Proposiciones a niños, niñas y adolescentes con fines sexuales

	Art. 5 Ley de Delitos Informáticos	Art. 183-B Código Penal
Redención de pena por trabajo (Art. 51 Código de Ejecución Penal)	Sí aplica	Su aplicación está expresamente prohibida por el Art. 51 del CPP.
Semi-libertad o libertad condicional (Art. 55 Código de Ejecución Penal)	Sí aplica	Su aplicación está expresamente prohibida por el Art. 55 del CPP

Elaboración propia

Es de observarse entonces que existen diferentes consecuencias jurídicas para la misma conducta ilícita, diferenciándose esta únicamente por el medio empleado para su comisión, lo que resulta contrario al principio de proporcionalidad en el sistema de justicia penal.

Esta situación plantea múltiples problemas en la aplicación de la ley, en principio porque dos personas que cometan el mismo acto podrían recibir penas muy diferentes simplemente porque se les acuse bajo diferentes disposiciones legales, lo que a su vez transgrede el principio de igualdad ante la ley. Pero también es el caso precisar que, en la actualidad, este delito podría cometerse en mayor medida utilizando los medios tecnológicos para contactar con niñas, niños y adolescentes; recibiendo, a pesar de ello, consecuencias jurídicas menos severas, pese a que el delito, al tener como sujeto pasivo a las niñas, niños y adolescentes, tiene como bien jurídico protegido la indemnidad sexual y la libertad sexual, respectivamente.

De acuerdo a cifras del INEI, para el primer trimestre del 2022, el 72,4% de niños en el país de entre 6 y 17 años hicieron uso del servicio de Internet, lo que representa un universo relativo de casi 7 millones de personas, que además representa un aumento de 6,3% frente a la medición del año anterior, lo que demuestra una tendencia al crecimiento[6]. Así mismo, una encuesta del Instituto de Estudios Peruanos (IEP), realizada por encargo de la organización CHS Alternativo, reveló que durante el 2022 unos 280,000 niñas, niños y adolescentes peruanas/os recibieron propuestas para tener relaciones sexuales por Internet.[7]

Esta situación da cuenta de la problemática actual, donde el internet y las tecnologías constituyen un espacio donde interactúan niñas, niños y adolescentes, y que a su vez podría constituir un riesgo si es que se utiliza ese mismo medio para tomar contacto con ellas/os con fines delictivos. No obstante, pese al incremento del uso de las tecnologías, el delito que considera dicho medio para cometer la conducta ilícita, es sancionado con menores penas que el delito general tipificado en el Código Penal.

En el caso presente, esto significa optar no solo por la tipificación que "beneficie" más a los agresores en términos de la pena, sino que implicaría la no aplicación de salvaguardas propias de ciertos sistemas de prevención, como las de la Ley N° 30364, Ley para prevenir, sancionar y erradicar la violencia contra las mujeres y los integrantes del grupo familiar, además de los mecanismos ya mencionados del Código Procesal Penal como la disminución de la pena por confesión sincera, terminación anticipada o conclusión anticipada.

A lo anterior hay que sumar la cantidad de casos investigados por los delitos anteriormente mencionados, conforme al reporte de la Oficina de Control de Productividad Fiscal del Ministerio Público, da cuenta que en el año 2022 se investigaron 262 casos por delito de Proposiciones a niños, niñas y adolescentes con fines sexuales, siendo que parte de ellos se hicieron bajo la figura tipificada en el artículo 183-B Código Penal y otros bajo a figura del artículo 5 de la Ley N° 30096, Ley de delitos informáticos, con lo que queda clara la necesidad de equiparar las consecuencias penales por la comisión de tales ilícitos, tomando en cuenta que estos únicamente se diferencian por el medio empleado, de manera que no resulta proporcional sancionar de manera más leve al delito cometido a través de medios tecnológicos, máxime cuando este es el entorno en que niñas, niños y adolescentes interactúan en mayor medida, por lo que es importante reforzar su protección en ese medio.

[6] INEI (2023). El 72,4% de la población de 6 a 17 años de edad accedió a internet.

[7] Andina. 280,000 niños y adolescentes en Perú recibieron propuestas para tener sexo por internet. Enlace: https://andina.pe/agencia/noticia-280000-ninos-y-adolescentes-peru-recibieron-propuestas-para-tener-sexo-internet-940568.aspx (Consultado por última vez: 05/10/2023)

b) Problemática respecto al delito de Suplantación de identidad

Según las cifras oficiales, luego del fraude informático, el delito de suplantación de identidad es el delito informático más recurrente en el país, pasando de un total de 935 denuncias en el 2020, hasta un total de 2 666 denuncias para el 2021[8].

La aparición de nuevas tecnologías digitales como la inteligencia artificial, están suponiendo un nuevo instrumento para la comisión de delitos, cuyas víctimas son menores de edad. El ejemplo que grafica esta situación son los casos recientes de niñas y adolescentes cuyas imágenes habrían sido presuntamente suplantadas para utilizarlas para crear videos de connotación sexual mediante el uso de herramientas de inteligencia artificial, por parte de sus compañeros de aula[9], casos que también han ocurrido en otras partes del mundo[10], ante el crecimiento exponencial del uso de la inteligencia artificial generativa.

Si bien el Perú ya ha regulado la suplantación de identidad en el artículo 9 de la Ley de delitos informáticos, se produce el desfase ya mencionado en el lenguaje y también la imposibilidad de aplicación a situaciones como las de las niñas y adolescentes víctimas del uso de *deepfakes*, que por su naturaleza no calificarían como casos de pornografía infantil tal como está regulada por el Código Penal, dado que las imágenes manipuladas no son "reales" y por lo tanto no se habría lesionado el bien jurídico de la indemnidad sexual (en caso de menores de 14 años) y libertad sexual (en caso de mayores de 14 años). A la luz de esta realidad, resulta conveniente adaptar la tipificación del delito para que recoja esta nueva realidad y permita combatir este fenómeno criminal de manera efectiva, con las garantías debidas.

c) Problemática respecto a la figura del agente encubierto en delitos informáticos

La Segunda Disposición Complementaria Final de la Ley Nº 30096, Ley de Delitos Informáticos establece:

SEGUNDA.- Agente encubierto en delitos informáticos
El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se

[8] Ministerio de Justicia y Derechos Humanos (2022). Reporte Ciberdelincuencia: Reporte de información estadística y recomendaciones para la prevención.
[9] Infobae. Chorrillos: Escolares que alteraron fotos de compañeras con IA y las comercializaron no fueron expulsados (2023). Enlace: https://www.infobae.com/peru/2023/08/29/chorrillos-escolares-que-alteraron-fotos-de-sus-companeras-con-ia-para-venderlas-no-fueron-expulsados/ (Consultado por última vez: 02/10/2023)
[10] El País. El caso de los desnudos con IA de Almendralejo se dispara: 26 menores implicados y 21 chicas afectadas. Enlace: https://elpais.com/sociedad/2023-10-03/el-caso-de-los-desnudos-con-ia-de-almendralejo-se-dispara-26-menores-implicados-y-21-ninas-afectadas.html (Consultado por última vez: 05/10/2023)

cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

De acuerdo a lo anterior, resulta necesario precisar esta figura con el propósito de establecer modificaciones sobre los dominios o entornos de aplicación, específicamente para admitir la posibilidad de la actuación de los agentes encubiertos en entornos digitales y los protocolos correspondientes.

d) Problemática en relación a la articulación de la PNP con la Secretaría de Gobierno y Transformación Digital

El Decreto Legislativo N° 1412, Ley de Gobierno Digital, señala en su artículo 8 que: "La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento." Posteriormente, en su artículo 9 desarrolla las funciones sobre estas materias:

Artículo 9.- Funciones del ente rector en materia de gobierno digital
La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector tiene las siguientes atribuciones:
9.1 Programar, dirigir, coordinar, supervisar y evaluar la aplicación de la materia de gobierno digital.
9.2 Elaborar y proponer normas reglamentarias y complementarias que regulan la materia de gobierno digital.
9.3 Elaborar lineamientos, procedimientos, metodologías, modelos, directivas u otros estándares de obligatorio cumplimiento para la implementación de las materias de gobierno digital.
9.4 Emitir opinión vinculante sobre el alcance, interpretación e integración de normas que regulan la materia de gobierno digital.
9.5 Emitir opinión previa a fin de validar técnicamente proyectos de tecnologías digitales de carácter transversal en materia de interoperabilidad, seguridad digital, identidad digital, datos, arquitectura digital o aquellos destinados a mejorar la prestación de servicios digitales.
9.6 Brindar apoyo técnico a las entidades públicas en la gestión e implementación de tecnologías digitales.
9.7 Definir los alcances del marco normativo en materia de gobierno digital.
9.8 Supervisar y fiscalizar, cuando corresponda, el cumplimiento del marco normativo en materia de gobierno digital.
9.9 Promover mecanismos que aseguren la identidad digital como pilar fundamental para la inclusión digital y la ciudadanía digital.
9.10 Promover y gestionar la implementación de proyectos de implementación de tecnologías digitales u otros mecanismos destinados a

mejorar la prestación de servicios digitales, en coordinación con las entidades públicas, según corresponda.
9.11 Promover la digitalización de los procesos y servicios a partir del uso e implementación de tecnologías digitales.
9.12 Realizar acciones de coordinación y articulación con representantes de la administración pública, ciudadanos u otros interesados con la finalidad de optimizar el uso de tecnologías digitales para el desarrollo del gobierno digital y tecnologías digitales. (El subrayado es nuestro)

La forma en que se han manifestado el ejercicio de las facultades anteriores ha sido diversa. Por un lado, la Secretaría de Gobierno y Transformación Digital ha desarrollado un conjunto de plataformas transversales para el uso de las entidades públicas, como es el caso de la Plataforma Digital Única del Estado Peruano para orientación al ciudadano (Gob.pe); la Plataforma Nacional de Datos Abiertos; y, Plataforma Nacional de Datos Georreferenciados Geo Perú. Por el otro lado, ha emitido normas de aplicación interna como la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, Resolución que aprueba el plan de implementación del Sistema de Gestión de Seguridad de la Información en las entidades públicas, asignación de un responsable y la creación de un equipo técnico multidisciplinario.

Precisamente en este último caso, normas con rango reglamentario que desarrollan las materias sobre las cuales la Secretaría de Gobierno y Transformación Digital tiene rectoría, han dispuesto que, en ciertas situaciones, esta entidad coordina y produce diferentes protocolos para el uso y despliegue de tecnologías digitales. Por ejemplo, lo que señala el artículo 100 del Reglamento de la Ley de Gobierno Digital:

Artículo 100. Ámbito de Justicia
100.1 Las acciones para garantizar la lucha eficaz contra la ciberdelincuencia es dirigida por el Ministerio del Interior (MININTER) y la Policía Nacional del Perú (PNP), quienes articulan con el Ministerio de Justicia y Derechos Humanos (MINJUSDH), el Instituto Nacional Penitenciario (INPE), el Ministerio Público - Fiscalía de la Nación, el Tribunal Constitucional, Academia de la Magistratura, la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros y el Poder Judicial (PJ), conforme a lo dispuesto en la Ley N° 30096, Ley de Delitos Informáticos, y los convenios aprobados y ratificados por el Estado Peruano en esta materia (...) (El subrayado es nuestro)

En ese orden de ideas, es preciso señalar que dicha articulación respecto del uso de las tecnologías digitales, especialmente en materia de ciberdelincuencia, con énfasis en la que afecta a los niños, niñas y adolescentes, no viene siendo efectiva, siendo esto consecuencia, en parte, de un bajo nivel de coordinación, entre las entidades involucradas en la Ley de delitos informáticos.

2.3. Situación futura deseada con la propuesta normativa

La situación futura deseada con la propuesta normativa es promover el uso seguro y responsable de las tecnologías digitales por niños, niñas y adolescentes, mediante el fortalecimiento de la persecución penal, de manera que se brinde una mayor y mejor protección a las víctimas de tales delitos, especialmente si se trata de niñas, niños y adolescentes, así como y se evite la impunidad respecto a tales delitos.

2.4. Identificación de los objetivos relacionados con el problema público

Para el logro de la situación futura deseada con la propuesta normativa, y teniendo en cuenta los problemas públicos desarrollados, se plantean los siguientes objetivos:

Tabla N° 6. Objetivos de la propuesta normativa

Óptica de la Administración Pública	Óptica del ciudadano
La tipificación del delito informático de suplantación de identidad, establecida en el artículo 9 de la Ley N° 30096, Ley de delitos informáticos, es más precisa en cuanto a la terminología utilizada, la misma que es desarrollada en la normatividad de gobierno y transformación digital	La ciudadanía cuenta con una protección mejor determinada en cuanto a la comisión de tales ilícitos, con una regulación penal que responde a los nuevos retos generados por los desarrollos tecnológicos.
La tipificación del delito de suplantación de identidad incluye la protección especial de las niñas, niños y adolescentes víctimas de tales delitos, mediante la incorporación de una circunstancia agravante por rango etario.	Las niñas, niños y adolescentes gozan de una mayor protección frente a la suplantación de su identidad en el ámbito digital, en atención al interés superior del niño y considerando la expansión de diversas tecnologías como la inteligencia artificial.

PRESIDENCIA DEL CONSEJO DE MINISTROS
Secretaría de Gobierno y Transformación Digital

Los operadores de justicia cuentan con mayor claridad al momento de investigar, procesar y sancionar el delito de Proposiciones a niños, niñas y adolescentes con fines sexuales, superando una situación de antinomia.	Las sanciones y consecuencias jurídicas por la comisión del delito de Proposiciones a niños, niñas y adolescentes con fines sexuales son proporcionales a la naturaleza del delito y daño causado, con prescindencia del medio empleado para su comisión, con lo que se refuerza la protección a las niñas, niños y adolescentes.
Los operadores de justicia encargados de la investigación del delito pueden actuar en el ámbito digital para investigar de manera más proactiva el delito.	Se reduce la impunidad de los delitos informáticos o cometidos a través de medios digitales o que precisen de una investigación en el ámbito digital, obteniendo una respuesta adecuada y oportuna ante la comisión del delito.
El Ministerio Público, Policía Nacional del Perú y, cuando corresponda, el Poder Judicial, cuentan con la asistencia técnica de la Secretaría de Gobierno y Transformación Digital para una mejor articulación en cuanto a los protocolos de investigación de delitos en el ámbito tecnológico.	Se fortalece la seguridad digital y se obtiene una respuesta estatal integral y articulada ante la comisión de delitos informáticos o cometidos por medios digitales.

PRESIDENCIA DEL CONSEJO DE MINISTROS
Secretaría de Gobierno y Transformación Digital

2.5. Análisis sobre la necesidad, viabilidad y oportunidad de la propuesta normativa

La necesidad de los cambios propuestos y aprobados a través del otorgamiento de facultades de la Ley N° 31880, Ley que delega facultades legislativas al Ejecutivo en materia de seguridad ciudadana gestión del riesgo de desastres-niño global, infraestructura social, calidad de proyectos y meritocracia, está fundamentada principalmente en dos hechos concurrentes: El primero de ellos es que la delincuencia informática o ciberdelincuencia se encuentra en aumento en nuestro país, especialmente a partir de la pandemia de COVID-19, que provocó un uso más intensivo de las tecnologías de información y comunicación.[11] El segundo es que existen diferentes estudios, informes y otros documentos de trabajo como los mencionados en el análisis contextual, que han determinado que los niños, niñas y adolescentes son un grupo etario especialmente vulnerable a esta realidad, por lo que se requieren tomar medidas específicas de prevención, contingencia y sanción.

[11] Defensoría del Pueblo (2023). Informe Defensorial N° 001-2023-DP/ADHPD, La ciberdelincuencia en el Perú: Estrategias y retos del Estado

Con relación a la viabilidad y oportunidad de la propuesta normativa se analiza lo siguiente:

- **Viabilidad política**, entendida como la consistencia de la propuesta normativa con las Políticas Nacionales. Al respecto, en el numeral 6 del presente Documento se desarrolla la vinculación de la modificación con las políticas nacionales vigentes.

- **Viabilidad legal**, que se refiere a la capacidad para implementar la propuesta normativa, el proyecto cuenta con coherencia normativa la cual se desarrolla en el numeral 5 del presente Documento.
- **Viabilidad de recursos,** conforme se establece en el numeral 4 del presente documento, la propuesta regulatoria no genera gastos adicionales al tesoro público.
- **Oportunidad de la propuesta normativa,** dado el otorgamiento de facultades por parte del Congreso de la Republica, resulta necesario y oportuno realizar las modificaciones a la Ley N° 30096, Ley de Delitos Informáticos y el Código Procesal Penal, aprobado por Decreto Legislativo N° 957, conforme fue desarrollado en el numeral 4 del presente documento con la finalidad de mantener la coherencia normativa en el ordenamiento jurídico vigente.

PRESIDENCIA DEL CONSEJO DE MINISTROS
Secretaría de Gobierno y Transformación Digital

III. CONTENIDO DE LA PROPUESTA NORMATIVA

a) Respecto al delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

Atendiendo a la problemática anteriormente descrita en relación a este delito tipificado en el artículo 5 de la Ley Nº 30096, Ley de Delitos Informáticos y el delito de proposiciones a niños, niñas y adolescentes con fines sexuales, tipificado en el artículo 183-B del Código Penal, delitos que, si bien sancionan la misma conducta ilícita, se diferencian en cuanto al medio empleado; se propone equiparar las consecuencias penales de ambos tipos penales, considerando la importancia de contar con un tipo penal que sancione específicamente el delito en el ámbito tecnológico debido a las características particulares de su comisión en dicho entorno y, por ende, en la investigación para identificar a los/as responsables de su comisión, en los siguientes términos:

Texto original	Propuesta de modificación
Artículo 5.- Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos El que a través de internet u otro medio análogo contacta con un	**Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos** El que a través de internet u otro medio análogo contacta con un

menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2, 4 y 9 del artículo 36 del Código Penal".	menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad **no menor de seis ni mayor de nueve años**. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años. **En todos los casos se impone, además, la pena de inhabilitación conforme a los numerales 1, 2, 3, 4, 5, 6, 8, 9, 10 y 11 del artículo 36 del Código Penal.**

PRESIDENCIA DEL CONSEJO DE MINISTROS
Secretaría de Gobierno y Transformación Digital

De esa manera, se equipara las consecuencias penales del delito tipificado en el artículo 5 de la Ley N° 30096 con las del ilícito comprendido en el artículo 183-B del Código Penal, de manera que se refuerza la protección a las niñas, niños y adolescentes en el ámbito digital.

Asimismo, se incluye una disposición complementaria final en el proyecto de Decreto Legislativo, orientada a la misma finalidad ya mencionada de equiparar las consecuencias penales entre el artículo 183-B del Código Penal y el artículo 5 de la Ley N° 30096, debido a que sancionan la misma conducta, con la única diferencia del medio empleado, pero que aun así son necesarias debido a las especificidades de la investigación en medios digitales que requiere este último delito; de manera que, de acuerdo al principio de proporcionalidad, ello también debe incluir las prohibiciones en términos del proceso penal y de la ejecución penal:

-	**Propuesta**
-	**Disposición Complementaria Final Única. –** Las improcedencias a las que hacen referencia los artículos 161, 372 y 471 del Código Procesal Penal, aprobado con Decreto Legislativo 957 y los artículos 51 y 55 del Texto Único Ordenado del Código de Ejecución Penal, aprobado con Decreto Supremo Nro. 003-2021-JUS, respecto al artículo 183-B del

	Código Penal, aprobado por el Decreto Legislativo N° 635, son también aplicables a la comisión del delito establecido en el artículo 5 de la Ley N°30096, Ley de Delitos Informáticos.

b) Respecto al delito de Suplantación de identidad

El Perú ha mostrado interés en adaptar su marco legal en materia de cibercrimen, incluyendo aquellos delitos especiales cuyas víctimas son menores de edad. Así pues, desde el 2022 el Perú se encuentra participando de la negociación de una Convención sobre ciberdelitos en las Naciones Unidas. Este proceso, que se encuentra actualmente en su fase final, marcará un hito importante en lo que respecta a la lucha contra la ciberdelincuencia en el mundo. Parte de esta negociación ha incluido la discusión sobre la creación o actualización de nuevos tipos penales teniendo como base el Convenio de Budapest. Precisamente una de las categorías de especial discusión ha sido la que concierne a los delitos que afectan a menores de edad, en las que el Perú ha presentado su aproximación, buscando recoger mejores prácticas y apoyando propuestas alineadas con la visión del país y el compromiso con el régimen democrático y el respeto de los derechos humanos.

En ese contexto, se han revisado múltiples propuestas, incluyendo de países de la región y que forman parte del Convenio de Budapest, las que apuntan a refinar la tipificación de los delitos informáticos (también llamados ciberdependientes) y los delitos ciberhabilitados, para incluir la regulación de conductas delictivas que empiezan a incrementarse a propósito del uso de tecnologías novedosas, siendo uno de estos casos la proliferación de los *deepfakes* o suplantación de identidad mediante el uso de inteligencia artificial[12].

Así pues, los cambios propuestos consisten en actualizar el término "tecnologías de información o de comunicación" por "tecnologías digitales" que incluyen el uso de tecnologías emergentes como la inteligencia artificial, conforme al Decreto Legislativo N° 1412, Ley de Gobierno Digital:

Artículo 3.- Definiciones
Para efectos de la presente Ley, se adoptan las siguientes definiciones:

1. *Tecnologías Digitales.- Se refieren a las Tecnologías de la Información y la Comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.*

[12] Chatham House (2022). Cybercrime convention could help and harm victims. Enlace: https://www.chathamhouse.org/2022/07/cybercrime-convention-could-help-and-harm-victims

En la misma línea, el Informe de opinión técnica vinculante Nº 002-2023-SSTSD de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros[13], en su calidad de ente rector del Sistema Nacional de Transformación Digital[14], define tecnologías digitales como:

- Son las tecnologías de la información y comunicaciones - TIC, que incluye internet, tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, eso, búsqueda y presentación de datos, información, contenido digital, incluido el desarrollo de servicios y aplicaciones.

- Son las tecnologías capaces de generar soluciones innovadoras tales como la robótica, la analítica, la inteligencia artificial, las tecnologías cognitivas, la nanotecnología y el Internet de las cosas (IoT), entre otras, que conforman la industria 4.0 como la nueva revolución que combina técnicas avanzadas de producción y operaciones con tecnología, generando un impacto en el ecosistema digital, las organizaciones y las personas.

Asimismo, atendiendo a la problemática contextual respecto al uso de internet y tecnologías digitales por niñas, niños y adolescentes, también se propone la inclusión de una agravante del tipo base, que se concretará cuando la suplantación se realice sobre un sujeto pasivo menor de 18 años, siempre que de la conducta resulte un tipo de daño material, moral o de cualquier otra índole, como también se propone en el tipo base.

En efecto, conforme fue descrito en la problemática, la aparición de nuevas tecnologías digitales como la inteligencia artificial, están suponiendo un nuevo instrumento para la comisión de delitos, cuyas víctimas son menores de edad. Casos como el de las niñas y adolescentes cuyas imágenes habrían sido presuntamente suplantadas para utilizarlas para crear videos de connotación sexual mediante el uso de herramientas de inteligencia artificial, por parte de sus compañeros de aula[15], puede llegar a ser cada vez más comunes si es que no se cuenta con legislación que contribuya a frenar este tipo de conductas especialmente perjudiciales para las niñas, niños y adolescentes.

Sin embargo, es necesario considerar que el tipo de conducta antes señalada y la creación de perfiles falsos en redes sociales, no es la única forma en que las personas menores de edad pueden ser víctimas de

[13] Disponible en: https://cdn.www.gob.pe/uploads/document/file/4338064/Informe%20de%20Opini%C3%B3n%20T%C3%A9cnica%20Vinculante-000002-2023-PCM-SGTD-SSPRD.pdf?v=1680052794

[14] Conforme al Decreto de Urgencia Nº 006-2020.

[15] Infobae. Chorrillos: Escolares que alteraron fotos de compañeras con IA y las comercializaron no fueron expulsados (2023). Enlace: https://www.infobae.com/peru/2023/08/29/chorrillos-escolares-que-alteraron-fotos-de-sus-companeras-con-ia-para-venderlas-no-fueron-expulsados/ (Consultado por última vez: 02/10/2023)

suplantación de su identidad, pues el crecimiento exponencial de las tecnologías también da lugar a nuevas formas que se han detectado en otros países.

Así, el estudio publicado en el año 2021 por la empresa de investigación estadounidense Javelin Strategy & Research[16], arrojó como resultado que uno de cada cincuenta niños en Estados Unidos fueron víctimas de suplantación o fraude de identidad, muchas veces debido a sus limitados historiales financieros, que brindan a la ciberdelincuencia una oportunidad a largo plazo para desarrollar lentamente redes de cuentas, imitando posesiones legítimas.

Esta situación puede extenderse en tanto exista más permisibilidad en el acceso a cuentas bancarias para niñas, niños y adolescentes, así como un acceso a internet sin las condiciones de seguridad debidas; pudiendo también suscitarse suplantación en plataformas de distintos servicios, incluyendo las de apuestas por internet, sobre todo, si a ello le sumamos que, de acuerdo al estudio publicado en la Society for Developmental and Behavioral Pediatrics (Sociedad para el desarrollo y comportamiento pediátrico), citado en el informe de la UNESCO sobre "Seguridad de los niños en línea: Minimizando el riesgo de la violencia, el abuso y la explotación en línea", de octubre de 2019 se encontró que casi todas las apps dirigidas a niños contienen publicidad, mucha de la cual los investigadores describen como "manipuladora", el referido informe también indica que el uso frecuente de anuncios emergentes que interrumpen el juego y personajes del juego que invitan a los niños a realizar compras voluntaria o involuntariamente

PRESIDENCIA DEL CONSEJO DE MINISTROS
Secretaría de Gobierno y Transformación Digital

En tal sentido, la legislación propuesta plantea dar respuesta frente a situaciones y así combatir el fenómeno criminal de la suplantación de identidad, desde el ámbito punitivo, de manera efectiva y en observancia del principio de interés superior del niño, brindándole una protección reforzada.

Finalmente, con respecto a la pena, recogemos lo expuesto en el artículo VIII del Título Preliminar del Código Penal sobre la proporcionalidad de las penas y justificamos la necesidad del incremento de la pena a partir del criterio de "grado de nocividad social de la conducta incriminada", desarrollado en el IV Pleno Jurisdiccional Penal Nacional del año 2000. Esto por cuanto se espera que el nuevo agravante tenga un efecto disuasorio y proteja a este grupo etario, haciendo que las consecuencias jurídicas sean proporcionales a la gravedad del delito cometido, considerando la condición de vulnerabilidad de los sujetos pasivos.

Por lo dicho, anteriormente, se proponen los siguientes cambios:

[16] Child Identity Fraud: A Web Of Deception And Loss. Javelin. Noviembre de 2021. Disponible en: https://www.aarp.org/content/dam/aarp/money/scams_fraud/2022/03/child-identity-fraud-study-2022.pdf Consultado el 30.11.2023.

Texto original	Propuesta de modificación
Artículo 9. Suplantación de identidad El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.	**Artículo 9. Suplantación de identidad** El que, mediante las tecnologías **digitales** suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material, moral **o de cualquier otra índole**, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. **La pena privativa de libertad es no menor de seis ni mayor de nueve años cuando se suplante la identidad de una persona menor de 18 años de edad y resulte algún perjuicio, material, moral o de cualquier otra índole."**

c) Respecto a la figura del agente encubierto

Se está proponiendo la clarificación de los ámbitos de aplicación, independientemente de los delitos a los cuales se puede aplicar la figura.

Así, con la introducción del lenguaje "incluso si estas acciones deben realizarse en entornos digitales" se clarifica que las acciones a ser autorizadas para los agentes encubiertos pueden incluir aquellas realizadas en Internet u otras tecnologías digitales.

La incorporación de que las acciones del agente encubierto[17] puedan efectuarse en el ámbito digital, virtual o tecnológico, responde a la necesidad de que las técnicas especiales de investigación puedan ser aplicadas a la actual delincuencia que se vale de medios informáticos o que los ataca para fines ilícitos; esta inclusión facultará a que el agente encubierto pueda adquirir, transportar o diferir la incautación de instrumentos delictivos que surgen o empleen medios informáticos a través de internet[18], aplicaciones en línea o cualquier método que utilice tecnologías digitales de la información o de la comunicación. Por ello, se plantean las siguientes modificaciones en la

[17] A nivel internacional, el agente encubierto ha sido empleado para lograr el conocimiento de los casos de redes de delitos diversos, los mismos que han empleado medios digitales (correos electrónicos, mensajería por aplicaciones, entre otros) se tiene, por ejemplo, los casos: United States of America v. Eoin Leng Churn Yeng and Gal Vin Yeo Siang Ann, (Distrito de Oregón, 23 de febrero de 2016) (Estados Unidos de América); BGH, Beschluss, StR 321/19 (Alemania), Tribunal Penal del Tercer Circuito Judicial de San José, causa penal número 15-001824-0057-PE y causa penal número 19-000031-0532-PE (Operación R-INO) (Costa Rica). Disponibles en el Compendio de Ciberdelincuencia organizada de la UNODC, recuperado de https://www.smv.gob.pe/ConsultasP8/temp/Compendio%20de%20Ciberdelincuencia%20Organizada%20%20UNO DC%20%202022.pdf

[18] Guía Didáctica de Ciberdelincuencia. Organización de las Naciones Unidas (Viena, 2020), p. 47. a) Delitos dependientes de la cibernética. Un delito cibernético que no podría ser posible sin internet y las tecnologías digitales; b) Delitos propiciados por medios cibernéticos. Un delito cibernético facilitado por internet y las tecnologías digitales. Recuperado de https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Teaching_Guide_ES_final.pdf.

Segunda Disposición Complementaria Final de la Ley N° 30096, Ley de Delitos Informáticos:

Texto original	Propuesta de modificación
Segunda Disposición Complementaria Final de la Ley Nº 30096, Ley de Delitos Informáticos **SEGUNDA.- Agente encubierto en delitos informáticos** El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.	**Segunda Disposición Complementaria Final de la Ley Nº 30096, Ley de Delitos Informáticos** **SEGUNDA.- Agente encubierto en delitos informáticos** El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, **incluso si estas acciones deben realizarse en entornos digitales,** y con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957. **Los protocolos para la actuación del agente encubierto en entornos digitales, tanto en el marco de la presente Ley, como en el marco del artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957, son coordinados, en cuanto corresponda, con la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en concordancia con las normas vigentes que regulan el Sistema Nacional de Transformación Digital."**

Cabe acotar que la figura del agente encubierto solo es posible aplicar de forma subsidiaria y en los supuestos necesarios; así lo ha detallado el Tribunal Constitucional en el Expediente N° 4750-2007-PHC-TC

(fundamento 17), el cual menciona que al regular la actuación del agente encubierto en escenarios digitales, debe tenerse en cuenta los principios de necesidad y subsidiariedad mencionados, en tanto que, como lo refiere la Sentencia del Tribunal Supremo Español su empleo puede involucrar la afectación a diversos derechos como la intimidad y el mismo derecho al entorno virtual[19]; de ahí que resulta necesario determinar además los límites del mencionado entorno digital.

d) Articulación de la Policía Nacional del Perú y el Ministerio Público con la Secretaría de Gobierno y Transformación Digital

En los últimos años, diferentes normas han establecido mecanismos más precisos para atender problemas derivados de la ciberdelincuencia, como el Decreto Legislativo N° 1412, Ley de Gobierno Digital; y los Decretos de Urgencia N° 006-020, que Crea el Sistema Nacional de Transformación Digital y Decreto de Urgencia N° 007-2020, que Crea el Marco de Confianza Digital y dispone medidas para su fortalecimiento. Estas normas, que desarrollan materias como la confianza digital y la seguridad, incluyen el ámbito de justicia, específicamente el de ciberdelitos, creando diferentes obligaciones de coordinación entre los actores del sector público.

En ese contexto, normas como el Decreto Supremo N° 029-2021-PCM, Reglamento de la Ley de Gobierno Digital, establecen en su artículo 100 delimita de forma explícita el ámbito de justicia, que forma parte del Marco de Seguridad Digital y señala que la entidad rectora en dicha materia es la Secretaría de Gobierno y Transformación Digital, incluyendo ciertas actuaciones especiales en materia de víctimas de la ciberdelincuencia que son niños, niñas y adolescentes:

Artículo 100. Ámbito de Justicia
100.1 Las acciones para garantizar la lucha eficaz contra la ciberdelincuencia es dirigida por el Ministerio del Interior (MININTER) y la Policía Nacional del Perú (PNP), quienes articulan con el Ministerio de Justicia y Derechos Humanos (MINJUSDH), el Instituto Nacional Penitenciario (INPE), el Ministerio Público - Fiscalía de la Nación, el Tribunal Constitucional, Academia de la Magistratura, la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros y el Poder Judicial (PJ), conforme a lo

[19] STS 816/2021 del 4 de marzo de 2021, Tribunal Supremo. Sala de lo Penal de España, ha sostenido respecto a la aplicación de la figura del agente encubierto, que "Hay principios no negociables (prohibición de la tortura, secreto de las comunicaciones salvo autorización judicial...). Pero aparecen otras cuestiones, especialmente algunas atinentes a derechos de nueva generación (autodeterminación informativa, derecho al entorno virtual), o en que confluyen derechos e intereses variados y contrapuestos (v.gr., infiltración policial como método de investigación) conformando una encrucijada susceptible de matices y modulaciones, en que las legislaciones nacionales presentan divergencias (quién debe autorizar la técnica del agente infiltrado -policía, fiscal o autoridad judicial-, v.gr). Estas propician mayor permeabilidad transfronteriza. No está legitimado un Estado para exigir que las actuaciones de otros países se atengan a su específica legislación cuando las soluciones admisibles, y respetuosas todas en lo esencial con la tutela del derecho fundamental, pueden ser variadas". Recuperado de https://www.poderjudicial.es/search/AN/openDocument/a1ee550df62101d7/20210317

dispuesto en la Ley Nº 30096, Ley de Delitos Informáticos, y los convenios aprobados y ratificados por el Estado Peruano en esta materia.
100.2 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en coordinación con la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú y el Ministerio Público-Fiscalía de la Nación proponen los protocolos de colaboración y comunicación para el reporte de casos de violencia sexual contra niños, niñas y adolescentes en el entorno digital, la cual se hace efectiva mediante Resolución de la Secretaría de Gobierno Digital. (El subrayado es nuestro)

Teniendo en cuenta lo dispuesto anteriormente, resulta necesario que esta capacidad de coordinación se exprese en la Ley de Delitos Informáticos, en los siguientes términos:

Texto original	Propuesta de modificación
DISPOSICIONES COMPLEMENTARIAS FINALES TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, el centro de respuesta temprana del gobierno para ataques cibernéticos (Pe-CERT), la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad.	**DISPOSICIONES COMPLEMENTARIAS FINALES** TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, **la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros** y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad.

IV. ANÁLISIS DE IMPACTOS CUANTITATIVOS Y/O CUALITATIVOS

4.1. Beneficios que genera la propuesta normativa

En el extremo del análisis cualitativo, los beneficios son significativos puesto que permitirá:

- Fortalecimiento de la investigación de delitos informáticos y cometidos en el entorno digital.
- Mayor protección de la ciudadanía que es víctima de delitos informáticos, con énfasis en los niños, niñas y adolescentes quienes, por su edad y exposición al internet y tecnologías digitales, se encuentran en condición de mayor vulnerabilidad a ser víctimas que los afectan especialmente, como las proposiciones sexuales o la suplantación de identidad.

SUJETO	EFECTO	SUSTENTO
Estado Peruano	Se fortalece la prevención, investigación y sanción frente a delitos cometidos mediante el uso de tecnologías digitales, en los que conciernen a niñas, niños y adolescentes como víctimas, para garantizar su protección. Asimismo, se fortalece la transformación digital a través de la articulación de la PNP y el Ministerio Público con la Secretaría de Gobierno y Transformación Digital, en su rol rector del Sistema Nacional de Transformación Digital.	Se perfeccionan los tipos penales relacionados con las proposiciones sexuales y suplantación de identidad de niñas, niños y adolescentes. Se garantiza que la figura del agente encubierto en el marco de la Ley N° 30096 también actúe en entornos digitales.
Ciudadanía	Generación de un ambiente favorable para el ejercicio de los derechos fundamentales de las personas, con especial protección a las niñas, niños y adolescentes.	Mayor protección frente a delitos cometidos en el ámbito digital que acechan a la ciudadanía, en especial a las niñas, niños y adolescentes.

4.2. Costos que genera la propuesta normativa

SUJETO	EFECTO	SUSTENTO
Estado Peruano	Presupuesto público existente	Las actividades de las entidades responsables para el ejercicio funcional, están debidamente previstas, no adicionándose otras

		labores que demanden gastos extraordinarios.

V. ANÁLISIS DE IMPACTO DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL

5.1. Análisis de la concordancia de la propuesta normativa con la Constitución y la legislación nacional

La Constitución Política del Perú señala en su artículo 1 que "la defensa de la persona humana y el respeto de su dignidad son el fin supremo del Estado y la sociedad". A continuación, en su artículo 2, desarrolla una lista abierta de derechos nominados, siendo de especial relevancia para esta propuesta el artículo 2, incisos 4 y 22 que señalan que:

Artículo 2. Toda persona tiene derecho:

(...)

4. A las libertades de información, opinión, expresión y difusión del pensamiento mediante la palabra oral o escrita o la imagen, por cualquier medio de comunicación social, sin previa autorización ni censura ni impedimento algunos, bajo las responsabilidades de ley.

El Estado promueve el uso de las tecnologías de la información y la comunicación en todo el país.

Los delitos cometidos por medio del libro, la prensa y demás medios de comunicación social se tipifican en el Código Penal y se juzgan en el fuero común.

(...)

22. A la paz, a la tranquilidad, al disfrute del tiempo libre y al descanso, así como a gozar de un ambiente equilibrado y adecuado al desarrollo de su vida. (El subrayado es nuestro)

Se tiene pues que nuestra Constitución otorga una especial atención a la promoción del uso de la tecnología por parte del Estado que, entendiéndose en su contexto de conexión con los demás derechos, debe darse en armonía con la satisfacción del derecho a la paz, tranquilidad y a gozar de un ambiente equilibrado y adecuado. Ahora bien, aunque esta redacción es general, es posible identificar en la misma Constitución referencias a grupos de especial interés en cuanto al cumplimiento de estos mandatos. Por ejemplo, en el artículo 4 se establece que "la comunidad y el Estado protegen especialmente al niño, al adolescente, a la madre y al anciano en situación de abandono".

En consecuencia, el presente proyecto no contraviene la Constitución Política del Perú, toda vez que no amenaza, recorta, afecta ni vulnera derechos; tampoco contraviene disposición legal vigente en el ordenamiento jurídico nacional, pues, por el contrario, se orienta a contribuir con la promoción el uso seguro y responsable de las tecnologías digitales para la protección de niños, niñas y adolescentes, en este caso, desde el ámbito penal y de coordinación con la Secretaría de Gobierno y Transformación

Digital de la Presidencia de Ministros, como ente rector del Sistema Nacional de Transformación Digital.

Asimismo, la propuesta normativa es concordante con las siguientes disposiciones normativas, para mantener la congruencia en el ordenamiento jurídico:

- Ley N° 29158, Ley Orgánica del Poder Ejecutivo.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Legislativo Nº 635, Código Penal
- Decreto Legislativo Nº 957, Código Procesal Penal
- Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
- Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, aprobado por Decreto Supremo N° 029-2021-PCM, en delante Reglamento de la Ley de Gobierno Digital.
- Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, aprobado por Decreto Supremo N° 157-2021-PCM
- Texto Único Ordenado del Código de Ejecución Penal, Decreto Supremo Nº 003-2021-JUS.
- Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Resolución Ministerial N° 224-2023-PCM.

Del mismo modo, la propuesta normativa guarda coherencia con la Política Nacional Multisectorial para las Niñas, Niños y Adolescentes (PNMNNA), aprobada mediante Decreto Supremo N° 008-2021-MIMP, en lo que respecta a al incremento en niñas, niños y adolescentes de los conocimientos y recursos para identificar, prevenir y denunciar diferentes formas de violencia para garantizar su protección; así como a la Política Nacional de Transformación Digital al 2030, aprobada mediante Decreto Supremo Nº 085-2023-PCM, en cuanto a garantizar la seguridad y confianza digital en el país para fortalecer las capacidades que permitan identificar, gestionar, tratar y mitigar los riesgos de seguridad digital y tiene un especial énfasis en protección de niños, niñas y adolescentes de riesgos digitales (OP5).

5.2. Impacto de la vigencia de la propuesta normativa en la legislación vigente

El presente proyecto realiza las siguientes modificaciones sobre:

1) La Ley Nº 30096, Ley de delitos informáticos: Precisando los delitos de grooming y suplantación de identidad. También al empleo del agente encubierto y al deber de coordinación con la Secretaría de Gobierno y Transformación Digital.

5.3. Revisión de la propuesta por otros sectores

La Secretaría de Gobierno y Transformación Digital, mediante reuniones de trabajo colaborativas y Oficio Múltiple N° D000014-2023-PCM-SGTD solicitó opinión a los sectores competentes para opinar sobre las materias que comprende el proyecto de Decreto Legislativo que nos ocupa, obteniendo las siguientes respuestas:

- Correo electrónico de fecha 29.09.2023 de la Dirección General contra el Crimen Organizado del Ministerio del Interior: Se indica que, haciendo una revisión básica, la propuesta de la SGTD no se superpondría al contenido de la propuesta sobre delitos informáticos que trabaja MININTER.

- Oficio N° 005683-2023-MP-FN-SEGFIN de fecha 03.11.2023 del Ministerio Público, trasladando el Informe N° 000003-2023-MP-FN-UFEC, a través del cual se realizan aportes respecto a los artículos 5 y 8 de la Ley Nº 30096, Ley de Delitos Informáticos, considerados en la presente propuesta. El Ministerio Público brinda opinión favorable al resto de la propuesta.

- Oficio N° D002160-2023-MIMP-SG de fecha 09.11.2023 del Ministerio de la Mujer y Poblaciones Vulnerables, traslada los informes N° D000959-2023-MIMP-OGAJ y D0000-2023-MIMP- DPNNA-ERA, a través de los cuales brinda opinión previa favorable al proyecto de Decreto Legislativo, en cuanto concierne a sus competencias, sugiriendo se realicen precisiones a la exposición de motivos, las mismas que se han efectuado.

- Oficio N° 0960-2023-JUS/GA del Ministerio de Justicia y Derechos Humanos, de fecha 17.11.2023, a través del cual se remitió el Informe N° 092-2023-ST/CEI-CPP, elaborado por la Secretaría Técnica de la Comisión Especial de Implementación del Código Procesal Penal, de Informe Legal N° 188-2023-JUS/DGDNCR, elaborado por la Dirección General de Desarrollo Normativo y Calidad Regulatoria, y el Informe Técnico N° 191- 2023-JUS/DGAC, elaborado por la Dirección General de Asuntos Criminológicos, que indican que el proyecto normativo es viable y habiendo aportado observaciones, las mismas que han sido adoptadas en el proyecto.

VI. CALIDAD REGULATORIA DE LA NORMA

En virtud al numeral 10.1 del artículo 10 del Reglamento que desarrolla el Marco Institucional que rige el Proceso de Mejora de la Calidad Regulatoria y establece los Lineamientos Generales para la aplicación del Análisis de Impacto Regulatorio Ex Ante, aprobado por Decreto Supremo N° 063-2021-PCM, la presente norma se considera excluida del alcance del AIR Ex Ante, puesto que no establece, incorpora o modifica reglas, prohibiciones,

limitaciones, obligaciones, condiciones, requisitos, responsabilidades o cualquier exigencia que genere o implique variación de costos en su cumplimiento por parte de las empresas, ciudadanos o sociedad civil que limite el otorgamiento o reconocimiento de derechos para el óptimo desarrollo de actividades económicas y sociales que contribuyan al desarrollo integral, sostenible, y al bienestar social.

Asimismo, cabe precisar que, el 06 de noviembre, se presentó el anexo 7 "Formato de aplicación de excepción al AIR Ex Ante" ante la Comisión Multisectorial de Calidad Regulatoria (CMCR) y se recibió respuesta de la solicitud de exclusión de la presente propuesta el 13 de noviembre del presente, indicando que se declara la improcedencia del AIR Ex Ante del proyecto normativo, en virtud a la excepción establecida en el numeral 18 del inciso 28.1 del artículo 28 del Decreto Supremo N° 063-2021-PCM, por lo tanto no se requiere realizar el AIR Ex Ante por parte de la entidad.

PRESIDENCIA DEL CONSEJO DE MINISTROS
Secretaría de Gobierno y Transformación Digital

El Peruano Firmado por: Editora Peru Fecha: 13/12/2023 01:01

PODER EJECUTIVO

DECRETOS LEGISLATIVOS

DECRETO LEGISLATIVO Nº 1591

LA PRESIDENTA DE LA REPÚBLICA

POR CUANTO:

Que, el Congreso de la República, mediante Ley Nº 31880, ha delegado en el Poder Ejecutivo la facultad de legislar en materia de seguridad ciudadana, gestión del riesgo de desastres-niño global, infraestructura social, calidad de proyectos y meritocracia, por un plazo de noventa (90) días calendario;

Que, el literal f) del numeral 2.3 del artículo 2 de la Ley Nº 31880, dispone que el Poder Ejecutivo está facultado para legislar en el marco de la promoción del uso seguro y responsable de las tecnologías digitales por niños, niñas y adolescentes, de acuerdo con las siguientes consideraciones: 1) La modificación de la Ley 30096, Ley de delitos informáticos, se encuentra delimitada a la precisión de los delitos de grooming, fraude informático y suplantación de identidad; 2) Las modificaciones de la Ley 30096, Ley de delitos informáticos, y del Decreto Legislativo 957, Código Procesal Penal, en cuanto a la figura del agente encubierto, se limitan a la mención expresa de la posibilidad de su actuación en entornos digitales, así como al deber de coordinación con la Secretaría de Gobierno y Transformación Digital en la elaboración de protocolos referidos a dicha actuación; y, 3) La modificación del Decreto Legislativo 1267 se limita a incorporar el deber de coordinación con la Secretaría de Gobierno y Transformación Digital en la elaboración de protocolos referidos al empleo de sistemas tecnológicos y registros previstos en el artículo 43 de dicha norma;

Que, en los últimos años, la comisión de delitos informáticos y los delitos cometidos a través de las tecnologías digitales se ha incrementado significativamente en el Perú, aspecto que supone un especial riesgo para las niñas, niños y adolescentes, cuya interacción en el ámbito digital también va en aumento. Esta situación requiere de una respuesta integral y eficiente del Estado que, entre diversos aspectos, incluye el fortalecimiento de la persecución penal, a través de la tipificación de delitos, precisión de actos de investigación y articulación entre las instancias competentes en materia penal y en materia de gobierno y transformación digital; con el propósito de contribuir a brindar una mayor protección a las víctimas de tales delitos, especialmente si se trata de niñas, niños y adolescentes, así como para evitar la impunidad respecto a tales delitos;

Que, en virtud a la excepción establecida en el numeral 18) del inciso 28.1 del artículo 28 del Reglamento que desarrolla el Marco Institucional que rige el Proceso de Mejora de la Calidad Regulatoria y establece los Lineamientos Generales para la aplicación del Análisis de Impacto Regulatorio Ex Ante, aprobado mediante Decreto Supremo Nº 063-2021-PCM, no corresponde que se realice el Análisis de Impacto Regulatorio Ex Ante debido a que las disposiciones contenidas no establecen, incorporan o modifican reglas, prohibiciones, limitaciones, obligaciones, condiciones, requisitos, responsabilidades o exigencias que generen o impliquen variación de costos en su cumplimiento por parte de las empresas, ciudadanos o sociedad civil que limite el otorgamiento o reconocimiento de derechos; sino modificaciones a la Ley Nº 30096, Ley de Delitos Informáticos; asimismo, en la medida que el presente Decreto Legislativo no desarrolla procedimientos administrativos bajo el alcance del Análisis de Calidad Regulatoria (ACR), no se requiere realizar el ACR Ex Ante previo a su aprobación;

De conformidad con lo establecido por el artículo 104 de la Constitución Política del Perú, y en ejercicio de las facultades delegadas según lo dispuesto en literal f) del numeral 2.3 del artículo 2 de la Ley Nº 31880;

Con el voto aprobatorio del Consejo de Ministros; y,

Con cargo a dar cuenta al Congreso de la República;

Ha dado el Decreto Legislativo siguiente:

DECRETO LEGISLATIVO QUE MODIFICA LA LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS, PARA PROMOVER EL USO SEGURO Y RESPONSABLE DE LAS TECNOLOGÍAS DIGITALES POR NIÑAS, NIÑOS Y ADOLESCENTES.

Artículo 1.- Objeto

El presente decreto legislativo tiene por objeto modificar la Ley Nº 30096, Ley de Delitos Informáticos, para promover el uso seguro y responsable de las tecnologías digitales por niñas, niños y adolescentes.

Artículo 2.- Modificación de los artículos 5 y 9, así como de la Segunda y Tercera Disposiciones Complementarias Finales de la Ley Nº 30096, Ley de Delitos Informáticos

Se modifican los artículos 5 y 9, así como la Segunda y Tercera Disposiciones Complementarias Finales de la Ley Nº 30096, Ley de Delitos Informáticos, en los siguientes términos:

"Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad **no menor de seis ni mayor de nueve años**.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años.

En todos los casos se impone, además, la pena de inhabilitación conforme a los numerales 1, 2, 3, 4, 5, 6, 8, 9, 10 y 11 del artículo 36 del Código Penal."

"Artículo 9. Suplantación de identidad

El que, mediante las tecnologías **digitales** suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material, moral **o de cualquier otra índole**, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

La pena privativa de libertad es no menor de seis ni mayor de nueve años cuando se suplante la identidad de una persona menor de 18 años de edad y resulte algún perjuicio, material, moral o de cualquier otra índole."

"DISPOSICIONES COMPLEMENTARIAS FINALES

(...)

SEGUNDA.- Agente encubierto en delitos informáticos

El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, **incluso si estas acciones deben realizarse en entornos digitales,** y con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

Los protocolos para la actuación del agente encubierto en entornos digitales, tanto en el marco de la presente Ley, como en el marco del artículo 341 del Código Procesal Penal, aprobado mediante

el Decreto Legislativo 957, son coordinados, en cuanto corresponda, con la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en concordancia con las normas vigentes que regulan el Sistema Nacional de Transformación Digital."

"TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados

La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, la **Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros** y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad."

Artículo 3.- Financiamiento

La implementación de lo dispuesto en el presente Decreto Legislativo se financia con cargo a los presupuestos institucionales de los pliegos involucrados, sin demandar recursos adicionales al Tesoro Público.

Artículo 4.- Refrendo

El presente Decreto Legislativo es refrendado por el Presidente del Consejo de Ministros, el Ministro del Interior, el Ministro de Justicia y Derechos Humanos y la Ministra de la Mujer y Poblaciones Vulnerables.

DISPOSICIÓN COMPLEMENTARIA FINAL

Única. Las improcedencias a las que hacen referencia los artículos 161, 372 y 471 del Código Procesal Penal, aprobado con Decreto Legislativo N° 957 y los artículos 51 y 55 del Texto Único Ordenado del Código de Ejecución Penal, aprobado con Decreto Supremo N° 003-2021-JUS, respecto al artículo 183-B del Código Penal, aprobado por el Decreto Legislativo N° 635, son también aplicables a la comisión del delito establecido en el artículo 5 de la Ley N°30096, Ley de Delitos Informáticos.

POR TANTO:

Mando se publique y cumpla, dando cuenta al Congreso de la República.

Dado en la Casa de Gobierno, en Lima, a los doce días del mes de diciembre del año dos mil veintitrés.

DINA ERCILIA BOLUARTE ZEGARRA
Presidenta de la República

LUIS ALBERTO OTÁROLA PEÑARANDA
Presidente del Consejo de Ministros

VÍCTOR MANUEL TORRES FALCÓN
Ministro del Interior

EDUARDO MELCHOR ARANA YSA
Ministro de Justicia y Derechos Humanos

NANCY TOLENTINO GAMARRA
Ministra de la Mujer y Poblaciones Vulnerables

2243815-1

PRESIDENCIA DEL CONSEJO DE MINISTROS

Crean Grupo de Trabajo Multisectorial de naturaleza temporal con el objeto de formular la propuesta de la Política Nacional de Demarcación y Organización Territorial, dependiente de la PCM

RESOLUCIÓN MINISTERIAL
N° 296-2023-PCM

Lima, 12 de diciembre de 2023

CONSIDERANDO:

Que, el artículo 17 de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo, establece que la Presidencia del Consejo de Ministros es el Ministerio responsable de la coordinación de las políticas nacionales y sectoriales del Poder Ejecutivo. Coordina las relaciones con los demás Poderes del Estado, los organismos constitucionales, gobiernos regionales, gobiernos locales y la sociedad civil;

Que, el numeral 22.2 del artículo 22 de la Ley N° 29158 señala que los Ministerios diseñan, establecen, ejecutan y supervisan políticas nacionales y sectoriales, asumiendo la rectoría respecto de ellas;

Que, según lo dispuesto en el numeral 8.1 del artículo 8 del Reglamento que regula las Políticas Nacionales, aprobado por Decreto Supremo N° 029-2018-PCM, las Políticas Nacionales constituyen decisiones de política a través de las cuales se prioriza un conjunto de objetivos y acciones para resolver un determinado problema público de alcance nacional y sectorial o multisectorial en un periodo de tiempo;

Que, asimismo, el numeral 15.5 del artículo 15 del citado Reglamento señala que, excepcionalmente, el diseño, formulación, coordinación, seguimiento y evaluación de una política nacional multisectorial puede requerir la conformación de un grupo de trabajo u otro mecanismo que determine la política nacional multisectorial o acuerden los Ministerios intervinientes, según corresponda;

Que, el numeral 9 de la Guía de Políticas Nacionales, cuya actualización ha sido aprobada mediante Resolución de Presidencia de Consejo Directivo N° 0030-2023/CEPLAN/PCD, dispone que, en caso se decida la formulación de una política nacional luego del análisis de pertinencia, los ministerios deben formalizar el proceso de formulación de una política nacional a través de una Resolución Ministerial del ministerio rector, en el caso de una política sectorial, o del ministerio conductor, en el caso de una política multisectorial; precisa, además, que, excepcionalmente, se puede conformar un grupo de trabajo u otro mecanismo que asegure la participación de los ministerios intervinientes a través de sus unidades de organización competentes, así como de representantes de los otros Poderes del Estado, organismos autónomos, gobiernos regionales y locales y sociedad civil, según corresponda;

Que, mediante Resolución Ministerial N° 075-2020-PCM se formaliza el proceso para el desarrollo de las etapas y pasos de elaboración de la Política Nacional de Demarcación y Organización Territorial;

Que, el artículo 113 del Texto Integrado del Reglamento del Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Resolución Ministerial N° 224-2023-PCM, establece que la Secretaría de Demarcación y Organización Territorial es el órgano de línea con autoridad técnico normativa a nivel nacional, encargada de elaborar la política de demarcación territorial, conforme a la normativa vigente, a fin de lograr el saneamiento de límites y una mejor organización del territorio;

Que, el numeral 28.1 del artículo 28 de los Lineamientos de Organización del Estado, aprobados por el Decreto Supremo N° 054-2018-PCM, establece que los grupos de trabajo son un tipo de órgano colegiado sin personería jurídica ni administración propia, que se crean