«Decenio de la Igualdad de Oportunidades para Mujeres y Hombres»
«Año de la Universalización de la salud»

Informe Jurídico Nº 9-2020-JUS/DGTAIPD

A : **Úrsula Desilú León Chempén**
Viceministra de Justicia

Jorge Luis León Vasquez
Jefe de Gabinete de Asesores de la Alta Dirección

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

ASUNTO : Opinión sobre Proyecto de Ley Nº 5091/2020-CR

FECHA : Miraflores, 31 de julio de 2020

I. ANTECEDENTES

1. Mediante Proveído 001356-2020-VMJ del 27 de julio del presente, el despacho Viceministerial de Justicia remite para opinión a esta Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, DGTAIPD), el Proyecto de Ley Nº 5091/2020-CR, "Proyecto de Ley que modifica los artículos 2, 3 y 4 del Decreto Legislativo Nº 1182 que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado" (en adelante, "PL1182"), con la finalidad de que se emita opinión técnica en el marco de sus competencias.

II. MARCO NORMATIVO DE ACTUACIÓN

2. En virtud de lo establecido en los artículos 70 y 71 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos corresponde a la DGTAIPD ejercer la Autoridad Nacional de Transparencia y Acceso a la Información Pública (ANTAIP) y la Autoridad Nacional de Protección de Datos Personales (ANPD).

3. El inciso 11 del artículo 33 de la Ley Nº 29733, Ley de Protección de Datos Personales (en adelante, LPDP), establece que la ANPD tiene entre sus funciones emitir opiniones técnicas respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la cual es vinculante.

4. En esa medida, esta Dirección General emite el presente Informe Jurídico en el ámbito de la interpretación de las normas en materia de su competencia.

III. ANÁLISIS

Contenido del Proyecto de Ley

5. El Proyecto de Ley materia de análisis tiene por objeto modificar los artículos 2, 3 y 4 del Decreto Legislativo Nº 1182 que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.

6. El Decreto Legislativo Nº 1182 (en adelante, DL1182), tiene por finalidad brindar acceso a la unidad especializada de la Policía Nacional del Perú, en caso de flagrancia delictiva de los datos de localización y geolocalización de los teléfonos móviles o dispositivos electrónicos de naturaleza similar, por parte de las empresas concesionarias de las telecomunicaciones o entidades públicas relacionadas a estos servicios.

7. El Proyecto de Ley plantea la modificación de los artículos 2 y 3, a fin de ampliar el acceso de la Policía Nacional del Perú a datos de localización, geolocalización y *rastreo* de terminales móviles –y/o de cualquier otro dispositivo electrónico de comunicación– en supuestos de investigaciones preliminares por el delito contra la vida, el cuerpo y la salud, el delito contra la libertad, el delito contra el patrimonio y los delitos comprendidos en la Ley de crimen organizado.

8. El artículo 4 del Proyecto de Ley modifica el original a fin de precisar que el plazo que tienen las concesionarias para dar acceso a los datos se considera un plazo máximo, bajo apercibimiento de responsabilidades de carácter administrativo, civil y penal.

Si la información referida a la localización, geolocalización o rastreo son considerados datos personales

9. El numeral 4, del artículo 2 de la Ley Nº 29733, Ley de Protección de Datos Personales (en adelante, LPDP) establece que son datos personales «*toda información sobre una persona natural que la identifica o la hace identificable a través de medios que puedan ser razonablemente utilizados*». Asimismo, el numeral 4 del artículo 2 del Reglamento de la LPDP, complementa la definición de datos personales estableciendo que «*es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales o de cualquier otro tipo que conciernen a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados*».

10. En cuanto a la localización, geolocalización o rastreo de equipos móviles o de cualquier otro dispositivo electrónico de comunicación, son herramientas que permiten determinar la ubicación geográfica de un dispositivo en el espacio. Asimismo, la Exposición de Motivos del DL1182 establece que la localización y geolocalización puede lograrse a partir del sistema de posicionamiento global (GPS), que permite determinar la posición exacta del dispositivo con una precisión exacta; y el de la triangulación, que es un sistema que permite conocer las coordenadas de ubicación de un celular a partir de la transmisión de información a una torre del proveedor del servicio de telefonía móvil.

11. Entonces resulta relevante precisar si la información referida a la localización, geolocalización o rastreo de los equipos móviles o de comunicación se considera un dato personal; esta Dirección General, que tiene el encargo de ejercer la Autoridad Nacional de Protección de Datos Personales, es de la opinión que sí, siempre que la ubicación de un dispositivo singularice a una persona física permitiendo su identificación, es decir, estos datos, serán considerados datos personales si tales equipos son asociados a los titulares de las líneas, como sucede con el DL1182, cuyo objeto es identificar y geolocalizar o rastrear al dispositivo para la investigación y represión del delito.[1]

12. Cabe señalar que el término *rastreo* que se incluye en el Proyecto de Ley, es un término que habitualmente se emplea para la identificación de los lugares por donde ha transitado el dispositivo móvil; vale decir, en términos materiales, es similar la acción a la geolocalización de un dispositivo en el espacio y, por tanto, para efectos de la legislación de datos personales, es un dato personal en la medida que permita identificar a una persona natural específica.

Sobre el ámbito de aplicación de la Ley Nº 29733, Ley de Protección de Datos Personales y la eficacia de sus principios sustantivos

13. De acuerdo al artículo 3 de la Ley Nº 29733, Ley de Protección de Datos Personales, la misma es de aplicación a *"(…) los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional"*.

14. A la vez, el citado artículo precisa en su segundo párrafo que las disposiciones de esta Ley no son de aplicación a los siguientes datos personales: *"(…) 2. A los contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional,* ***seguridad pública****,* ***y para el desarrollo de actividades en materia penal para la investigación y represión del delito****"*. (el subrayado es nuestro).

15. El citado articulado pudiera llevar a la equivocada idea de que la Ley de Protección de Datos Personales, los derechos, deberes y obligaciones que reconoce y establece, no son de aplicación *in toto* cuando se trata de datos personales que se recolectan por la administración pública con fines de defensa nacional, seguridad pública o para la investigación y represión del delito. No es así. Pese al circunscrito ámbito de aplicación de la Ley Nº 29733, delimitado en su artículo 3, hay normas en ella que son manifestaciones de principios que tienen basamento constitucional, como es el caso del principio de

[1] Ya la ANPD ha emitido antes documentos donde fija su posición respecto a la condición de datos personales de los números de teléfonos celulares y los datos de localización y geolocalización. Son citables la Opinión Consultiva Nº 26-2019-JUS/DGTAIPD del 24 de abril de 2019 (Ver: https://www.minjus.gob.pe/wp-content/uploads/2019/07/OC-26.pdf) y la Opinión Técnica Nº 4-2020/JUS-DGTAPD, párrafo 11.

interdicción de la arbitrariedad en el ejercicio del poder público, así como el de razonabilidad y proporcionalidad (artículo 200 de la Constitución).[2]

16. En efecto, este sería el caso de las normas contenidas en los artículos 6, 7 o 9 de la Ley Nº 29733. Normas que recogen principios como el de finalidad[3], proporcionalidad[4] o seguridad[5] en el tratamiento de datos personales de ciudadanos, por citar unos ejemplos. Dado el basamento constitucional de estos, su fuerza normativa y eficacia irradia para todo tratamiento de datos personales, sea que este provenga de entidad pública o privada.

17. Así pues, para la ANPD, una agencia gubernamental dedicada a la defensa nacional o la seguridad pública, sólo puede exhibir finalidad legítima en el tratamiento de datos personales que realiza de los ciudadanos, si y sólo si, esa legitimidad comulga materialmente con los postulados constitucionales arriba reseñados. Siendo así, resulta necesario analizar si el PL1182 configura un esquema de tratamiento de datos personales deferente con el principio de razonabilidad y proporcionalidad a la luz de la finalidad trazada en dicho proyecto.

Sobre el estándar interamericano de derechos humanos para tratamientos de datos personales derivados de telecomunicaciones

18. Con la dación del DL1182, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la Organización de Estados Americanos, tuvo ocasión de exponer los estándares que debían tomar en cuenta los Estados que aprobaran leyes que obligasen a los proveedores de servicios de telecomunicaciones e Internet a retener datos (personales) de las comunicaciones electrónicas.[6]

---

[2] Es basta la jurisprudencia constitucional que se ha ocupado de dar contenido a la arbitrariedad como cuestión interdicta. Aquí citamos la recaída en el Expediente Nº 0090-2004-AA/TC (fundamento jurídico 12): *"El concepto de arbitrario apareja tres acepciones igualmente proscritas por el derecho: a) lo arbitrario entendido como decisión caprichosa, vaga e infundada desde la perspectiva jurídica; b) lo arbitrario entendido como aquella decisión despótica, tiránica y carente de toda fuente de legitimidad; y c) lo arbitrario entendido como contrario a los principios de razonabilidad y proporcionalidad jurídica. De allí que desde el principio del Estado de Derecho, surgiese el principio de interdicción de la arbitrariedad, el cual tiene un doble significado: a) En un sentido clásico y genérico, la arbitrariedad aparece como el reverso de la justicia y el derecho. b) En un sentido moderno y concreto, la arbitrariedad aparece como lo carente de fundamentación objetiva; como lo incongruente y contradictorio con la realidad que ha de servir de base a toda decisión. Es decir, como aquello desprendido o ajeno a toda razón de explicarlo. En consecuencia, lo arbitrario será todo aquello carente de vínculo natural con la realidad."*

[3] "Artículo 6. Principio de finalidad
Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización."

[4] "Artículo 7. Principio de proporcionalidad
Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados."

[5] "Artículo 9. Principio de seguridad
El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate."

[6] Lo hizo a través de una comunicación que dirigió a la Misión Permanente del Perú ante la OEA, el 28 de agosto de 2015. Puede consultarse el documento en el siguiente enlace: https://hiperderecho.org/wp-content/uploads/2015/09/carta_relator_cidh_ley_stalker.pdf, visionada el 31 de julio de 2020.

19. Dicho documento contiene fragmentos que resultan especialmente relevantes en este contexto de análisis del PL1182. En primer término, como toda intromisión a los derechos fundamentales, recuerda estándares de la organización –ampliamente desarrollados y compartidos en sede nacional a decir de la jurisprudencia constitucional peruana– que sirven de guía para dar por legítimas las limitaciones a estos; a saber:

> *"En su Informe sobre Libertad de Expresión e Internet[7], la Relatoría Especial indicó que la interceptación y retención de datos sobre las comunicaciones privadas comporta tanto una limitación directa al derecho a la intimidad como una afectación del derecho a la libertad de pensamiento y expresión.* ***Para que esta limitación pueda considerarse legítima****, debe cumplir con una serie de condiciones impuestas de conformidad con los artículos 11, 13, 8 y 25 de la Convención Americana. Esto es: (1) consagración legal; (2) búsqueda de una finalidad imperativa; (3)* ***necesidad, idoneidad y proporcionalidad de la medida para alcanzar la finalidad perseguida****; (4) garantías judiciales; y (5) satisfacción del debido proceso."*

20. Así también, reiterando lo señalado en documentos pasados[8], la Relatoría indica que serán incompatibles con la Convención Americana las restricciones sustantivas definidas en disposiciones administrativas *"(…)* ***o las regulaciones amplias o ambiguas que no generan certeza sobre el ámbito del derecho protegido y cuya interpretación puede dar lugar a decisiones arbitrarias*** *que comprometan de forma ilegítima los derechos a la intimidad y la libertad de expresión."*

21. Sobre ilegitimidad en la retención de datos personales[9], la Relatoría ha afirmado, reiterando anteriores posiciones[10], que:

> *"(…) la obligación de retener o las prácticas de retención de datos personales de forma indiscriminada con el fin de mantener el orden público o por motivos seguridad no son legítimos. En cambio, los datos personales deberían ser retenidos con fines de orden público o para temas de seguridad* ***solo de forma limitada y selectiva y en una forma que represente un equilibrio adecuado*** *entre los agentes del orden público y la seguridad y los derechos a la libertad de expresión y a la privacidad"*

22. Sobre el mismo punto, enfatiza:

---

[7] *Cfr.*: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf, visionado el 31 de julio de 2020.
[8] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013.
[9] En el propio documento, la Relatoría cita su Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión [Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la Organización de los Estados Americanos (OEA) y Relator Especial de las Naciones Unidas (ONU) para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión. 21 de junio de 2013], donde reconoció de manera particular que los metadatos de las comunicaciones digitales, que incluyen, entre otros, la ubicación, actividades en línea, y con quiénes se comunican los usuarios de Internet, pueden ser altamente reveladores, y su recolección y conservación equivalen a una limitación directa al derecho a la intimidad y vida privada de las personas.
[10] Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relator Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). 3 de mayo de 2015. Declaración conjunta sobre la libertad de expresión y las respuestas a las situaciones de conflicto.

> *"Dada la importancia del ejercicio de estos derechos para el sistema democrático, la ley debe autorizar el acceso a las comunicaciones y a datos personales* ***sólo en las circunstancias más excepcionales definidas en la legislación****. Cuando se invoquen causales más o menos abiertas como la seguridad nacional como razón para vigilar la correspondencia y los datos personales,* ***la ley debe especificar claramente los criterios que deben aplicarse para determinar los casos en los cuales este tipo de limitaciones resulta legítimo****".*

23. Además de la ley, la Relatoría Especial para la Libertad de Expresión encuentra en la figura del juez una garantía procesal indispensable para autorizar tareas de vigilancia sobre la privacidad de las personas; en buena cuenta, para que el tratamiento sobre esos datos personales se repute legítimo:

> *"(…) las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas* ***deben ser autorizadas por autoridades judiciales independientes****, que deben dar cuenta de las razones por las cuales la medida* ***es idónea*** *para alcanzar los fines que persigue en el caso concreto;* ***de si es lo suficientemente restringida*** *para no afectar el derecho involucrado más de lo necesario; y* ***de si resulta proporcional*** *respecto del interés que se quiere promover. Con este fin, la autoridad judicial debe estar capacitada en materias relacionadas y competente para tomar decisiones judiciales sobre la legalidad de la Vigilancia de las Comunicaciones, las tecnologías utilizadas y los derechos humanos."*

24. Finalmente, la Relatoría Especial, en su afán de remarcar la necesidad de establecer límites robustos a este tipo de prácticas de vigilancia, trae a colación el examen que practicó el Tribunal de Justicia Europeo en el fallo *Digital Rights Ireland Ltd* del 8 de abril de 2014, en el que declaró inválida la Directiva 2006/24 del Parlamento Europeo y del Consejo de la Unión sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas.[11] Este Alto Tribunal lo hizo bajo el convencimiento de que aquella directiva no reunía los siguientes límites o garantías:

> *"a)* ***Limitar la retención a datos relacionados con un período temporal o zona geográfica determinados*** *o a un círculo de personas concretas que puedan estar implicadas de una manera u otra en un delito grave, o a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la prevención, detección o enjuiciamiento de delitos graves.*
> *b) Establecer excepciones respecto de personas cuyas comunicaciones están sujetas al secreto profesional con arreglo a las normas de la legislación nacional.*
> *c) Establecer los periodos de retención en función a la posible utilidad de distintas categorías de datos para el objetivo perseguido o de las personas afectadas. En todo caso, la determinación del período de conservación debe basarse en criterios objetivos para garantizar que ésta se limite a lo estrictamente necesario.*
> *d)* ***Supeditar el acceso a los datos a un control judicial previo****, o a la revisión de autoridades administrativas independientes.*

[11] Tribunal Europeo de Justicia (Gran Sala). 8 de abril de 2014. *Digital Rights Ireland Ltd* e Irlanda. Comunicaciones Electrónicas –Directiva 2006/24/CE– Servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones – Conservación de datos generados o tratados en relación con la prestación de tales servicios –Validez– Artículos 7, 8 y 11 de la Carta de los Derechos Fundamentales de la Unión Europea.

> *e)* ***Establecer criterios objetivos que permitan delimitar el acceso de las autoridades nacionales competentes*** *a los datos y su utilización posterior con fines de prevención, detección o enjuiciamiento de delito.* ***Por ejemplo, precisar las condiciones materiales*** *y de procedimiento correspondientes.*
> *f) Definir expresamente que el acceso y la utilización posterior de los datos de que se trata deberán limitarse estrictamente a fines de prevención y detección de delitos graves delimitados de forma precisa o al enjuiciamiento de tales delitos.*
> ***g) Limitar el número de personas que disponen de la autorización de acceso*** *y utilización posterior de los datos conservados a lo estrictamente necesario teniendo en cuenta el objetivo perseguido.*
> *h) Garantizar que los proveedores de servicios de comunicaciones electrónicas apliquen un nivel especialmente elevado de protección y seguridad de los datos conservados a través de medidas técnicas y organizativas.*
> *i)* ***Garantizar la destrucción definitiva de los datos*** *al término de su período de conservación.*
> *j) Asegurar que los datos conservados se mantengan en el territorio de la Unión Europea."*

25. En base a estas consideraciones, la Corte Europea entendió que la examinada directiva sobrepasó los límites que exige el *principio de proporcionalidad*. Esta Dirección General, que por encargo ejerce la Autoridad Nacional de Protección de Datos Personales, comparte estas mismas consideraciones *in abstracto* como criterio material para evaluar todo tipo de medidas de similar naturaleza que pretendan incidir o afectar el derecho a la protección de los datos personales de los individuos.

¿Es legítimo el tratamiento de datos personales que haría la Policía Nacional, a propósito del PL1182, en su afán de luchar contra la delincuencia y el crimen organizado?

26. El DL1182 establece que el objeto de la norma es fortalecer las acciones de prevención, investigación y combate de la delincuencia común y el crimen organizado a través de las TIC's, por parte de la Policía Nacional del Perú. Y es que, a la luz de la Exposición de Motivos, tras 5 años del DL1182, *"el balance de su efectividad refleja algunos vacíos legales que impiden la efectividad y la acción rápida de los operadores de justicia que exigen al legislador proponer las mejoras en el ordenamiento jurídico, para la efectiva actuación judicial y operativa de la Policía Nacional."*

27. Se aduce también –siempre en la Exposición de Motivos– que esta iniciativa nace de la reflexión sobre el comportamiento delictivo de los últimos tiempos y de diversos estudios que han demostrado que los establecimientos penitenciarios se han convertido en lugares de adoctrinamiento de delincuentes, que se valen de argucias para introducir en ellos aparatos de comunicación, agudizando así la inseguridad ciudadana.

28. Es así como el PL1182 –artículo 2– plantea ampliar el objetivo e incluir las *investigaciones preliminares* por el delito contra la vida, el cuerpo y la salud; el delito contra la libertad; delito contra el patrimonio; y, los delitos comprendidos en la Ley Nº 30077, Ley contra el Crimen Organizado. Además, el citado proyecto y artículo, plantea no sólo acceder a datos de localización y geolocalización, sino también hacer *rastreo* del dispositivo *y/o de cualquier otro dispositivo electrónico de comunicación*.

29. Así pues, con la modificación planteada se añaden algunos supuestos adicionales al original artículo 3 del DL1182, para la procedencia del acceso a estos datos a instancia de la unidad especializada de la Policía Nacional:

    a. Cuando se trate de flagrante delito, de conformidad con lo dispuesto en el artículo 259 del Decreto Legislativo Nº 957, Código Procesal Penal **o investigaciones preliminares por el delito contra la vida, el cuerpo y la salud; el delito contra la libertad, el delito contra el patrimonio y los delitos comprendidos en la Ley de Crimen Organizado.**
    b. Cuando el delito investigado sea sancionado con pena superior a los cuatro años de privación de libertad.
    c. El acceso a los datos constituya un medio necesario para la investigación.

30. A juicio de esta Dirección General que ejerce la Autoridad Nacional de Protección de Datos Personales, el tratamiento de datos personales que derivaría de esta modificación planteada al DL1182 no resultaría legítimo a la luz de la Ley Nº 29733, dada su amplitud y desproporción en la intensidad de su afectación al derecho a la protección de datos personales.

31. En efecto, como se ha señalado *supra*, regulaciones amplias o ambiguas pueden dar lugar a decisiones arbitrarias. El esquema propuesto no garantiza selectividad y limitación de los vigilados a lo estrictamente necesario. Ampliar el abanico delictivo, más allá del supuesto de flagrancia por delitos cuya pena sea superior a los cuatro años de privación de la libertad, le confiere a la Policía Nacional potestades mayores para la investigación que el propio Ministerio Público.[12]

32. ¿Cómo se genera convicción la Policía Nacional acerca de la comisión de un delito grave en la fase de una investigación preliminar, tomando en cuenta que en ella sólo pueden realizarse actos urgentes o inaplazables destinados a determinar si han tenido lugar los hechos objeto de conocimiento y su delictuosidad, así como asegurar los elementos materiales de su comisión e individualizar a las personas involucradas[13]? Está claro que

[12] Como sabemos, a decir del artículo 230 del Nuevo Código Procesal Penal, el Fiscal requiere la autorización del juez para intervenir, grabar o registrar comunicaciones telefónicas u otras formas de comunicación y geolocalización de teléfonos móviles:
"Artículo 230. - Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles
1. El Fiscal, cuando existan suficientes elementos de convicción para considerar la comisión de un delito sancionado con pena superior a los cuatro años de privación de libertad y la intervención sea absolutamente necesaria para proseguir las investigaciones, podrá solicitar al Juez de la Investigación Preparatoria la intervención y grabación de comunicaciones telefónicas, radiales o de otras formas de comunicación. Rige lo dispuesto en el numeral 4) del artículo 226.
(…)".

[13] Nuevo Código Procesal Penal, aprobado mediante Decreto Legislativo Nº 957.
"Artículo 330 Diligencias Preliminares.-
1. El Fiscal puede, bajo su dirección, requerir la intervención de la Policía o realizar por sí mismo diligencias preliminares de investigación para determinar si debe formalizar la Investigación Preparatoria.
2. Las Diligencias Preliminares tienen por finalidad inmediata realizar los actos urgentes o inaplazables destinados a determinar si han tenido lugar los hechos objeto de conocimiento y su delictuosidad, así como asegurar los elementos materiales de su comisión, individualizar a las personas involucradas en su comisión, incluyendo a los agraviados, y, dentro de los límites de la Ley, asegurarlas debidamente.

no puede ser la mera sospecha policial la que guíe una decisión de vigilancia y recolección de estos datos personales[14], así que, a falta de un conocido[15] *Protocolo de Acceso a los datos de Localización o Geolocalización de Teléfonos Móviles o Dispositivos Electrónicos de Similar Naturaleza*, sólo queda asumir que dicha decisión se sustenta al menos en la sindicación por parte de una persona, una denuncia ciudadana, o las conclusiones a las que arribe el cuerpo policial –luego de haber transcurrido 24 horas del hecho punible– tras el análisis de las circunstancias del mismo y los elementos objetivos que permiten la identificación del presunto perpetrador.[16] Asumiendo que ello sea así, ¿alguna de estas situaciones sería capaz de justificar por sí sola la decisión policial de acceder a los datos personales de ciudadanos cuya inocencia se presume en mérito de la Constitución y la ley penal? Nosotros creemos que no.

33. Puede aceptarse preliminarmente[17] la idea de que el acceso a los datos personales de localización y geolocalización esté legitimado –y el tratamiento de datos que él conlleva– en el supuesto de flagrancia delictiva (DL1182). Si se acepta, es porque, dada la inmediatez personal y temporal que exige la flagrancia delictiva[18], es decir, la "estrecha

---

3. El Fiscal al tener conocimiento de un delito de ejercicio público de la acción penal, podrá constituirse inmediatamente en el lugar de los hechos con el personal y medios especializados necesarios y efectuar un examen con la finalidad de establecer la realidad de los hechos y, en su caso, impedir que el delito produzca consecuencia ulteriores y que se altere la escena del delito."

[14] Véase la sentencia del Tribunal Constitucional recaída sobre el Expediente Nº 1324-2000-HC/TC: *"2. Que, por consiguiente y partiendo de la merituación de las pruebas obrantes en el expediente constitucional así como de las diligencias realizadas en el presente proceso, resultan plenamente acreditadas las aseveraciones efectuadas por la accionante de la presente causa respecto de los ciudadanos afectados en sus derechos, habida cuenta que (…) f) Que por tal motivo y reiterando los precedentes sentados con anterioridad, y a los cuales deben observancia obligatoria todos los jueces y tribunales de la República, conforme lo señala la Primera Disposición General de la Ley N.° 26435 –Ley Orgánica del Tribunal Constitucional,* ***este Tribunal ratifica que las variables de causalidad a los efectos de ejercer la potestad de detención, esto es, mandato judicial y flagrante delito, constituyen la regla general aplicable a todos los casos de detención, sea cual sea la naturaleza del ilícito cometido, de modo tal que las llamadas detenciones preventivas o detenciones sustentadas en la mera sospecha policial, carecen de toda validez o legitimidad constitucional*** *(…)"* (El énfasis es nuestro).

[15] Escribimos "conocido" no porque no conozcamos de su existencia –como se sabe este fue aprobado por la Resolución Ministerial Nº 0631-2015-IN–, sino porque es una interrogante su contenido. Prueba de ello es la calificación de "Reservado" que tiene el documento, según alega el propio Sector Interior, de acuerdo a lo reseñado por la Tercera Sala Civil de la Corte Superior de Justicia de Lima en su sentencia (Resolución Nº 4 del 18 de mayo de 2018) recaída sobre el Expediente Nº 003811-2017-0-1801-JR-CI-05, Proceso de Hábeas Data, que se resolvió a favor de la demandante al revocarse la resolución que venía en grado y ordenarse la entrega del referido protocolo. Pues bien, en el considerando Tercero de la citada resolución, la Sala reseña los argumentos de la Procuradora del Ministerio del Interior, quien alega: *"Los documentos solicitados por el demandante son especializados que* ***no tienen acceso público****, ya que derivan de investigaciones efectuadas* ***con carácter reservado*** *por parte de la Policía Nacional del Perú (…)"*. El énfasis es nuestro.

[16] "Artículo 259.- Detención Policial
La Policía Nacional del Perú detiene, sin mandato judicial, a quien sorprenda en flagrante delito. Existe flagrancia cuando:
1. El agente es descubierto en la realización del hecho punible.
2. El agente acaba de cometer el hecho punible y es descubierto.
3. El agente ha huido y ha sido identificado durante o inmediatamente después de la perpetración del hecho punible, sea por el agraviado o por otra persona que haya presenciado el hecho, o por medio audiovisual, dispositivos o equipos con cuya tecnología se haya registrado su imagen, y es encontrado dentro de las veinticuatro (24) horas de producido el hecho punible.
4. El agente es encontrado dentro de las veinticuatro (24) horas después de la perpetración del delito con efectos o instrumentos procedentes de aquel o que hubieren sido empleados para cometerlo o con señales en sí mismo o en su vestido que indiquen su probable autoría o participación en el hecho delictuoso."

[17] Para efectos de este ejercicio discursivo, no porque la ANPD avale en términos legales el DL1182.

[18] Véase la Sentencia del Tribunal Constitucional recaída sobre el Expediente N° 6142-2006-PHC/TC: *"4. Según lo ha establecido este Tribunal en reiterada jurisprudencia,* ***la flagrancia en la comisión de un delito requiere el cumplimiento***

ventana de oportunidad" para apreciar los elementos convincentes alrededor del hecho punible, hacen presumir que estos son de tal rotundidad como para justificar una detención policial, y con ella una afectación a la libertad personal, que pudieran también ser suficientes para admitir una afectación a los datos personales derivados de las telecomunicaciones. Pero esa legitimidad se difumina cuando no se conocen los criterios objetivos o condiciones materiales que emplearía la Policía Nacional para decidir, por sí y ante sí, el acceso a dichos datos. Eso es lo que apreciamos en el PL1182.

34. Por lo tanto, a juicio de esta Dirección General, no se aprecia legitimidad para el tratamiento de datos personales que haría la Policía Nacional en el marco del PL1182. Esta opinión se sustenta no solo por lo analizado *supra*, sino también por la ausencia de otras garantías indispensables reseñadas en el párrafo 24: no intervención previa de juez (sólo convalida según detalla el artículo 5 del DL1182); no garantía de eliminación de la información, una vez culminada la finalidad; no determinación de un marco temporal para el acceso a esos datos derivados de las telecomunicaciones; y, no determinación de los sujetos que disponen de la autorización de acceso, ya que la propuesta normativa –artículo 3– sólo alude genéricamente a la unidad de investigación policial que lo requiera.

IV. CONCLUSIÓN

El Proyecto de Ley Nº 5091/2020-CR, que modifica los artículos 2, 3 y 4 del Decreto Legislativo Nº 1182 que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado, puesto a examen, no supera en su versión actual el examen de legalidad efectuado por esta Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en el marco de la Ley Nº 29733, Ley de Protección de Datos Personales.

PERÚ Ministerio de Justicia y Derechos Humanos
DIRECCIÓN GENERAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES
E. LUNA C.

Firmado digitalmente por LUNA CERVANTES Eduardo Javier FAU 20131371617 soft
Fecha: 2020.08.03 19:26:16 -05'00'

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

de cualquiera de los dos requisitos siguientes: a) la inmediatez temporal, es decir, que el delito se esté cometiendo o se haya cometido momentos antes; y, b) la inmediatez personal, es decir, que el presunto delincuente se encuentre en el lugar de los hechos, en el momento de la comisión del delito, y esté relacionado con el objeto o los instrumentos del delito. *(…)"* (El énfasis es nuestro).