Informe escrito
de la "Open Society Justice Initiative"

sobre la adecuación del
Decreto Legislativo Nº 1129 del Perú con el Derecho internacional

I. INTRODUCCIÓN

1. El secretismo excesivo fundado en razones de seguridad nacional es irreconciliable con el control democrático. Además, si bien la seguridad nacional puede justificar restricciones legítimas al derecho del público a acceder a la información cuando se cumplen ciertas condiciones, el interés en el conocimiento público de las actividades del Estado, incluyendo las de sus fuerzas de seguridad es, a menudo, protector de los legítimos intereses de seguridad nacional de los ciudadanos. El acceso a la información pública promueve la responsabilidad para evitar las violaciones de los derechos humanos, la corrupción, el despilfarro y los abusos.

2. El escrutinio público supone una salvaguardia frente a los abusos por parte de funcionarios públicos y garantiza la participación democrática y la supervisión de las políticas empleadas en un campo donde existen muchos poderes discrecionales por parte del ejecutivo y, a veces, una excesiva deferencia. La invocación excesiva de motivos de seguridad nacional por parte del gobierno, o la excesiva deferencia a estas afirmaciones de seguridad nacional, pueden socavar gravemente las principales garantías institucionales frente a los abusos del gobierno: la independencia del poder judicial, el estado de Derecho, el control legislativo, la libertad de prensa y la transparencia administrativa.

3. En 2002, el Perú promulgó la Ley de Transparencia y Acceso a la Información Pública (la Ley "TAIP") en un momento de transición gubernamental, luego de que se descubrieron abusos de poder por parte de políticos, militares y funcionarios de inteligencia de la más alta jerarquía bajo un velo de secretismo y a raíz del compromiso público de la nueva administración de luchar contra la corrupción.[1] La Ley TAIP incluye, como todas o casi todas las leyes similares promulgadas en todo el mundo, una exención de la ley que permite retener legítimamente información por motivos de seguridad nacional.[2] La Ley TAIP también incluye, dentro de la misma disposición en la que se recoge la exención por motivos de seguridad nacional, la prohibición de la clasificación de la información "relacionada a la violación de derechos humanos o de las Convenciones de Ginebra de 1949 realizada en cualquier circunstancia, por cualquier persona".[3] La estricta exención por motivos de seguridad nacional en el Perú está muy influenciada por razones históricas relacionadas con la excesiva invocación de la seguridad nacional para justificar el carácter secreto de la información sobre las violaciones de los derechos humanos.

---

[1] *Véase* Javier Casas, *A Legal Framework for Access to Information in Peru* ("Un marco legal para el acceso a la información en el Perú"), en Article 19, Time for Change: Promoting and Protecting Access to Information and Reproductive and Sexual Health Rights in Peru, 2006, disponible en http://www.article19.org/data/files/pdfs/publications/peru-time-for-change.pdf.
[2] Ley de Transparencia y Acceso a la Información Pública (2002), artículo 15.
[3] *Idem.*

4. En diciembre de 2012, el Presidente promulgó el Decreto Legislativo Nº 1129 que incluye una amplia disposición relativa al secretismo en las áreas de seguridad y defensa nacional. El artículo 12 del Decreto Legislativo 1129 establece lo siguiente: "en general, toda información o documentación que se genere en el ámbito de los asuntos referidos a la Seguridad y Defensa Nacional, y aquellas que contienen las deliberaciones sostenidas en las sesiones del Consejo de Seguridad y Defensa Nacional, son de carácter secreto". El Decreto Nº 1129 se encuentra actualmente bajo revisión por el Tribunal Constitucional del Perú.

5. A la luz de la demanda de inconstitucionalidad presentada contra el artículo 12 del Decreto Nº 1129, la Defensoría del Pueblo solicitó a la Open Society Justice Initiative un análisis de la compatibilidad de esta disposición con el Derecho internacional y el Derecho comparado. Open Society Justice Initiative utiliza el Derecho para proteger y reconocer poderes o facultades a las personas en todo el mundo. Mediante su participación en litigios, la defensa de los derechos, la investigación y la ayuda técnica, la Justice Initiative fomenta los derechos humanos y construye capacidad jurídica para sociedades abiertas. En el campo de la libertad de expresión y el acceso a la información, la Justice Initiative ha brindado asistencia jurídica gratuita o ha presentado escritos en calidad de *amicus curiae* en los tres sistemas regionales de derechos humanos y en el Comité de Derechos Humanos de las Naciones Unidas. Entre otros, la Justice Initiative presentó escritos en calidad de *amicus curiae* ante la Corte Interamericana de Derechos Humanos y la Comisión Interamericana de Derechos Humanos (la "Comisión Interamericana") en el emblemático caso *Claude Reyes y otros v. Chile*, y ante la Corte Interamericana en el caso *Gomes Lund y otros (la "Guerrilha do Araguaia") v. Brasil* y el caso *Gudiel Álvares y otros ("Diario Militar") v. Guatemala*.

6. La Justice Initiative, junto con otras 21 organizaciones y centros académicos, elaboró un conjunto de Principios Globales para la Seguridad Nacional y el Derecho a la Información (los llamados "Principios de Tshwane", que toman su nombre del municipio donde se celebró la reunión para ultimar su redacción). Los Principios de Tshwane, promulgados el 12 de junio de 2013, se basan en leyes, normas, buenas prácticas nacionales e internacionales, así como en los escritos de expertos. Han sido avalados por los Relatores Especiales de la ONU para la protección y la promoción de los derechos humanos en la lucha contra el terrorismo, y para la libertad de expresión; y por los tres relatores especiales regionales para la libertad de expresión y medios de comunicación de la Organización de los Estados Americanos (OEA), la Organización para la Seguridad y la Cooperación en Europa (OSCE), y la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP); así como por la Asamblea Parlamentaria del Consejo de Europa (APCE).[4] Los Principios de Tshwane se adjuntan al presente informe como Anexo A y se detallan a continuación.

7. En el presente informe se procederá a analizar, en primer lugar, las normas que rigen el derecho al acceso a la información pública según el Derecho internacional, incluyendo un análisis de las restricciones legítimas al mismo por razones de seguridad nacional. A continuación, se analizará la compatibilidad del Decreto Nº 1129 con la normativa internacional en la materia. De dicho análisis se desprende que el alcance del secretismo en relación a información relacionada con la seguridad y la defensa nacional que establece el Decreto Nº 1129 es incompatible con las obligaciones del Perú

[4] Principios Globales sobre Seguridad Nacional y el Derecho a la Información (los "Principios de Tshwane"), 2013, disponibles en http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principle, que figuran adjuntos como Anexo. Aprobados por la APCE y los Relatores Especiales: Recomendación APCE 2024 (2013), numeral 1.3, aprobada el 2 de octubre de 2013. Resolución APCE 1954 (2013), adoptada el 2 de octubre de 2013, numerales 7-9. Open Society Justice Initiative, comunicado de prensa: *New Principles Address the Balance between National Security and the Public's Right to Know* ("Los nuevos principios abordan el equilibrio entre la seguridad nacional y el derecho del público a saber"), 12 de junio de 2013, disponible en http://www.opensocietyfoundations.org/press-releases/new-principles-address-balance-between-national-security-and-publics-right-know. La Open Society Justice Initiative fue una de las entidades que participaron en la elaboración de los Principios de Tshwane.

en materia de Derecho internacional. Dicha limitación al derecho de acceso a la información (1) no es necesaria ni proporcionada, (2) vulnera el principio de máxima divulgación, (3) permitiría el mantenimiento del secretismo a perpetuidad, y (4) exime a la retención de la información en estas categorías de un control independiente. El artículo 12 del Decreto Nº 1129 es absolutamente incompatible con el marco jurídico peruano pues éste solo permite excepciones limitadas (y no absolutas) frente a la obligación del Estado de divulgar información; requiere que cada restricción esté debidamente justificada; y requiere la revelación de información en asuntos de violaciones de los derechos humanos y crímenes de Derecho internacional.

II. LAS NORMAS JURÍDICAS MÁS RELEVANTES: EL DERECHO DE ACCESO A LA INFORMACIÓN EN EL DERECHO INTERNACIONAL

8. (A) El derecho de acceso a la información está bien establecido en el derecho internacional, incluyendo los tratados internacionales vinculantes para el Perú. (B) Existe un amplio consenso respecto al contenido de ese derecho, el cual incluye el principio fundamental de divulgación máxima, es decir, el requisito de que todas las restricciones a ese derecho estén limitadas, y consecuentemente sean necesarias y proporcionales, así como el derecho a la revisión independiente y eficaz de todas las limitaciones del derecho al acceso a la información. (C) Estos principios deben aplicarse a cualquier restricción al derecho de acceso a la información, incluida la restricción basada en aras de la seguridad nacional.

A. El Acceso a la Información como un Derecho Plenamente Establecido en el Derecho Internacional

9. El derecho de acceso a la información ha sido ampliamente aceptado en el mundo democrático como un derecho político fundamental. Ya sea como parte de las garantías tradicionales de la libertad de expresión o como un derecho importante por sí mismo se percibe como un componente integral e imperativo del derecho más amplio de la gobernabilidad democrática, así como un requisito para otros derechos fundamentales. De hecho, actualmente es insostenible afirmar que el público *no* tiene un derecho general a conocer lo que su estado sabe y hace, sujeto únicamente a determinadas excepciones imperiosas.

10. El derecho de acceso a la información, incluida la información en posesión del estado, está bien establecido en el derecho internacional sobre derechos humanos, y ampliamente reconocido en los Estados democráticos. El derecho a buscar y recibir informaciones está protegido expresamente en el artículo 13 de la Convención Americana y en el artículo 19 del PIDCP. En 2011, el Comité de Derechos Humanos de las Naciones Unidas, al que se le había encomendado interpretar de modo definitivo las obligaciones impuestas a los Estados por el PIDCP, adoptó una Observación General en la que establecía que el artículo 19 del Pacto garantiza el derecho de acceso a la información en posesión del estado.[5] Así mismo, los Relatores Especiales sobre la libertad de expresión de las Naciones Unidas (ONU), la Organización de los Estados Americanos (OEA), la Organización para la Seguridad y la Cooperación en Europa (OSCE) y la Comisión Africana sobre Derechos Humanos y de los Pueblos (ACHPR) han afirmado, en repetidas ocasiones, que la libertad de expresión incluye el derecho a conocer la información en posesión del estado.[6]

---

[5] Comité de Derechos Humanos de Naciones Unidas, *Observación general Nº 34 sobre el artículo 19*, Doc. CCPR/C/GC/34, 12 de septiembre de 2011.

[6] Declaración Conjunta del Relator Especial de las Naciones Unidas para la Libertad de Opinión y Expresión, el Representante de la OSCE para la Libertad de los Medios de Comunicación y el Relator Especial de la OEA para la Libertad de Expresión, de 6 de diciembre de 2004 (en adelante, la "Declaración Conjunta de los Relatores Especiales de 2004"). Declaración Conjunta del Relator Especial de las Naciones Unidas para la Libertad de Opinión y Expresión, el Representante de la OSCE para la Libertad de los Medios de Comunicación, el Relator Especial de la OEA para la Libertad de Expresión y el Relator Especial de la ACHPR para la Libertad de Expresión, de 20 de diciembre de 2006.

11. De los tres sistemas regionales de derechos humanos el Sistema Interamericano es el más desarrollado en el reconocimiento del derecho de acceso a la información y las correspondientes obligaciones de los Estados. En la histórica sentencia de 2006 proferida respecto al caso *Claude Reyes v. Chile*, la Corte Interamericana volvió a afirmar que el artículo 13 de la Convención Americana "ampara el derecho de las personas a recibir dicha información y la obligación positiva del Estado de suministrarla."[7] La naturaleza fundamental del derecho de acceso a la información también ha sido reconocida por la Comisión Interamericana[8] y por los Estados de la región, mediante su aprobación de declaraciones pertinentes, incluida la Declaración de Chapultepec [9] y la Declaración Interamericana de Principios sobre Libertad de Expresión.[10]

12. Del mismo modo, las instituciones regionales europeas y africanas también han reconocido que el derecho a la libertad de expresión incluye un derecho autónomo de acceso a la información. En decisiones recientes, el Tribunal Europeo de Derechos Humanos ha reconocido que el artículo 10 del Convenio Europeo, que protege la libertad de expresión, da lugar a un derecho independiente a recibir la información en poder de las autoridades públicas y que es relevante para el debate público, con independencia del interés personal, que el solicitante tenga respecto a esa información, aparte del interés de contribuir al debate público.[11] El Consejo de Europa también ha adoptado un Convenio sobre el Acceso a los Documentos Públicos, el primer tratado de este tipo, que garantiza un derecho de acceso vinculante, [12] y la Carta de Derechos Fundamentales de la Unión Europea concede un derecho de acceso a los documentos de las instituciones de la Unión.[13] La Comisión Africana sobre Derechos Humanos y de los Pueblos, por su parte, ha sostenido que el artículo 9 de la Carta Africana sobre los Derechos Humanos y de los Pueblos[14] protege no solo el derecho de todo individuo a expresar y difundir su opinión, sino también los derechos de las persona interesadas en recibir información e ideas de las fuentes legalmente disponibles.[15]

---

[7] *Claude Reyes v. Chile*, Corte IDH, sentencia del 9 de septiembre de 2006, Serie C, nº 151, numeral 77. *Véase también La Colegiación Obligatoria de Periodistas para el Ejercicio del Periodismo,* Corte IDH, Opinión Consultiva OC-5/85, de 13 de noviembre de 1985, Serie A nº 5, numeral 32 ("Para el ciudadano común tiene tanta importancia el conocimiento de la opinión ajena o de la información de que disponen otros como el derecho a difundir la propia").

[8] *Declaración de Principios de la Comisión Interamericana sobre la Libertad de Expresión*, aprobados en la sesión ordinaria 108 de la CIDH el 19 de octubre de 2000, numeral 4.

[9] *Declaración de Chapultepec*, adoptada por La Conferencia Hemisférica sobre Libertad de Expresión celebrada en México, D.F., el 11 de marzo de 1994, Preámbulo y Principio 2.

[10] *Declaración de Principios de la Comisión Interamericana sobre la Libertad de Expresión,* nota 8 anterior, Preámbulo.

[11] *Gillberg v. Suecia*. TEDH, sentencia de la Gran Sala de 3 de abril de 2012. Exp. nº 41723/06, numeral 82. *Véanse también los asuntos Társaság a Szabadságjogokért v. Hungría*, TEDH, sentencia de 14 de abril de 2009, numerales 36-38; *Kenedi v. Hungría*, TEDH, sentencia de 26 de mayo de 2009, numerales 43 y 45. El artículo 10 del Convenio Europeo de Derechos Humanos establece que "[t]oda persona tiene derecho a la libertad de expresión," lo que comprende la libertad de "recibir [...] informaciones o ideas sin que pueda haber injerencia de autoridades públicas." La Jurisprudencia del Tribunal Europeo ha reconocido desde hace tiempo un derecho condicional de acceso a la información pública en posesión del Estado, en circunstancias en que la denegación de esa información afecte al disfrute de otros derechos del Convenio. *Véase, por ejemplo, el asunto Guerra y otros v. Italia*, TEDH, sentencia de 19 de febrero de 1998.

[12] Consejo de Europa. Serie de Tratados Europeos nº 205, adoptado por el Consejo de Europa el 27 de noviembre de 2008, ratificado por seis Estados y firmado por otros ocho (requiere diez ratificaciones para su entrada en vigor). *Véase también la Recomendación No. (81) 19 sobre el acceso a la información en poder de las autoridades públicas,* aprobada por el Consejo de Ministros el 25 de noviembre de 1981, y la *Recomendación No. (2000)2 sobre el acceso a los documentos oficiales,* aprobada por el Consejo de Ministros el 21 de febrero de 2002.

[13] Art. 42. La Carta fue solemnemente proclamada el 7 de diciembre de 2000 y se hizo vinculante a raíz de la adopción del Tratado de Lisboa.

[14] El artículo 9 de la Carta Africana establece: "1. Todo individuo tendrá derecho a recibir información. 2. Todo individuo tendrá derecho a expresar y difundir sus opiniones, siempre que respete la ley."

[15] *Véanse, entre otros, los asuntos Sir Dawda K. Jawara v. Gambia*. ACHPR, Decisión de 11 de mayo de 2000, numeral 65. ACHPR, *Declaración de Principios sobre la Libertad de Expresión en África*, adoptada en la 32ª Sesión Ordinaria, 17-23 de octubre de 2002 (Banjul), Principio IV, donde se reconoce que "los organismos públicos guardan información no para sí mismos, sino como custodios del bien público."

13. El reconocimiento del derecho fundamental de acceso a la información se ve cada vez más reflejado en las constituciones,[16] en las leyes estatutarias, en la práctica de los Estados y en la jurisprudencia nacional.[17] Más de noventa países y grandes territorios de todo el mundo, incluidos al menos veinte en América, han aprobado leyes de acceso a la información que regulan el acceso a la información que obra en poder del Estado.[18] Desde mayo de 2012, cuando la ley promulgada por Brasil entró en vigor, más de 5.500 millones de personas de todo el mundo viven en países cuya regulación nacional prevé un derecho exigible a obtener información de sus estados.

14. El derecho de acceso a la información es fundamental por sí mismo, pero también ha sido reconocido como condición previa para el ejercicio de los derechos básicos de participación y representación política, así como el derecho a la verdad. La Corte Interamericana ha establecido que "el acceso a la información bajo el control del Estado puede permitir la participación en la gestión pública, a través del control social que se puede ejercer con dicho acceso."[19] De igual manera, el derecho a la verdad sólo puede satisfacerse si se adoptan mecanismos adecuados para el acceso a la información pertinente. Un estudio realizado en 2006 por el Alto Comisionado de las Naciones Unidas para los Derechos Humanos concluía, después de hacer un exhaustivo análisis de la legislación y prácticas internacionales, que la legislación sobre el acceso a la información constituye un importante paso para garantizar el derecho a la verdad, y que "[e]l acceso a la información y, en particular, a los archivos oficiales, es fundamental para el ejercicio del derecho a la verdad."[20]

B. Contenido del Derecho de Acceso a la Información

15. Cada vez hay más claridad sobre el contenido del derecho de acceso a la información, en particular, aunque no únicamente en el continente americano. Este aparte contiene una descripción general de los principales componentes del derecho que son relevantes para valorar el cumplimiento del Decreto Legislativo Nº 1129 del Perú con el Derecho Internacional, basándose en gran parte en las autoridad vinculante y persuasiva de las Américas, e incorporando la jurisprudencia internacional y comparada de otras regiones como guía.

16. La jurisprudencia de la Corte Interamericana, así como las decisiones de la Comisión Interamericana y las declaraciones e informes de la Relatoría Especial de la OEA para la Libertad de Expresión, manifiestan un consenso regional respecto al contenido del derecho de acceso a la información.[21] En 2010, la Relatoría Especial elaboró un manual sobre el derecho de acceso a la información en el marco jurídico interamericano, el cual es un resumen sobre el Estado de este

---

[16] Colombia, Costa Rica, México, Panamá, Perú y Venezuela se encuentran entre los países que han incorporado expresamente el derecho de acceso a la información pública en sus textos constitucionales. *Disponible (en inglés) en* http://www.right2info.org/.

[17] *Véase, por ejemplo*, en el asunto de inconstitucionalidad del artículo 13 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado (nº 18.575) (asunto Casas Cordero), sentencia del Tribunal Constitucional de Chile de 9 de agosto de 2007. Acordada de la Corte Suprema de Justicia de la Nación (Argentina), No. 1/2004 Exp. 315/2004 Adm. Gral. Para casos fuera del continente americano: *véase, por ejemplo, S.P. Gupta v. Union of India*, Tribunal Supremo (India), sentencia de 30 de diciembre de 1981, AIR [1982] (SC) 149, apdo. 232 ("cuando una sociedad ha escogido aceptar la democracia como credo de fe, es elemental que los ciudadanos deban saber qué hace su gobierno").

[18] *Véase, con carácter general*, http://www.right2info.org/laws.

[19] *Claude Reyes v. Chile*, nota 7 anterior, numeral 86. *Véase también la* Declaración Conjunta del Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y Expresión, el Relator Especial de la OEA para la Libertad de Expresión y el Representante de la OSCE para la Libertad de los Medios de Comunicación, de 26 de noviembre de 1999.

[20] Comisión de Derechos Humanos de Naciones Unidas, *Estudio sobre el Derecho a la Verdad, Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, 8 de febrero de 2006, E/CN.4/2006/91, disponible en http://www.unhcr.org/refworld/docid/46822b6c2.html, numerales 32 y 52.

[21] *Claude Reyes v. Chile*, nota 7 anterior, numeral 78 ("un consenso regional … sobre la importancia del acceso a la información pública y la necesidad de su protección").

derecho en la región, basado en las decisiones de la Corte Interamericana y la Comisión Interamericana, así como otras autoridades regionales.[22]

17. También en 2010, la Asamblea General de la OEA aprobó una Ley Modelo Interamericana sobre Acceso a la Información ("Ley Modelo Interamericana"),[23] que "establece la más amplia aplicación posible del derecho de acceso a la información que esté en posesión, custodia o control de cualquier autoridad pública [...] basada en el principio de máxima publicidad," con excepciones muy limitadas.[24] La Asamblea alentó a los Estados a diseñar, aplicar y evaluar sus leyes sobre el acceso a la información, de conformidad con la Ley Modelo Interamericana[25]; las leyes más recientes de la región, se han visto influenciadas por las disposiciones de la Ley Modelo Interamericana.

18. Tal como se desprende de estos documentos y de la jurisprudencia, el derecho de acceso a la información se deriva, en parte, del hecho de que el Estado posee una parte significativa de la información pública que una ciudadanía debidamente informada necesita. Este cuerpo de información se produce, recopila y maneja utilizando recursos públicos y en última instancia pertenece al público.

19. Así, el derecho tiene como principio fundamental el de la **máxima divulgación**: la presunción de que toda la información en posesión del estado (o de particulares, relacionada con el cumplimiento de funciones administrativas) debe estar sujeta a divulgación, a menos que exista un interés público o privado superior que justifique su no divulgación. La divulgación es la norma y no la excepción, y todas las dudas deben resolverse en favor de la divulgación.[26] El principio de máxima divulgación exige que restricciones limitadas sobre el derecho de acceso a la información, así como que toda limitación debe estar adecuadamente motivada.

20. El **ámbito de las instituciones y el tipo de información que cubren** las leyes de acceso a la información deben ser amplios. El ámbito de las leyes de acceso a la información debe incluir todos los organismos públicos "y las organizaciones que operan con fondos públicos o que desarrollan funciones públicas."[27] El público debería, en principio, tener acceso a toda la información producida o recopilada por el Estado, o que esté bajo la custodia, posesión o administración del Estado.[28] La Ley Modelo Interamericana también se aplica a toda autoridad pública que pertenezca a alguna de las ramas del estado (poderes ejecutivo, legislativo y judicial), las autoridades

---

[22] Oficina de la Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos, *El derecho de acceso a la información en el marco jurídico interamericano* (2010), disponible a http://www.oas.org/es/cidh/expresion/docs/publicaciones/ACCESO%20A%20LA%20INFORMACION%20FINAL%20CON%20PORTADA.pdf.

[23] *Véase la* Organización de los Estados Americanos, Ley Modelo Interamericana sobre Acceso a la Información Pública de 2010 ("Ley Modelo Interamericana"), aprobada en la cuarta sesión plenaria, celebrada el 8 de junio de 2010, por la Asamblea General de la OEA, mediante la resolución 2607 (XL-O/10). La Ley Modelo fue redactada por el Grupo de Expertos sobre Acceso a la Información (coordinado por el Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos), de conformidad con la resolución AG/RES. 2514 *Véase también los* Comentarios a la Ley Modelo Interamericana.

[24] *Ídem*, art. 2.

[25] *Proyecto de resolución: Acceso a la información pública y protección de datos personales*, CP/CAJP-2965/11 rev. 3 de 11 de mayo de 2011.

[26] *Claude Reyes v. Chile*, nota 7 anterior, numeral 92. Declaración Conjunta de los Relatores Especiales de 2004, nota 6 anterior. La mayor parte de los marcos jurídicos de los Estados miembros de la OEA incorporan el principio de máxima divulgación o de máxima publicidad, directa o indirectamente. *Véase* la Oficina de la Relatoría Especial para la Libertad de Expresión, Informe Anual de la Comisión Interamericana de Derechos Humanos, 2001, págs. 73, 198-211.

[27] *Véase, por ejemplo,* Comité Jurídico Interamericano, Principios sobre el derecho de acceso a la información, adoptado el 7 de agosto de 2008 en el 73º Periodo Ordinario de Sesiones (Río de Janeiro), principio 2. Ley Modelo Interamericana, nota 23 anterior, art. 3.

[28] *Véase* El derecho de acceso a la información en el marco jurídico interamericano, nota 22 anterior. Comité Jurídico Interamericano, Principios sobre el derecho de acceso a la información, nota 27 anterior, principio 3. Ley Modelo Interamericana, nota 23 anterior, art. 2.

constitucionales y legislativas, los órganos, organismos o entidades independientes o autónomos de propiedad del estado, así como a las organizaciones privadas que reciben fondos o beneficios públicos sustanciales (directa o indirectamente), o que desempeñan funciones y servicios públicos, pero solamente con respecto a los fondos o beneficios públicos recibidos, o a las funciones y servicios públicos desempeñados.[29]

21. El derecho de acceso a la información conlleva una **obligación de las autoridades públicas de divulgar** esa información. En respuesta a una solicitud de información, toda autoridad pública debe conformar o denegar la existencia de la información solicitada, y divulgar esa información, salvo en los casos en que se aplique una restricción legítima.[30] La denegación debe expresarse por escrito, y debe identificar las razones de la negativa y el daño específico que puede provocar a un interés protegido.[31] La carga de la prueba para justificar la no divulgación recae sobre la autoridad pública.[32] Si resulta aplicable una excepción legítima, que justifique no divulgar parte de la información de un registro, la autoridad pública está obligada a divulgar la parte del registro que contiene la información no sujeta a la excepción.[33] La información que se facilite y el proceso para acceder a ésta debe ser gratuita o de bajo costo, y accesible.[34]

22. El derecho de acceso a la información no es absoluto. La libertad de información está sujeta a limitaciones para proteger la divulgación de determinados tipos de información. No obstante, esas restricciones al acceso deben ser **excepciones muy limitadas, necesarias para proteger intereses legítimos**, e interpretadas estrictamente de conformidad con la presunción de acceso.[35] En virtud del artículo 13 de la Convención Americana y la jurisprudencia de la Corte Interamericana, las limitaciones al derecho a la información deben superar la prueba de proporcionalidad en tres pasos:

- En primer lugar, debe haber una **base jurídica clara y precisa para la limitación**.[36] El principio de legalidad garantiza una expectativa razonable de la interpretación de la ley y que la limitación no sea resultado del arbitrio del poder público.[37] El requisito de que una restricción debe estar prevista por la ley se refiere, tanto a la existencia como a la calidad de la ley, la cual debe evitar la interferencia arbitraria con el derecho de acceso a la información pública.[38]

- En segundo lugar, la limitación del derecho a la información debe responder a un **objetivo legítimo** reconocido por el artículo 13 de la Convención Americana. Los únicos objetivos legítimos reconocidos por el artículo 13.2 de la Convención Americana son "el respeto a los

---

[29] *Véase, con carácter general*, Sandra Coliver, *The Right to Information and the Increasing Scope of Bodies Covered by National Laws Since 1989* (2011), *disponible en* http://www.right2info.org/resources/publications/coliver-scope-of-bodies-covered-by-rti-laws. Algunas de las leyes más recientes, incluidas las de India (2005), Liberia (2010) y Nigeria (2011), se encuentran entre las más comunes.
[30] *Claude Reyes v. Chile*, nota 7 anterior, numeral 120.
[31] *Véase, p.ej., Ídem*, numeral 77. Los Comentarios a la Ley Modelo Interamericana, nota 23 anterior, Cap. 2(A), 2(D).
[32] Comité Jurídico Interamericano, Principios sobre el derecho de acceso a la información, nota 27 anterior, principio 7.
[33] *Véase* la Ley Modelo Interamericana, nota 23 anterior, art. 42.
[34] *Véase* El derecho de acceso a la información en el marco jurídico interamericano, nota 22 anterior, numeral 26. Declaración Conjunta de los Relatores Especiales de 2004, nota 6 anterior. Comité Jurídico Interamericano, Principios sobre el derecho de acceso a la información, nota 27 anterior, principio 5.
[35] *Claude Reyes v. Chile*, nota 7 anterior, numeral 92. Comité de Derechos Humanos de Naciones Unidas, *Observación general Nº 34 sobre el artículo 19*, nota 5 anterior, numeral 11.
[36] *Ídem*, en el numeral 89,
[37] *Ídem*, numerales 89 y 98.
[38] Comité de Derechos Humanos de Naciones Unidas, *Observación general Nº 34*, nota 5 anterior, numeral 25. *Véase también* el asunto *De Telegraaf contra los Países Bajos*, Tribunal Europeo de Derechos Humanos, sentencia de 22 de noviembre de 2012, numeral 90.

derechos o a la reputación de los demás" y "la protección de la seguridad nacional, el orden público o la salud o la moral públicas".[39]

- En tercer lugar, las restricciones que se impongan deben ser **necesarias en una sociedad democrática, lo que depende de que estén orientadas a satisfacer un interés público imperativo**[40] **y proporcionado al interés que lo justifica**.[41]

23. En lo que concierne a la tercera parte de esta prueba, para que la restricción sea **necesaria** debe ser el medio menos restrictivo para alcanzar el logro de ese legítimo objetivo.[42] Las restricciones "deben ser objeto de una interpretación estrictamente ceñida a las 'justas exigencias' de 'una sociedad democrática' que tenga en cuenta el equilibrio entre los distintos intereses en juego y la necesidad de preservar el objeto y fin de la Convención."[43]

24. Para que una restricción a la libertad de información sea **proporcionada**: (i) la restricción debe estar relacionada con un objetivo legítimo; (ii) la autoridad pública debe demostrar que la divulgación de la información efectivamente amenaza con causar un perjuicio sustancial a ese objetivo legítimo; [44] y (iii) la autoridad pública debe demostrar que el perjuicio al objetivo es mayor que el interés público en contar con la información.[45] El Estado debe demostrar, mediante "una decisión escrita fundamentada" las razones para restringir el acceso "en el caso concreto."[46]

25. La llamada prueba del daño e interés público se deriva del requisito de que las restricciones al derecho de acceso a la información sean proporcionadas y necesarias. De conformidad con la **prueba del daño**, una autoridad pública debe demostrar que la divulgación de información amenaza con provocar daños sustanciales a un interés protegido, lo que justifica su no publicación.[47] En particular, la Ley Modelo Interamericana exige que la excepción a la divulgación "genere un riesgo claro, probable y específico de un daño significativo" a un interés público identificado.[48]

26. La tendencia en las legislaciones nacionales es a considerar el daño que la divulgación puede causar al interés protegido a la hora de determinar si la clasificación es legítima. Varios países de la región, entre ellos Guatemala y Nicaragua, han incorporado un criterio de daño en sus leyes sobre clasificación o retención de información, limitando así la justificación para la no divulgación de la información a los casos en los que el "daño o perjuicio que pudiera causarse con la revelación de la

---

[39] *Ídem*, en el numeral 90. El PIDCP enumera una lista exhaustiva de objetivos legítimos para las excepciones a la libertad de expresión, incluido el derecho a la información. Entre ellos se encuentran (i) la seguridad nacional, (ii) la seguridad pública, (iii) el orden público, (iv) la protección de la salud o moral públicas, o (v) la protección de los derechos de los demás. PIDCP, artículos 19, 21. Comité de Derechos Humanos de Naciones Unidas, *Observación general Nº 34*, nota 5 anterior, numeral 22.

[40] *Claude Reyes v. Chile*, nota 7 anterior, numeral 91. *Opinión sobre La Colegiación Obligatoria de Periodistas*, nota 7 anterior, numerales 39 y 46 (demostrar la "necesidad" de una restricción requiere demostrar la existencia de una "interés público imperativo [...] que prepondere claramente sobre la necesidad social del pleno goce del derecho que el artículo 13 garantiza).

[40] *Opinión sobre La Colegiación Obligatoria de Periodistas*, nota 7 anterior, numeral 39.

[41] *Claude Reyes v. Chile*, nota 7 anterior, numerales 89-91. *Véase también la* Oficina de la Relatoría Especial para la Libertad de Expresión, Informe Anual de la Comisión Interamericana de Derechos Humanos, 2011 (el "Informe de la Relatoría Especial de la OEA de 2011"), cap. III, numerales 342-43, 347.

[42] *Véase Claude Reyes v. Chile*, nota 7 anterior, numeral 91.

[43] *Opinión sobre La Colegiación Obligatoria de Periodistas*, nota 7 anterior, numeral 67.

[44] *Véanse* los Comentarios a la Ley Modelo Interamericana, nota 23 anterior, p. 10. Para un ejemplo comparado, véase también *Kuije/Consejo*, un asunto del Tribunal de Primera Instancia de las Comunidades Europeas, el Tribunal falló en favor del solicitante de información, señalando que la autoridad pública no había tenido en cuenta los efectos prácticos que podría tener la divulgación, en este caso, sobre las relaciones de la UE con esos terceros países.

[45] El derecho de acceso a la información en el marco jurídico interamericano, nota 22 anterior, p. 53.

[46] *Claude Reyes v. Chile*, nota 7 anterior, numeral 95.

[47] Los Comentarios a la Ley Modelo Interamericana, nota 23 anterior, Cap. 2(F). *Véase* la Ley Modelo Interamericana, nota 23 anterior, arts. 41(b), 44.

[48] Ley Modelo Interamericana, nota 23 anterior, art. 41(b).

información es mayor que el interés público en conocer la información".[49] Al menos diez países europeos[50] exigen que el gobierno pruebe que la divulgación puede causar un daño real o potencial para imponer cualquier sanción a la revelación no autorizada de información gubernamental; y otros tres países[51] permiten alegar la inexistencia de daño como defensa o circunstancia atenuante. Varios países exigen también que se pruebe el daño real o potencial.[52]

27. La **prueba del interés público** exige que una autoridad pública o un organismo de revisión pondere el daño que la divulgación provocaría al interés protegido, respecto al interés público al que sirve la divulgación de la información. El interés público en la revelación es mayor cuando la información se refiere a delitos, "incluidos los cometidos por miembros de los servicios secretos" e incluyendo, en especial, información sobre corrupción.[53] Además, el derecho de acceso a la información es inviolable cuando se refiere a las violaciones graves de los derechos humanos o a las violaciones graves del derecho internacional humanitario.[54] Así, la Corte Interamericana de Derechos Humanos ha reconocido un derecho autónomo a la verdad al amparo de la Convención Americana.[55] La Ley Modelo Interamericana,[56] y las leyes de otros países de la región,[57] han reconocido que las excepciones a la divulgación no son aplicables a casos de información relacionada con violaciones de los derechos humanos o crímenes contra la humanidad.

28. El Tribunal Europeo de Derechos Humanos también ha reconocido que existe "poco margen (...) para la restricción del debate en torno a cuestiones de interés público", ya que "las acciones u omisiones del gobierno deben estar sujetas a un examen minucioso no solo por parte de los poderes legislativo y judicial, sino también de los medios de comunicación y de la opinión pública".[58] La Asamblea Parlamentaria del Consejo de Europa ha identificado diversos motivos —aparte de los casos en los que se hayan demostrado que existen delitos— que constituyen un caso de "interés público superior" que requiere la revelación de la información a pesar de la existencia de una "excepción legítima" al acceso a la misma. Entre estos motivos se incluyen los casos en los que la información pudiera "suponer una importante contribución a un debate público; promover la

---

[49] Ley de Acceso a la Información Pública (Guatemala), Decreto Nº 57/2008, disponible en http://www.scspr.gob.gt/docs/infpublic.pdf, art. 26. Ley de Acceso a la Información Pública, Ley 621 de 2007 (Nicaragua), disponible en http://legislacion.asamblea.gob.ni/NormaWeb.nsf/($All)/675A94FF2EBFEE9106257331007476F2?OpenDocument, artículo 3(7).

[50] Albania, República Checa, Alemania, Italia, Moldavia, Noruega, Países Bajos, Rumania, España y Suecia. *Véase, en general*, Amanda Jacobsen, *National Security and the Right to Information in Europe* ("La seguridad nacional y el derecho a la información en Europa") (marzo 2013) (estudio de la Universidad de Copenhague, en colaboración con la Open Society Justice Initiative).

[51] Dinamarca, Francia y Hungría. *Ídem*

[52] Chile establece sanciones penales por revelación no autorizada solo en aquellos casos en que la revelación produce daños reales y "graves". Paraguay exige que la revelación exponga al Estado a un "riesgo de daño grave para su seguridad externa".

[53] *Véase, p. ej.,* Asamblea Parlamentaria del Consejo de Europa, Resolución 1838 (2011), adoptada el 6 de octubre de 2011, art. 8.

[54] ACNUDH, *Estudio sobre el Derecho a la Verdad,* nota 20 anterior, numeral 59. Conjunto de principios actualizado para la protección y promoción de los derechos humanos mediante la lucha contra la impunidad, Resolución 2005/81, ONU Doc. E/CN.4/2005/102/Add. l, del 8 de febrero de 2005, Principios 2, 16.

[55] *Véase, p. ej., Gomes Lund contra Brasil,* Corte IDH, Sentencia de 24 noviembre de 2010, Serie C Nº 219. numerales 200-01; *Gelman contra el Uruguay,* Corte I.D.H., Sentencia de 24 de febrero 2011, numerales 118, 192, 243.

[56] Ley Modelo Interamericana, nota 23 anterior, artículo 44 (las excepciones al derecho de acceso estipuladas en la ley "no deberán aplicarse en casos de graves violaciones de derechos humanos o de delitos contra la humanidad").

[57] Ley de Transparencia y Acceso a la Información Pública Nº 27806 de 2002 (Perú), artículo 15. Ley Federal de Transparencia y Acceso a la Información Pública de 2002 (México), artículo 14. Ley de Acceso a la Información Pública, aprobada por Decreto 57-2008 del Congreso de 2008 (Guatemala), artículo 24. Ley de Acceso a la Información Pública, Ley Nº 12.527 del año 2011 (Brasil), artículo 21. Ley sobre el Derecho de Acceso a la Información Pública, Ley n. º 18.381 de 2008 (Uruguay), artículo 12.

[58] *Guja contra Moldavia*, Tribunal Europeo de Derechos Humanos (GC), Sentencia de 12 de febrero de 2008, numerales 72, 74. *Véase también Palamara-Iribarne contra Chile,* Corte IDH, Sentencia del 22 de noviembre de 2005, numeral 88.

participación pública en el debate político; … mejorar la responsabilidad en la gestión de los asuntos públicos en general, y en el uso de fondos públicos en particular; [y] suponer un beneficio para la salud pública o la seguridad".[59]

29. La existencia de una prueba de interés público en una ley de acceso a la información se considera, por lo general, una señal de la fortaleza de ese derecho. Casi la mitad de las leyes estudiadas en un análisis comparativo reciente incluyen una prueba del interés público.[60] Este análisis reciente de 93 leyes nacionales sobre el derecho de acceso a la información identificó que las pruebas del interés público son sólidas y eficaces cuando (i) son obligatorias, (ii) se aplican a todas las excepciones; (iii) están estructuradas de forma que favorezcan la divulgación, y (iv) establecen los factores correspondientes que hay que tener en cuenta.[61]

30. Además, **la no divulgación debe tener una duración limitada**, ya que todas las justificaciones legítimas para la no divulgación de registros se debilitan con el paso del tiempo.[62] Unos periodos de clasificación de la información excesivamente largos minan la esencia propia del derecho de acceso a la información del artículo 13. Por estas razones, muchos países democráticos han adoptado regímenes para la desclasificación periódica o automática de información reservada al objeto de promover que se libere la información, incluso cuando no haya sido expresamente solicitada.[63] A este respecto, la Ley Modelo Interamericana establece que las excepciones a la divulgación, incluida la excepción en aras de la seguridad nacional, "no son aplicables en el caso de un documento que tenga más de [doce] años de antigüedad," a período que puede ampliarse solo una vez, "por autorización de la Comisión de Información" y no por la autoridad que originariamente clasificó la información.[64] Las leyes nacionales de prácticamente todos los países de la región

---

[59] Resolución APCE 1954 (2013), adoptada el 2 de octubre de 2013, numeral 9.5. *Véanse también* Principios de Tshwane, nota 4 anterior, Principio 3, nota ("factores que favorecen la divulgación").

[60] Maeve McDonagh, *La prueba del interes public en la legislation del derecho a la información*, pág. 6 (44 de 93 países).

[61] *Ídem*, p. 19.

[62] *Véase también Turek v. Eslovaquia*, TEDH, sentencia de 14 de febrero de 2006, numeral 115 (el Tribunal rechazó la presunción de que "existe un interés público continuado y efectivo en imponer limitaciones al acceso a los materiales clasificados como confidenciales por regímenes anteriores").

[63] En la región, Chile, Colombia, Guatemala, Nicaragua y Panamá disponen un período máximo de clasificación. El Informe de la Relatoría Especial de la OEA de 2011, nota 41 anterior, numeral 357. Ley de Acceso a la Información Pública (Nicaragua) (2007), arts. 28, 29, disponible en http://legislacion.asamblea.gob.ni/NormaWeb.nsf/($All)/675A94FF2EBFEE910625733100747 6F2?OpenDocument. Ley de Transparencia en la Administración Pública (Panamá) (2002), artículo 7, disponible en http://www.presidencia.gob.pa/ley_n6_2002.pdf. Ley de Transparencia en la Administración Pública y Acceso a la Información de la Administración del Estado (Chile) (2009), disponible en http://www.leychile.cl/Navegar?idNorma=276363. Ley de Acceso a la Información Pública (Guatemala), artículo 44, disponible en http://www.scspr.gob.gt/docs/infpublic.pdf. Ley Orgánica de Transparencia y Acceso a la Información Pública (Ecuador, artículo 9 (2), disponible en http://www.informatica.gob.ec/files/LOTAIP.pdf. Ley de Acceso a la información del Uruguay, Ley n. º 18.381, artículo 18, disponible en http://www.informacionpublica.gub.uy/sitio/descargas/normativa-nacional/ley-no-18381-acceso-a-la-informacion-publica.pdf. Ley de Transparencia y Acceso a información pública (Perú), artículo 11, disponible en http://www.peru.gob.pe/normas/docs/LEY_27806.pdf. Lay Federal de Transparencia y Acceso a Información Pública Gubernamental (México), artículo 44, disponible en http://www.ifai.org.mx/English. Ley 57 de 1985 (Colombia), artículo 13. Ley 594 de 2000 (Colombia), artículo 28 (que establece que las clasificaciones con respecto a cualquier documento legal terminarán después de 30 años a partir de su expedición); Ley 1097 de 2006 (Colombia), artículo 5 (que establece un período de clasificación de 20 años para "gastos clasificados"). La tendencia entre los Estados miembros del Consejo de Europa ha sido la de establecer procedimientos de desclasificación que estipulen un límite de tiempo, un supuesto determinante, o un período obligatorio de revisión a fin de garantizar que la información no permanezca indefinidamente clasificada. Un estudio realizado sobre las leyes y los reglamentos que rigen la clasificación y la desclasificación de información en los países europeos encontró que 13 (de 19) tienen períodos de clasificación máxima obligatoria. Otros tres exigen que se revisen las decisiones de clasificación, al menos, cada cinco años. *Véase, en general*, Amanda Jacobsen, *National Security and the Right to Information in Europe*, nota 50 anterior, y en comunicación con expertos de distintos países.

[64] *Véase* la Ley Modelo Interamericana, nota 23 anterior, art. 43. La mayor parte de categorías de información reservada o clasificada deben hacerse públicas tras un periodo de 12 años. Para los registros más confidenciales, la clasificación inicial podría extenderse por otros 12 años, con sujeción a la aprobación de una autoridad de información independiente.

contemplan periodos máximos durante los que se puede mantener información clasificada en secreto,[65] y "una vez vencido ese periodo, la información debe poder ser consultada por el público."[66]

31. **La información procedente de los servicios de seguridad de un régimen autoritario anterior debe estar sujeta a una presunta obligación de divulgación**, dado que la no divulgación de información a lo largo de un período de tiempo prolongado resulta especialmente injustificable en lo referente a los archivos relacionados con las violaciones de los derechos humanos que impliquen a las fuerzas de la seguridad de dichos regímenes autoritarios. La Corte Interamericana de Derechos Humanos ha destacado —ampliando su jurisprudencia en relación con el derecho a la verdad y el deber de los Estados de revelar información sobre las violaciones de los derechos humanos— la superior obligación de los Estados, tras la desaparición de un régimen represivo, de divulgar la información relativa a todas las violaciones de los derechos humanos cometidas por dicho régimen represivo, incluidos, especialmente, los registros de las fuerzas de la seguridad e identificados como clasificados o destruidos.[67] En el asunto *Turek contra Eslovaquia*, el Tribunal Europeo de Derechos Humanos consideró que "no es posible suponer que persiste un interés público real y continuado en la imposición de limitaciones al acceso a los materiales clasificados como confidenciales por los regímenes [autoritarios] anteriores", especialmente cuando tales registros "no están directamente ligados a las funciones y operaciones actuales de los servicios de seguridad".[68]

32. La práctica de los Estados es cada vez más coherente con el principio de que la información relacionada con las acciones de los regímenes autoritarios anteriores —y, en especial, las violaciones de los derechos humanos cometidas por dichos regímenes—, debe ser objeto de divulgación obligatoria o presunta. Así, los gobiernos de diferentes países de América Latina y Europa han desclasificado masivamente los registros de regímenes autoritarios anteriores.[69]

33. La experiencia acumulada en varios procesos judiciales de transición ha evidenciado que la clasificación de registros antiguos no sirvió verdaderamente a ningún interés de seguridad nacional, siendo a menudo invocada tan solo para proteger a los autores frente a la acción de la justicia.[70] La reconstrucción objetiva de la verdad acerca de los abusos cometidos en el pasado resulta esencial para que las naciones puedan aprender de su historia y tomen las medidas necesarias para evitar que

---

[65] El Informe de la Relatoría Especial de la OEA de 2011, nota 41 anterior, cap. III, numeral 357.

[66] *Ídem*, en el numeral 348 ("[S]olo podrá mantenerse la reserva mientras subsista efectivamente el riesgo cierto y objetivo de que, al revelarla, resultará afectado de manera desproporcionada uno de los bienes que el artículo 13.2 de la Convención Americana autoriza proteger").

[67] *Véase Myrna Mack contra Guatemala*, Corte IDH., 25 de noviembre de 2003, numeral 180; *Gomes Lund contra Brasil*, nota 55 anterior, numerales 200, 202.

[68] *Turek contra Eslovaquia*, Tribunal Europeo de Derechos Humanos, 14 de febrero de 2006, numeral 115 (procedimiento de depuración en contra del demandante). *Véase también Jalowiecki contra Polonia*, Tribunal Europeo de Derechos Humanos, 17 de febrero de 2009, numeral 37.

[69] Emi MacLean, *Archives of State Security Service Records* ("Archivos de los registros de los servicios de seguridad del Estado") (2013), disponible en http://www.right2info.org/resources/publications/publications_nat-sec_archives-of-state-security-service-records.

[70] *Véase, por ejemplo,* Dale McKinley, *The State of Access to Information in South Africa*, ("El estado del acceso a la información en Sudáfrica"), preparado por el Centro para el Estudio de la Violencia y la Reconciliación, pág. 23; Informe Anual de la Oficina del Relator Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos (2010), Capítulo III, disponible en http://www.oas.org/en/iachr/expression/docs/reports/access/Right%20to%20Access%20Araguaia%202010.pdf, págs. 316-317. *Véase en general* Peter Kornbluh, *The Pinochet File*: *A Declassified Dossier on Atrocity and Accountability* ("El sumario Pinochet: la desclasificación de un informe sobre atrocidades y responsabilidad") (The New Press), 2004.

se repitan crímenes atroces en el futuro.[71] Al mismo tiempo, el paso del tiempo elimina cualquier justificación legítima para mantener la clasificación.

34. **La información importante para prevenir y hacer responsables a las personas por corrupción también deberá ser divulgada.** El reconocimiento internacional del derecho fundamental de acceso a la información relativa a la corrupción se demuestra en el aumento de instrumentos internacionales y regionales, leyes y reglamentos nacionales, para proteger la divulgación autorizada y no autorizada de información relacionada con corrupción pública o de entidades designadas, aun cuando existiera otro tipo de obligaciones de proteger la confidencialidad de la información por seguridad nacional u otras razones.

35. Los instrumentos internacionales y regionales requieren cada vez más la divulgación de dicha información, y recomiendan o exigen que los estados protejan a los empleados y miembros del público de cualquier sanción por suministrar información sobre hechos de corrupción.[72] Ninguno especifica si los empleados del sector de seguridad pueden o no acceder a tal protección. Esto se debe al gran interés público en su divulgación. Aun cuando normalmente los empleados tengan deber de confidencialidad sobre dicha información, los instrumentos internacionales reconocen claramente que el interés público prevalece incluso sobre los deberes de lealtad y confidencialidad.

36. Algunos países impiden la clasificación de información sobre temas relacionados con la corrupción,[73] o proveen una justificación para la divulgación no autorizada de información allá donde se lleve a cabo en nombre del interés público, ya sea como un elemento de discrecionalidad del ministerio público fiscal o como defensa ante cualquier cargo.[74] Otros países incluso requieren

---

[71] Comisión de Derechos Humanos de la ONU, Conjunto de Principios actualizado para la Protección y Promoción de los Derechos Humanos mediante la lucha contra la impunidad, Resolución 2005/81, aprobada en 2005 ("Principios actualizados sobre la impunidad"), Principios 2, 3.

[72] La Convención de las Naciones Unidas contra la corrupción, adoptada el 31 de octubre de 2003, que entró en vigencia el 14 de diciembre de 2005 (con 167 estados miembros), Arts. 8(4), 10, 32-33. de la Convención Interamericana contra la Corrupción, adoptada por la Organización de los Estados Americanos el 29 de Marzo de 1996, que entró en vigencia el 3 de junio 1997, Arts. III(8). Organización de los Estados Americanos, Ley Modelo para la Protección de la Libertad de Expresión contra la Corrupción, 2002 (para implementar la disposición de la Convención Interamericana contra la Corrupción que protege a los funcionarios públicos y miembros del público contra sanciones por denuncias de corrupción), Art. 2. Convenio de Derecho Civil contra la Corrupción, adoptado por el Consejo de Europa el 4 de noviembre de 1999, que entró en vigencia el 1 de noviembre de 2003, Art. 9. Asamblea Parlamentaria del Consejo de Europa, Resolución 1729, adoptada el 29 de abril de 2010, Art. 6.1.2 (la ley de protección de los denunciantes "debería, por lo tanto, alcanzar tanto a denunciantes del sector público y privado, incluyendo a los miembros de las fuerzas armadas y los servicios especiales"). Convención para Prevenir y Combatir Corrupción de la Unión Africana, adoptada el 11 de julio 2003, que entró en vigencia el 5 de agosto de 2006 (ratificada por Sudáfrica en 2005), Arts. 1, 5(5), 5(6) (requiriendo a los estados miembros la adopción de medidas para "asegurar que los ciudadanos denuncien casos de corrupción sin temor a represalias posteriores"). Para derecho y práctica comparadas, véase en general Venkatesh Nayak, *Public Interest Disclosure and Protection to Persons Making the Disclosures Bill (India's Whistleblower Bill): A comparison with International Best Practice Standards* (2010) (un estudio comparativo de la legislación de protección de los denunciantes en 20 países que se considera aplican "buenas prácticas"); Benjamin Buckland & Aidan Wills, *Blowing in the Wind? Whistleblowing in the security sector*, 2012, disponible en http://www.right2info.org/resources/publications/pretoria-finalization-meeting-april-2013-documents/whistleblowing-and-security-sector-buckland-and-wills/view.

[73] La ley de secretos de estado de Albania est que la información no podrá ser clasificada si su objetivo es encubrir ineficiencias o errores del gobierno, limitar indebidamente el acceso a información que no debiera ser clasificada en interés de la seguridad nacional. Ley No. 8457, sobre información clasificada "secretos de estado" (Albania), 1999, Art. 10.

[74] Código Penal (Argentina), Art. 155. Ley No. 8.122, estableciendo un régimen legal para los funcionarios públicos (Brasil), 1990, en http://www.planalto.gov.br/ccivil_03/leis/l8112compilado.htm, Art. 126-A. Código Penal (Dinamarca), 2008, Art. 152, en https://www.retsinformation.dk/Forms/R0710.aspx?id=142912#Kap13, Art. 152(e)(2). Ley del Funcionario Público (*Beamtenstatusgesetz*), 2008, en http://www.gesetze-im-internet.de/bundesrecht/beamtstg/gesamt.pdf, Sec. 38(2); Ley de Restructuración del Servicio (*Dienstrechtsneuordnungsgesetz*), 2008 (citado en Jacobsen, *National Security and the Right to Information in Europe*, nota 354). Código Penal (Alemania), 1998 (a partir del 2 de octubre de 2009), en http://www.gesetze-im-internet.de/stgb/BJNR001270871.html, Sec. 93(2). Ley del Denunciante, Ley 720/2006 (Ghana), en http://www.parliament.gh/assets/file/Acts/Whitsleblwer%20Act%20720.pdf, Arts. 1, 3. Ley de Libertad de Información (Nigeria), 2011, en http://www.noa.gov.ng/attachments/article/140/Freedom%20Of%20Information%20Act.pdf, Art. 27(2)

la denuncia de actos de corrupción o de la comisión de un delito (o de ciertos tipos de delitos), generalmente a través de la divulgación a las autoridades, y en algunos casos sancionando a los funcionarios públicos que no lo hacen.[75]

37. La Ley de protección de los denunciantes de Rumania, por ejemplo, se aplica a las autoridades públicas y a las instituciones de la administración pública central y no excluye al sector de la seguridad. Esta ley protege divulgaciones concernientes a corrupción, incompetencia o infracciones legales relacionadas con la buena administración y la protección del interés público. Las divulgaciones protegidas se pueden hacer internamente, cuando se trate de los órganos de control, las autoridades judiciales, las comisiones parlamentarias, o bien públicamente, como en los casos relativos a medios de comunicación, sindicatos y organizaciones no gubernamentales. [76] La ley estipula sanciones penales para los funcionarios públicos que no divulguen información concerniente a la comisión de un delito.[77]

38. El solicitante de la información debe tener derecho a un **recurso independiente y eficaz** de la denegación de su derecho de acceso a la información.[78] La decisión final sobre si se debe divulgar o no cierta información no puede dejarse a la discreción de las autoridades públicas, sino que debe estar sujeta a la revisión independiente de un "tribunal o corte competente."[79] De hecho, "la salvaguarda de la persona frente al ejercicio arbitrario del poder público es el objetivo primordial de la protección internacional de los derechos humanos."[80] En el contexto del derecho de acceso a la información, la revisión y el recurso independientes y eficaces deben incluir un recurso "sencillo, efectivo, expedito y no oneroso, y que permita controvertir las decisiones de los funcionarios públicos que nieguen el derecho de acceso a una determinada información o que simplemente omitan dar respuesta a la solicitud."[81] El recurso debe ser adecuado para proteger el derecho y eficaz, es decir, capaz de conseguir el resultado que se pretende.[82]

39. Además del derecho a solicitar información y la correspondiente obligación de la autoridad pública de responder a dicha solicitud, también ha habido un creciente reconocimiento de la importancia de la **divulgación proactiva**.[83] Muchos de los principales regímenes sobre la libertad de la información en América y en el resto del mundo exigen a las autoridades públicas que recopilen, manejen y publiquen, de forma proactiva, la información sobre determinados asuntos que se consideren importantes para la responsabilidad democrática.[84] Un lenguaje similar, utilizado en la

---

(estableciendo que el estado no puede procesar por la Ley de Secretos Oficiales o el Código Penal a ningún funcionario público que divulgue información sin autorización a cualquier persona "cuando razonablemente crea que demuestra (a) la violación de cualquier ley, norma o reglamento, (b) mala gestión, grave dilapidación de fondos, fraude y abuso de autoridad; o (c) un peligro sustancial y específico para la salud o la seguridad pública…"). Ley de Integridad y Prevención de la Corrupción (Eslovenia), 2011, Art. 23(4). Ley de Protección del Denunciante (Uganda), 2010, en http://igg.go.ug/static/files/publications/Whistle_blowers_Act.pdf, Arts. 1-4. Servicio de Fiscalía de la Corona, Código de Fiscales de la Corona 2.6, 3.4 (2010) (R.U.).

[75] Código Penal (Argentina), Art. 277(d). Código Penal (México), Art. 215. Amanda Jacobsen, *National Security and the Right to Information in Europe*, nota 50 anterior, pág. 54 (se hace referencia a Italia).

[76] Ley de protección de los funcionarios públicos que denuncien violaciones a la ley (Ley del denunciante), Ley 571/2004 (Rumania), 2004, Arts. 1, 5, 6.

[77] Código Penal (Rumania), Art. 263.

[78] *Véase* El derecho de acceso a la información en el marco jurídico interamericano, nota 22 anterior, numerales 26-31.

[79] *Claude Reyes v. Chile*, nota 7 anterior, numeral 129.

[80] *Ídem*, en el numeral 129.

[81] Oficina de la Relatoría Especial para la Libertad de Expresión, Informe Anual de la Comisión Interamericana de Derechos Humanos, 2009, apdo. 29. *Claude Reyes v. Chile*, nota 7 anterior, numeral 137.

[82] *Véase el asunto Hermanas Serrano-Cruz v. El Salvador*, Corte IDH, sentencia de 23 de noviembre de 2004 (Excepciones Preliminares), Serie C nº 118, numeral 134. *Gomes Lund v. Brasil*, nota 55 anterior, numeral 231.

[83] *Véase la* Declaración Conjunta de los Relatores Especiales de 2004, nota 6 anterior.

[84] *Véase, con carácter general*, Helen Darbishire, *Proactive transparency: the future of the right to information?* (el Serie del Instituto de Gobernación del Banco Mundial), 2010.

Ley Modelo Interamericana, recomienda que se obligue a las autoridades públicas a publicar y actualizar, de forma proactiva, 16 categorías distintas de información, relacionadas con sus respectivas políticas internas, servicios y operaciones, gestión financiera, altos funcionarios y sistemas de mantenimiento de documentos.[85]

C. Acceso a la Información y la Seguridad Nacional

40. El derecho de acceso a la información, y la justificación que subyace a este derecho, sirven para garantizar el acceso público a la información mantenida por las instituciones de las fuerzas de la seguridad y a la información relacionada con la seguridad nacional.[86] Aunque el Estado puede imponer restricciones necesarias y proporcionadas al derecho de acceso a la información por razones de seguridad nacional en determinadas circunstancias, cualquier restricción basada en la seguridad nacional debe cumplir con los principios enumerados anteriormente.[87]

41. La Corte Interamericana de Derechos Humanos, el Tribunal Europeo de Derechos Humanos y el Comité de Derechos Humanos de la ONU han reconocido en numerosas ocasiones que la información relacionada con la seguridad nacional, incluso la clasificada, no está exenta del acceso público solo por dicha razón; las decisiones sobre su clasificación deben justificarse y el público debe poder solicitar su desclasificación.[88] Este principio está siendo cada vez más reconocido por la legislación y la práctica nacionales. Por ejemplo la Corte Constitucional de Colombia en una decisión de 2013 rechazó, tanto por inconstitucional como por infringir el Derecho internacional vinculante, la propuesta de excluir del ámbito de aplicación de una nueva ley sobre acceso a la información aquella información relacionada con la defensa y la seguridad nacional.[89] Tanto la Ley Modelo Africana como la Interamericana son aplicables a todos los poderes públicos sin limitación alguna.[90]

42. El Comité de Derechos Humanos de la ONU ha declarado oficialmente que no es compatible con el artículo 19(3) del PIDCP que un Estado invoque las leyes sobre el secreto de Estado para "sustraer del conocimiento público aquella información de interés legítimo que no perjudique a la seguridad nacional", y que la divulgación pública solo debe ser objeto de castigo "cuando la divulgación de dicha información pudiera perjudicar a la seguridad nacional".[91]

43. Los Principios Globales sobre Seguridad Nacional y el Derecho a la Información (los "Principios de Tshwane"), mencionados anteriormente (véase párr. 6), fundamentan el hecho de limitar las restricciones al derecho de acceso a la información por razones de seguridad nacional. El Principio de Tshwane Nº 3 establece que: "No podrán aplicarse restricciones al derecho a la información por

---

[85] *Véase* la Ley Modelo Interamericana, nota 23 anterior, art. 12.
[86] Comité de Derechos Humanos de Naciones Unidas, *Observación general Nº 34*, nota 5 anterior, numerales 7, 18.
[87] *Véase, por ejemplo,* Asamblea Parlamentaria del Consejo de Europa, Resolución 1551 (2007), Resolución sobre el espionaje y la divulgación de secretos de Estado, 19 de abril de 2007, numerales 1, 9 ("el interés legítimo del Estado en proteger los secretos no debe convertirse en un pretexto para restringir indebidamente la libertad de expresión y de información").
[88] *Gomes Lund contra Brasil*, nota 55 anterior. *Turek contra Eslovaquia*, Tribunal Europeo de Derechos Humanos, Sentencia del 14 de febrero de 2006, numeral 115. *Toktakunov contra Kirguistán,* Comité de Derechos Humanos, decisión de 28 de marzo de 2011, ONU Doc. CCPR/C/101/D/1470/2006, numerales 7.7 – 7.8 (considerando como una violación del artículo 19 del ICCPR el hecho de que el Estado parte clasifique y retenga por motivos de seguridad nacional estadísticas sobre la pena de muerte, dado el "legítimo interés público en el acceso a la información sobre el empleo de la pena de muerte"). Comité de Derechos Humanos de Naciones Unidas, *Observación general Nº 34*, nota 5 anterior, numeral 30.
[89] Caso Nº D-9095, sentencia C-262/13, Corte Constitucional (Colombia), 8-9 de mayo de 2013, numeral 16, disponible en http://www.corteconstitucional.gov.co/comunicados/No.%2018%20comunicado%2008%20y%2009%20de%20mayo%20de%202013.pdf (rechazando como inaplicable el artículo 5, numeral 2).
[90] Ley Modelo sobre el acceso a la información de África, aprobada por la CADHP, 6 de mayo de 2013, arts. 1, 2(a), 12(1) *Ley Modelo Interamericana*, nota 23 anterior, art. 1(e), 3.
[91] Comité de Derechos Humanos de Naciones Unidas, *Observación general Nº 34*, nota 5 anterior, numeral 30. *Véanse también* observaciones finales de la Federación de Rusia (CCPR/CO/79/RUS), 1 de diciembre de 2003, numeral 22. CDHNU, Observaciones Finales del Reino Unido (CCPR/CO/73/REINO UNIDO), 6 de diciembre de 2001, numeral 21.

razones de seguridad nacional a menos que el gobierno demuestre que: (1) la restricción (a) está establecida en una ley y (b) resulta necesaria en una sociedad democrática (c) para proteger un interés legítimo de seguridad nacional; y (2) la ley establece garantías adecuadas contra la posibilidad de abuso, incluido el escrutinio oportuno, pleno, accesible y efectivo de la validez de las restricciones por una autoridad de supervisión independiente y su revisión exhaustiva por la justicia".

44. Los Principios de Tshwane reconocen que el derecho de acceso a la información en poder del Estado, "incluida la información relativa a la seguridad nacional", resulta necesario para que el público pueda "controlar la conducta de su gobierno y participar plenamente en una sociedad democrática, que tengan acceso a información en poder de autoridades públicas".[92] Los Principios definen cuáles son dichas autoridades públicas, incluyendo entre ellas a las fuerzas de seguridad, y prohíben expresamente la exención categórica de ninguna autoridad pública de la obligación de divulgar información.[93]

45. Los Principios señalan específicamente que el público tiene derecho a conocer la existencia de todas las entidades que integran las fuerzas de seguridad, las leyes y reglamentos por los que se rigen y sus presupuestos.[94] Además, de acuerdo a los Principios de Tshwane, los gobiernos nunca deben retener información sobre violaciones de los derechos humanos y del Derecho internacional humanitario.[95]

46. Los Principios de Tshwane reconocen que los gobiernos pueden legítimamente retener información en áreas muy definidas, tales como los planes de defensa, el desarrollo de armas y las operaciones y fuentes utilizadas por los servicios de inteligencia.[96] Sin embargo, en cada caso, el gobierno tiene la carga de la prueba para demostrar la necesidad de las restricciones al derecho de acceso a la información pública, incluyendo el deber de la autoridad pública de "aportar razones concretas y sustantivas que demuestren sus afirmaciones" de que existe un "riesgo de daño" derivado de la revelación de información identificable. Una declaración genérica indicando que la divulgación podría perjudicar la seguridad nacional puede ser inconcluyente.[97]

47. La clasificación, cuando se utilice, debería requerir que se identifique en qué "categoría acotada de información" queda comprendida la información, así como "cuál sería el perjuicio si esta se difundiera".[98] Además, la información debería ser clasificada solo durante el tiempo necesario y nunca de forma indefinida. La legislación deberá establecer el período máximo permitido para mantener información clasificada.[99]

48. Reconociendo la obligación de revelar la verdad sobre los abusos cometidos en el pasado por los regímenes autoritarios —y la disminución de las razones que justifican el secreto de esta información histórica—, los Principios de Tshwane establecen que "existe un interés público preponderante en cuanto a la divulgación de las informaciones relativas a violaciones de los derechos humanos cometidas bajo el anterior régimen", y además establecen que "[E]l gobierno sucesor debería, inmediatamente, dedicarse a proteger y preservar la integridad de todos los documentos que contengan dichas informaciones ocultas por el gobierno anterior, y publicarlas inmediatamente".[100]

---

[92] Principios de Tshwane, nota 4 anterior, Preámbulo.
[93] *Idem.*, Definiciones y Principio n. º 5.
[94] *Idem.*, Principios 10C, 10F.
[95] *Idem.*, Principio 10A.
[96] *Idem.*, Principio 9.
[97] *Idem.*, Principio 4.
[98] *Idem.*, Principio 11.
[99] *Idem.*, Principios 16, 10D.
[100] *Idem.*, Principio 10A (3).

49. Con frecuencia, la corrupción en el sector de la seguridad es particularmente preocupante, ya que la cantidad de fondos aumenta el riesgo en un clima de secretismo.[101] Andrew Feinstein, un experto en corrupción en el comercio de armas, escribe, por ejemplo, que aproximadamente el 40 por ciento de la corrupción en el comercio mundial se produce como resultado del tráfico de armas, y que el secretismo es una de las causas más importantes: "El pequeño número de personas que deciden sobre contratos multimillonarios, las grandes sumas de dinero en juego y el velo de secretismo que cubre las transacciones que se llevan a cabo (en interés de la 'seguridad nacional') aseguran la propensión de la industria a la corrupción."[102] Reconociendo la obligación de divulgar información para prevenir la corrupción y hacer responsables a sus autores, los Principios de Tshwane requieren la divulgación pública de "información suficiente para que el público pueda entender las finanzas del sector de seguridad, así como las normas que regulan las finanzas de dicho sector."[103]

50. El acceso del público a la información del gobierno sobre las fuerzas de seguridad es especialmente importante debido a la discrecionalidad con que el poder ejecutivo suele moverse en ésta área debido a sus amplios poderes, como la financiación de la guerra y de las operaciones contra el terrorismo, el desarrollo de operaciones de vigilancia, detención e interrogatorio de personas; y su control de importantes fondos públicos. La excesiva deferencia con los argumentos relativos al secreto por causa de la seguridad nacional puede contribuir a las violaciones de los derechos humanos, la corrupción, el despilfarro y los abusos, siendo el secreto un obstáculo para la atribución de responsabilidades.[104]

III. LA ADECUACIÓN DEL DECRETO LEGISLATIVO Nº 1129 AL DERECHO INTERNACIONAL

51. En esta sección se presentan, en primer lugar, las disposiciones de la Constitución del Perú y de las leyes que regulan el derecho de acceso a la información, incluyendo las disposiciones del Decreto Legislativo Nº 1129 que restringen este derecho. Basándose en el Derecho internacional y en los principios de Derecho comparado esbozados anteriormente, se argumenta, a continuación, que la limitación al derecho de acceso a la información recogida en el artículo 12 del Decreto Nº 1129 es incompatible con el Derecho internacional. Tal y como se indica en el apartado 7 anterior, esta restricción: (1) no es necesaria en una sociedad democrática ni proporcionada, (2) vulnera el principio de máxima divulgación, (3) permite el mantenimiento del secretismo a perpetuidad, y (4) exime a la retención de la información en estas categorías de un control independiente.

A. La Legislación Peruana

52. La **Constitución** Política del Perú de 1993 garantiza el derecho de acceso a la información. De conformidad con el artículo 2(5): "Toda persona tiene derecho a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública." El artículo 2(5) establece excepciones limitadas "por razones de seguridad nacional".[105]

53. La **Ley de Transparencia y Acceso a la Información Pública** del Perú del año 2002 exige, con carácter general, que las restricciones previstas al derecho de acceso a la información sean casos excepcionales, que el acceso a la misma se niegue solamente cuando resulte necesario y

---

[101] *Véase, por ejemplo,* Enrique Pasquel, *Orgía a oscuras: Los secretos de la seguridad nacional*, El Comercio (Perú), 24 de octubre, 2013.
[102] Andrew Feinstein, *The shadow world: corruption in the arms trade*, New Internationalist Magazine, Issue 448, 1 diciembre 2011, disponible en http://newint.org/features/2011/12/01/corruption-in-the-arms-trade/.
[103] Principios de Tshwane, nota 4 anterior, Principio 10F.
[104] *Véase, por ejemplo,* Asamblea Parlamentaria del Consejo de Europa, Resolución 1507 (2006), Presuntas detenciones secretas y transferencias ilegales de detenidos entre los Estados que implican a Estados miembros del Consejo de Europa, en el numeral 19.5.
[105] Constitución Política, artículo 2(5). *Véase* Ley de Transparencia y Acceso a la Información Pública, Ley Nº 27806, de 3 de julio de 2002, artículo 1.

proporcionado, cuando venga establecido por la ley y de conformidad con los principios de una sociedad democrática. La ley reconoce que toda la información del Estado, ya sea "creada u obtenida" por éste, o "en [la] posesión o bajo [el] control" del Estado, "se presume pública" a menos que la información se halle legítimamente sujeta a "las excepciones expresamente previstas" en la ley.[106] La Ley se aplica a todas las "entidades de la Administración Pública", sin ningún tipo de limitación.[107]

54. La ley no prevé una justificación general para retener información pública ni la posibilidad de mantener el secretismo perpetuamente. De acuerdo con la ley, si el Estado trata de ocultar información al público "debe ser debidamente fundamentada en las excepciones del Artículo 15 de esta Ley, señalándose expresamente y por escrito las razones por las que se aplican esas excepciones y el plazo por el que se prolongará dicho impedimento".[108] Las excepciones deben ser "interpretadas de manera restrictiva por tratarse de una limitación a un derecho fundamental".[109] La ley exige que las decisiones de clasificación se revisen cada cinco años y que se revele la información si ésta ya no "pone en riesgo la seguridad de las personas, la integridad territorial y/o la subsistencia del sistema democrático".[110]

55. El artículo 15 de la Ley identifica las excepciones específicas al derecho a la información en relación a "información expresamente clasificada como secreta, que se sustente en razones de seguridad nacional". Para justificar la retención de información por razones de seguridad nacional, la autoridad pública debe demostrar que la información "tenga como base fundamental garantizar la seguridad de las personas y cuya revelación originaría riesgo para la integridad territorial y/o subsistencia del sistema democrático, así como respecto a las actividades de inteligencia y contrainteligencia del CNI dentro del marco que establece el Estado de Derecho en función de las situaciones expresamente contempladas en esta Ley". La disposición, además, establece un limitado número de subcategorías "comprendidas únicamente" en dicha excepción por motivos de seguridad nacional, a saber: "(1) información clasificada en el ámbito militar, tanto en el frente interno como externo: (a) … (2) información clasificada en el ámbito de inteligencia tanto en el frente externo como interno".[111]

56. La ley prohíbe expresamente la clasificación de la información "relacionada a la violación de los derechos humanos o de las Convenciones de Ginebra de 1949 realizada en cualquier circunstancia, por cualquier persona".[112] Existen disposiciones análogas en otras leyes sobre acceso a la información de otros países de la región.[113] Sin embargo, la disposición pertinente de la Ley TAPI del Perú se encuentra únicamente en la disposición que define la exención de la seguridad nacional. Los expertos en esta materia entienden que esto se debe a que la disposición fue incorporada a la ley de TAPI como consecuencia de razones históricas del Perú relacionadas con la excesiva invocación de la seguridad nacional para justificar el carácter secreto de la información sobre las violaciones de los derechos humanos.[114]

---

[106] *Ídem.*, artículo 3(1), 10.
[107] *Ídem.*, artículos 4, 8, 10.
[108] *Ídem.*, artículo 13.
[109] *Ídem.*, artículo 15.
[110] *Ídem.*, artículo 15.
[111] *Ídem.*
[112] *Ídem.*
[113] *Véase* notas 55-57 anterior.
[114] Comunicaciones, en el archivo. *Véase también* Edward Vargas Valderrama, *El derecho de acceso a la información pública en el Perú*, 9 de febrero de 2011, disponible en http://blogs.monografias.com/dextrum/2011/02/09/el-derecho-de-acceso-a-la-informacion-publica-en-el-peru/ ("No obstante, en el Perú se constata que subsiste una antigua «cultura del secretismo», que se manifiesta en algunas Instituciones del Estado. En respuesta a ello, y como resultado del trabajo conjunto del Estado y de la sociedad civil, surge la Ley de transparencia y acceso a la información pública.").

57. El 6 de diciembre de 2012, el Presidente Ollanta Humala promulgó el **Decreto Nº 1129**, con el objetivo declarado de "regular la naturaleza, finalidad, funciones y estructura del Sistema de Defensa Nacional".[115]El artículo 12 del Decreto 1129 refiere explícitamente al acceso a la información y exige que "toda la información" relacionada con la "seguridad y la defensa nacional" sea secreta. Dice así:

> "Acceso a la Información: Los acuerdos, actas, grabaciones, transcripciones y en general, toda información o documentación que se genere en el ámbito de los asuntos referidos a la Seguridad y Defensa Nacional, y aquellas que contienen las deliberaciones sostenidas en las sesiones del Consejo de Seguridad y Defensa Nacional, son de carácter secreto".

B. El excesivo secretismo dispuesto por el Decreto Nº 1129 no está justificado por razones de Seguridad Nacional

58. El artículo 12 del Decreto Nº 1129 efectivamente sirve como una limitación del alcance de la Ley TAIP, excluyendo absolutamente la información relativa a la seguridad y defensa nacional, sin necesidad de justificar cada caso de retención de la información por parte de la autoridad pública. Además, el Decreto Nº 1129 no establece ningún límite temporal para esta exclusión, ni ninguna consideración de los intereses públicos que pudieran requerir el levantamiento de la misma. El marco constitucional y legislativo del Perú garantiza el derecho del ciudadano al acceso a la información pública, admitiendo solo contadas excepciones por razones de seguridad nacional. El Decreto Nº 1129, al establecer el secretismo de forma amplia y absoluta sin estar sujeto a una supervisión significativa, adopta una medida extrema e incompatible con el Derecho internacional.

1) <u>El Decreto 1129 no es necesario ni proporcionado.</u>

59. Toda limitación al acceso a la información debe ser necesaria en una sociedad democrática y proporcional al interés protegido que la justifica, y debe interferir lo menos posible en el ejercicio de ese derecho. La exclusión de amplias categorías de información del ámbito de aplicación de la Ley no es necesaria ni proporcional. Puede disponerse de otras opciones, menos restrictivas, para proteger los mismos intereses, incluidos los mecanismos de protección alternativos ya incluidos en la Ley TAIP del Perú. La limitación absoluta al derecho de acceso a la información, tal y como se encuentra en el Decreto Nº 1129, infringe esta obligación de Derecho internacional puesto que no se hace un análisis casuístico y no se sopesa el interés público en cada una de las decisiones de no divulgar la información. La exclusión de grandes categorías de información del ámbito de aplicación del derecho a la información mina la responsabilidad democrática y la eficacia del derecho de acceso a la información.

60. Lo establecido en el Decreto Legislativo No. 1129 **se opone de manera directa al grupo de normas que protegen el acceso a la información pública**. Este grupo está compuesto por el artículo 2.5 de la Constitución y por la Ley de Transparencia y acceso a la información pública peruana. La norma cuestionada contraviene claramente la regulación de excepciones en materia de seguridad nacional establecida por la Ley de Transparencia y acceso a la información pública, así como el parámetro internacional en la materia, que ha sido expuesto a lo largo del informe.

61. La amplia exclusión de categorías enteras de información del ámbito del Ley TAIP **no es necesaria, puesto que la divulgación de la información en cuestión ya está protegida, cuando**

[115] El Decreto 1129 fue promulgado con arreglo a lo dispuesto en el artículo 104 de la Constitución, que permite al Congreso delegar en el Poder Ejecutivo funciones legislativas cuando la materia y el plazo de tiempo estén estrictamente definidos, y a la Ley 29915, que delegó en el Poder Ejecutivo facultades legislativas para, entre otras cosas, la "reforma del Sistema de Seguridad y Defensa Nacional." Ley n. º 29915, de 11 de septiembre de 2012, arts. 1, 2(3), 2(4). El preámbulo al Decreto 1129 hace hincapié en la obligación del Estado que "promueve el desarrollo del país y garantiza la seguridad de la Nación, así como la plena vigencia de los derechos fundamentales, el bienestar de la población y la consolidación del Estado democrático de derecho; lo que contribuye a la paz, el desarrollo integral y la justicia social". Decreto Legislativo Nº 1129, preámbulo.

procede, en virtud del sistema de excepciones existente. Si una opción menos restrictiva es suficiente para conseguir el objetivo, las restricciones adicionales no son necesarias. La protección frente a la divulgación por el sistema de excepciones es una restricción más limitada al derecho de acceso a la información de lo que sería la exclusión completa de categorías de información.

62. En las leyes sobre acceso a la información de otros países, la protección a los intereses relativos a la seguridad nacional, defensa, orden público y relaciones internacionales se maneja correctamente mediante excepciones muy restrictivas, en lugar de excluir categorías de información completas del ámbito de aplicación de la ley. Un examen de 50 leyes nacionales sobre el derecho de acceso a la información realizado por los autores de este informe, encontró que prácticamente todas estaban incluidas en el ámbito de la defensa y asuntos de seguridad nacional, e incluían excepciones explícitas relativas a la seguridad nacional para proteger el interés público en limitadas circunstancias en las que la autoridad pública puede justificar la retención.[116] La Ley Modelo Interamericana también prevé excepciones de seguridad nacional planteadas caso por caso, pero no prevé la no aplicación de la Ley TAIP a esta categoría de información.

63. En particular, en el Perú, estas exclusiones del ámbito de aplicación de la ley están protegidas por el sistema actual, normal y equilibrado, de excepciones desarrollado en el artículo 15. Bajo este sistema, la autoridad pública debe identificar el daño concreto para un interés protegido resultante de la divulgación de la información; el daño potencial al interés protegido que la divulgación pudiera causar debe evaluarse y ponderarse frente al interés público en la divulgación, y existen limitaciones temporales a la divulgación y un control independiente de la negativa a revelar información. Todo ello permite lograr un equilibrio adecuado y la protección de información relativa a la seguridad nacional cuando resulte realmente necesario, con sujeción a las garantías establecidas por el Derecho internacional. Ninguna de esas protecciones contra los abusos podrían aplicarse a las categorías de información excluidas en virtud de las disposiciones del Decreto Nº 1129. Tampoco se han aportado argumentos para justificar la mayor restricción, la que se afirma que no existe.

64. En virtud del derecho internacional, **las restricciones al derecho de acceso a la información no pueden ser absolutas ni categóricas, y requieren mecanismos de revisión y un análisis caso por caso** de lo adecuado de denegar la divulgación. El Estado está obligado a justificar la denegación del acceso a la información con motivos específicos, en los casos en los que se apliquen las excepciones. De este modo, las restricciones a la divulgación no serán arbitrarias.[117] La carga de la prueba para justificar cualquier negativa de acceso a la información "debe recaer en el órgano al cual se le solicitó la información."[118] Las excepciones también permiten una divulgación parcial, si procede, en lugar de la retención en bloque de toda la información, así como la imposición de límites temporales a la obligación de secreto (véase más adelante). La exclusión absoluta de la información no cumple estos requisitos. Dado que estas opciones, menos restrictivas, han demostrado ser adecuadas en muchas otras leyes y han sido respaldadas por los Estados de la OEA en la Ley Modelo Interamericana, el método mucho más restrictivo de clasificar categorías enteras de información como secreta y, por lo tanto, excluir todas estas de aplicación de la ley no es necesario.

65. Así mismo, una exclusión absoluta y categórica, por su propia definición, **no puede cumplir la prueba de proporcionalidad**. Esa exclusión no exige a la autoridad pública demostrar que la divulgación en cuestión provocaría daños a un objetivo legítimo, y no incluye la obligación de sopesar el posible daño al interés protegido contra el interés público que se ve menoscabado por la

[116] Este incluye 18 leyes de los países miembros de la OEA, así como leyes de África, Asia y Europa.
[117] *Claude Reyes v. Chile*, nota 7 anterior, numerales 58 y 77.
[118] Comité Jurídico Interamericano, Principios sobre el derecho de acceso a la información, nota 27 anterior, principio 7.

retención de la información. Solamente, mediante la revisión de la naturaleza y contenido de cada documento específico, pueden valorar las autoridades el daño que su divulgación podría provocar y los aspectos del interés público a los que serviría la divulgación, requisitos necesarios para que las restricciones al derecho sean proporcionadas.

66. Las clases de información cuya absoluta exclusión se permite —defensa y seguridad nacional, orden público y relaciones internacionales— cubren algunas de las decisiones fundamentales adoptadas por el Estado que son clave para la toma de decisiones democráticas. Existen justificaciones bien fundadas para la retención de información de estas clases con el objeto de proteger los intereses legítimos en circunstancias apropiadas. De hecho, la seguridad nacional constituye uno de los motivos públicos más significativo para no divulgar información.[119]

67. Sin embargo, también es cierto que el acceso a la información contribuye a la protección de los abusos, al permitir el escrutinio público de las medidas gubernamentales, incluidas las adoptadas en las áreas de defensa, seguridad nacional, orden público y relaciones internacionales, en las que las decisiones tienen generalmente gran interés público y pueden recibir una deferencia indebida. Estas clases de información incluyen, por ejemplo, las decisiones gubernamentales de participar en una guerra, responder a un discrepante democrático o privar a las personas de libertad.

68. Por tanto, debe existir una justificación sólida—y que pueda demostrarse individualmente—para no divulgar esa información, comparado con el interés público que sí justifica esa divulgación.[120] Las excepciones limitantes de ese derecho, como las contempladas en el artículo 15 de la Ley TAIP del Perú, requieren de un análisis caso por caso de si la restricción es procedente, así como de pruebas del daño sustantivo y del interés público para garantizar la ponderación obligatoria de daños y beneficios de la divulgación o no divulgación.[121] Este sistema, que ha demostrado ser adecuado en las leyes de acceso a la información de otros países y que también se encuentra en la Ley Modelo Interamericana y la Ley TAIP del Perú, garantiza que toda restricción a la divulgación sea proporcional. El artículo 12 del Decreto Nº 1129 es excesivo y no satisface el requisito de proporcionalidad requerido por el Derecho internacional.

69. Además, la exclusión de estas clases de información del ámbito de aplicación de la ley no sólo no es necesaria en una sociedad democrática, sino que **mina el propio concepto de la responsabilidad democrática**. Como la Corte Constitucional de Colombia ha afirmado:

> "[L]a garantía más importante del adecuado funcionamiento del régimen constitucional está en la plena publicidad y transparencia de la gestión pública. Las decisiones o actuaciones de los servidores públicos, que no se quieren mostrar, son usualmente aquellas que no se pueden justificar. Y el uso secreto e injustificado del poder del Estado repugna al Estado de derecho y al adecuado funcionamiento de una sociedad democrática."[122]

70. En América, en particular, la importancia de la divulgación pública en esas áreas está bien reconocida, en vista de las graves violaciones de los derechos humanos que se han cometido en secreto, con la seguridad nacional como pretexto durante mucho tiempo. Las leyes de secreto de Estado, que existieron durante mucho tiempo, sancionaban la revelación de información que pudiera dañar las actividades económicas o militares de un Estado, como un "delito contra la patria," "utilizando la 'seguridad nacional' como una gran pantalla para ocultar información del saber público."[123] La Comisión Interamericana de Derechos Humanos, con los Comentarios a la Ley Modelo Interamericana, incluso señala específicamente al Perú por afirmar indebidamente la

---

[119] *Véanse* los párrs. 22 y 40, anterior.
[120] *Véase, por ejemplo, Claude Reyes v. Chile*, nota 7 anterior, numerales 77, 86-87 y 95.
[121] *Ídem*, numerales 77 y 95 (que requieren un análisis caso por caso de todas las restricciones del acceso a la información).
[122] Sentencia C-491/07, Corte Constitucional Colombiana, 27 de junio de 2007, pág. 1.
[123] Comentarios a la Ley Modelo Interamericana, nota 23 anterior, pág. 5.

necesidad de secreto por seguridad nacional para encubrir abusos: "las disposiciones relativas al secreto de Estado fueron derogadas de los códigos penales de México y Perú en el siglo XX, cuando principalmente se utilizaban para cubrir actos discrecionales y la mala gestión del gobierno."[124]

71. La clasificación de grandes categorías de información como secreta y su exclusión categórica del ámbito del derecho del público de acceso a la información, también **limitan la eficacia del propio acceso a la información, y minan los objetivos del derecho de acceso a la información** de garantizar el pleno ejercicio de la libertad de expresión, facilitar la información pública y fomentar la confianza del público en el funcionamiento del gobierno, promover la responsabilidad democrática y el buen gobierno, y reducir la corrupción y los abusos gubernamentales.

2) El Decreto Nº 1129 vulnera el principio de máxima divulgación

72. Una amplia exclusión del derecho a la información con respecto a múltiples categorías de información no cumple el requisito de que las autoridades públicas deben "regirse por el principio de máxima divulgación".[125] A pesar de que la Ley TAIP incorpora el principio de máxima divulgación, la exclusión categórica de amplias clases de información del ámbito de aplicación de la Ley TAIP a través del Decreto Nº 1129 invalida totalmente ese principio. Para estas clases de información, se presume el secreto en lugar de la divulgación y no existe ningún mecanismo en la ley para desvirtuar tal presunción.

3) El Decreto 1129 vulnera la prohibición de secretismo perpetuo.

73. Como se señaló anteriormente[126], el secreto perpetuo es inadmisible e incompatible con las obligaciones de necesidad y proporcionalidad. La Ley TAIP del Perú reconoce la importancia del principio que señala que las restricciones al derecho deben ser limitadas en el tiempo, junto con el requisito de revisar la clasificación cada cinco años y con el mandato de revelar la información si las condiciones para la clasificación ya no se cumplen. Sin embargo, la clasificación automática de amplias categorías de información como secretas y su exclusión efectiva del ámbito de aplicación de la ley a través del artículo 12 del Decreto Nº 1129, elimina el requisito de que estas categorías deben ser reveladas después de un cierto período de tiempo y permite —de hecho, podría decirse, incluso, que exige— el secreto perpetuo. Con arreglo a lo dispuesto en el Decreto Nº 1129, ello resulta cierto también para las informaciones relativas a los abusos cometidos en el pasado por regímenes autoritarios, así como para la información actual de las fuerzas de seguridad y de defensa nacional, e incluso, como se señaló anteriormente (véanse los párrs. 31-33), en el caso de las primeras, no existe un interés público en retener esta información.[127]

4) El Decreto Nº 1129 pretende eliminar el control independiente del secreto respecto de la información de seguridad y defensa nacional.

74. Toda restricción del derecho de acceso a la información debe también estar sujeta a un mecanismo de revisión independiente.[128] Sin embargo, clasificar categorías enteras de información como secreta y excluirlas del ámbito de la Ley TAIP impide toda revisión independiente de una decisión de no divulgar cierta información. Las clases de información excluidas del ámbito de aplicación de la Ley TAIP no estarían sujetas a los mecanismos contemplados por la Ley TAIP, y el acceso a éstas quedaría por tanto enteramente a discreción de las autoridades públicas.

---

[124] *Ídem.*, p. 4.
[125] *Véanse* los párrs. 17, 19, anterior.
[126] *Véase* párr. 30, anterior.
[127] Principios de Tshwane, nota 4 anterior, Principios 16(a), 16 (c). *Véanse también* los párrs. 22, 24-29 anterior.
[128] *Véanse* los párrs. 38, 43 anterior.

75. Diferentes mecanismos podrían ser adecuados y eficaces para garantizar el cumplimiento y el control del derecho de acceso a la información, tales como la intervención de autoridades independientes seguido de una revisión exhaustiva por parte de los tribunales o directamente mediante control judicial.[129] Independientemente de cómo se implemente dicho control, la ley peruana debería, en virtud de las obligaciones jurídicas contraídas internacionalmente, proporcionar garantías adecuadas frente a posibles abusos, incluyendo la revisión judicial inmediata, completa, accesible y eficaz de la validez de cualquier restricción al derecho de acceso a la información. Parece que el Decreto Nº 1129 establece que las negativas a acceder a información relacionada con la seguridad y la defensa nacional no serían revisables en cuanto al fondo, ya sea de forma inmediata o de cualquier otra forma.

IV. CONCLUSIÓN

76. Por las razones expresadas anteriormente, el artículo 12 del Decreto Nº 1129 es incompatible con el Derecho internacional. Al establecer una amplia y categórica exclusión del derecho de acceso público a determinadas clases de información, el Decreto Nº 1129 ignora el requisito que las limitaciones al mismo deben ser necesarias y proporcionadas a un objetivo legítimo, y socava la obligación de máxima divulgación de la información. Asimismo, el Decreto Nº 1129 abre la puerta a la posibilidad de que se mantengan secretos perpetuamente y deja la decisión de revelar grandes clases de información enteramente en manos de la autoridad pública, sin ningún control independiente.

77. Las exclusiones identificadas en el decreto están debidamente identificadas en la Ley TAIP del Perú como situaciones en las que se pueden establecer excepciones a la comunicación caso por caso y, por tanto, ya están protegidas por el marco legal establecido. No hay fundamento para clasificarlas categóricamente como secretas y excluirlas por completo de una revisión, ya sea total o parcial, según el caso, o de una posible revelación.

James A. Goldston, Director Ejecutivo
Emilou MacLean, Responsable de Asuntos Jurídicos
Open Society Justice Initiative
224 West 57th Street
New York, New York 10019
Estados Unidos

5 de noviembre de 2013

[129] *Véase* a Los Comentarios a la Ley Modelo Interamericana, nota 23 anterior, Capítulo 3 sobre las ventajas y desventajas, así como sobre su estructura y función, de los comisarios de información con mandato para emitir tanto órdenes vinculantes como recomendaciones, y sobre la revisión judicial.

ANEXO

PRINCIPIOS GLOBALES SOBRE
SEGURIDAD NACIONAL Y EL DERECHO A LA INFORMACIÓN

("LOS PRINCIPIOS TSHWANE")

concluidos in Tshwane, Sudáfrica
emitidos el 12 de junio de 2013

Introducción

Estos Principios han sido formulados para orientar a quienes intervienen en la redacción, revisión o implementación de leyes o disposiciones relativas a la potestad del Estado para retener información por motivos de seguridad nacional o sancionar su divulgación.

Están basados en normas, estándares y buenas prácticas del derecho nacional e internacional (incluso regional) y la doctrina especializada.

Abordan aspectos específicos de seguridad nacional, y no todos los supuestos en los cuales se podría retener información. Todos los demás motivos de interés público para limitar su acceso deberían, como mínimo, cumplir estos estándares.

Estos Principios fueron redactados por 22 organizaciones y centros académicos (que se enumeran en el Anexo) con el asesoramiento de más de 500 expertos procedentes de más de 70 países en 14 reuniones celebradas por todo el mundo y moderadas por la Iniciativa Pro-Justicia de la Sociedad Abierta, y con la ayuda de los cuatro relatores internacionales para la promoción y protección de la libertad de expresión y/o la libertad de prensa y el relator especial sobre la promoción y protección de los derechos humanos y libertades fundamentales en la lucha contra el terrorismo:

- el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión,
- el Relator Especial de las Naciones Unidas (ONU) sobre la promoción y protección de los derechos humanos y libertades fundamentales en la lucha contra el terrorismo,
- la Relatora Especial de la Comisión Africana de Derechos Humanos y de los Pueblos sobre Libertad de Expresión y Acceso a la Información (ACHPR),
- la Relatora Especial de la Organización de los Estados Americanos (OEA) para la Libertad de Expresión y
- La Representante de la Organización para la Seguridad y la Cooperación en Europa (OSCE) para la libertad de los medios.

ANTECEDENTES Y EXPOSICIÓN DE MOTIVOS

La seguridad nacional y el derecho del público a la información a menudo se consideran objetivos contrapuestos. Si bien a veces puede haber cierto grado de tensión entre el interés de un gobierno por preservar el carácter reservado de cierta información por razones de seguridad

nacional y el derecho de la población a acceder a información en poder de autoridades públicas, un examen exhaustivo del pasado reciente indica que los intereses legítimos de seguridad nacional, en la práctica, se ven favorecidos cuando el público está bien informado sobre las actividades del Estado, incluidas aquellas llevadas a cabo para resguardar la seguridad nacional.

El acceso a la información, al facilitar el escrutinio público de los actos del Estado, no sólo previene abusos por parte de funcionarios públicos, sino que además permite que la población intervenga en la definición de las políticas del Estado y, por ende, constituye un elemento clave para la preservación efectiva de la seguridad nacional, la participación democrática y la formulación de políticas sólidas. Para proteger el pleno goce de los derechos humanos, en ciertas circunstancias, podría ser necesario mantener información en secreto para salvaguardar intereses legítimos de la seguridad nacional.

Encontrar un punto de equilibrio adecuado se torna aún más difícil debido a que, en muchos países, la justicia actúa con menor grado de independencia y mayor deferencia frente a los reclamos del gobierno cuando este apela a argumentos de seguridad nacional. Esta deferencia se ve reforzada por disposiciones de las leyes sobre seguridad de numerosos países que prevén excepciones al derecho a la información y a las normas procesales comunes sobre prueba y derechos de los acusados ante la mínima demostración, o mera afirmación, por parte del gobierno de que existe un riesgo para la seguridad nacional. Cuando un gobierno apela excesivamente a argumentos de seguridad nacional, esto puede socavar las principales garantías institucionales contra el abuso gubernamental: la independencia de la justicia, el estado de derecho, el control legislativo, la libertad de los medios de comunicación y el gobierno participativo.

Los presentes Principios se formulan en respuesta a los obstáculos de larga data mencionados precedentemente y a que, en los últimos años, una cantidad significativa de Estados de todo el mundo se han propuesto adoptar o reformar regímenes de clasificación de información y leyes relacionadas. A su vez, esta tendencia ha sido provocada por varios acontecimientos. El más significativo ha sido, quizás, la rápida adopción de leyes sobre acceso a la información desde la caída del Muro de Berlín, lo que ha tenido como consecuencia, desde la fecha de vigencia de dichos Principios, que más de 5.200 millones de personas en 95 países del mundo pueden disfrutar del acceso a la información—al menos por ley, no siempre en la práctica. La población de estos países se enfrenta —a menudo por primera vez— con la cuestión de si la información ha de mantenerse en secreto, y bajo qué circunstancias. Otros acontecimientos que han contribuido a un aumento de la legislación propuesta en materia de secretos están relacionadas con las respuestas gubernamentales al terrorismo o la amenaza terrorista, además de con un interés por proteger los secretos por ley en el contexto de las transiciones democráticas.

PRINCIPIOS GLOBALES SOBRE
SEGURIDAD NACIONAL Y EL DERECHO A LA INFORMACIÓN

("LOS PRINCIPIOS TSHWANE")

concluidos in Tshwane, Sudáfrica
emitidos el 12 de junio de 2013

Preámbulo

Las organizaciones y personas que intervinieron en la redacción de los presentes Principios:

Recordando que el acceso a la información retenida por el Estado es un derecho público y que, por tanto, se trata de un derecho que ha de ser protegido por leyes formuladas con precisión y que contemplen excepciones claramente delimitadas, y de tutelar este derecho por medio de tribunales independientes, organismos de control parlamentario y otras instituciones independientes;

Reconociendo que los estados tienen el derecho legítimo de mantener la confidencialidad de cierta información, incluso por razones de seguridad nacional, y destacando que encontrar un punto de equilibrio adecuado entre la divulgación y la retención de información resulta indispensable para una sociedad democrática y su seguridad, progreso, desarrollo y bienestar, así como para el pleno goce de los derechos humanos y las libertades fundamentales;

Ratificando que resulta imperativo, para que las personas puedan controlar la conducta de su gobierno y participar plenamente en una sociedad democrática, que tengan acceso a información en poder de autoridades públicas, incluida información relativa a seguridad nacional;

Observando que estos Principios están basados en normas y estándares internacionales y regionales sobre el derecho público de acceso a la información en poder de autoridades estatales y otros derechos humanos, la evolución de las prácticas de los Estados (según se refleja, entre otras medidas, en las sentencias de los tribunales nacionales e internacionales), los principios generales del derecho reconocidos por la comunidad de naciones, y la doctrina de los expertos;

Teniendo en cuenta disposiciones relevantes de la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Carta Africana sobre los Derechos Humanos y de los Pueblos, la Convención Americana sobre Derechos Humanos, el Convenio Europeo para la Protección de los Derechos Humanos y el Convenio del Consejo de Europa sobre Acceso a los Documentos Públicos;

Teniendo en cuenta también la Declaración de Principios sobre Libertad de Expresión de la Comisión Inter-Americana de Derechos Humanos; la ley Modelo Interamericana sobre Acceso a la Información Pública; la Declaración de Principios sobre Libertad de Expresión en África, y la ley Modelo sobre Acceso a la Información Pública en África;

Recordando la Declaración Conjunta de 2004 del Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión, la Representante de la OSCE para la Libertad de los Medios de Comunicación y el Relator Especial de la OEA para la Libertad de Expresión; las Declaraciones Conjuntas emitidas en 2006, 2008, 2009 y 2010 por estos tres expertos y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos; la Declaración Conjunta sobre WikiLeaks de los Relatores Especiales de la ONU y la Comisión Interamericana, de diciembre de 2010; y el Informe sobre Medidas contra el Terrorismo y Derechos Humanos, adoptado por la Comisión de Venecia en 2010;

Recordando asimismo los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información adoptados por un grupo de expertos convocados por la organización Artículo 19 en 1995 y los Principios sobre Control y Rendición de Cuentas de los Servicios de Seguridad en una Democracia Constitucional elaborados en 1997 por el Centro de Estudios sobre Seguridad Nacional (Centre for National Security Studies, CNSS) y la organización polaca Helsinki Foundation for Human Rights;

Teniendo en cuenta que existen principios internacionales — como los incluidos en la Ley Modelo sobre Acceso a la Información Pública en África, los Principios de la ONU sobre Empresas y Derechos Humanos (Ruggie Principles), el Tratado de Comercio de Armas, las Líneas Directrices de la OCDE para Empresas Multinacionales y el Documento de Montreal sobre las obligaciones legales y las buenas prácticas de los Estados en relación con las operaciones de empresas militares privadas y empresas de seguridad durante un conflicto armado —que reconocen la importancia de acceder a información sobre, o en relación con, empresas en ciertas circunstancias; y que algunos abordan específicamente la necesidad de que las empresas

militares privadas y las empresas de seguridad trabajen dentro del sector de la seguridad nacional para hacer pública ciertas informaciones;

Observando que estos Principios no contemplan normas sustantivas sobre recopilación de datos por los servicios de inteligencia, gestión de información personal o transmisión de datos, los cuales son adecuadamente abordados en las "buenas prácticas relativas a marcos jurídicos e institucionales para los servicios de inteligencia y su supervisión", emitidas en 2010 por Martin Scheinin, el entonces Relator Especial de la ONU sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo a petición del Consejo de los Derechos Humanos de las Naciones Unidas.

Reconociendo la importancia del intercambio de información de inteligencia entre Estados, tal como se insta en la Resolución 1373 del Consejo de Seguridad de la ONU;

Reconociendo asimismo que los obstáculos al control público e independiente interpuestos en nombre de la seguridad nacional agravan el riesgo de que se produzcan comportamientos ilícitos, corruptos y fraudulentos y de que tales actos no sean descubiertos, y que con frecuencia se cometen violaciones del derecho a la privacidad y otros derechos individuales invocando indebidamente el argumento de la confidencialidad de datos por razones de seguridad nacional;

Preocupados por los costos que supone para la seguridad nacional la clasificación excesiva de información como reservada, incluidos los obstáculos a la transmisión de información entre organismos gubernamentales y aliados, la imposibilidad de resguardar información confidencial legítima y de identificar datos importantes entre el gran volumen de información, la superposición de la información recabada por distintos organismos, y la asignación excesiva de responsabilidades a directores de seguridad;

Destacando que los Principios se centran en el derecho del *público* a la información, y que abordan los derechos a la información de personas detenidas, víctimas de violaciones de derechos humanos y otras personas con derechos especiales sobre acceso a información únicamente en la medida en que tales derechos se vinculen directamente con el derecho público a la información y la justicia participativa;

Reconociendo que cierta información que no debería ser clasificada como confidencial por motivos de seguridad nacional podría igualmente ser retenida por otras razones reconocidas por el derecho internacional, como las relaciones internacionales, la imparcialidad de los procedimientos judiciales, el derecho de las partes litigantes y la privacidad personal, tomando en cuenta siempre el principio según el cual no podrá retenerse información cuando el interés público en acceder a ella sea mayor al interés público en mantener su confidencialidad;

Manifestando nuestra intención de ofrecer orientación práctica a gobiernos, organismos legislativos y regulatorios, autoridades públicas, legisladores, tribunales, otros organismos de supervisión y la sociedad civil con respecto a algunos de los desafíos más importantes que plantea la convergencia de la seguridad nacional con el derecho a información en esta materia, especialmente aquellos vinculados con el respeto de los derechos humanos y la rendición de cuentas democrática;

Esforzándonos por formular Principios de aplicación y valor universal;

Reconociendo que los Estados enfrentan múltiples desafíos al procurar encontrar un equilibrio entre el interés público en la divulgación y la necesidad de la confidencialidad para proteger intereses legítimos de la seguridad nacional, y que toda vez que estos Principios son universales, su puesta en práctica debería tomar en cuenta las distintas realidades en el ámbito local, como la diversidad de sistemas jurídicos;

Recomiendan que los órganos pertinentes a nivel nacional, regional e internacional adopten medidas para difundir y debatir estos Principios, y los avalen, adopten o implementen en la mayor medida posible, a fin de contribuir progresivamente al pleno goce del derecho a la información conforme se establece en el Principio 1:

Definiciones

En estos Principios, y a menos que el contexto requiera algo distinto:

"**Compañías dentro del sector de la seguridad**" es una persona jurídica que lleva a cabo o ha llevado a cabo negocios en el sector de la seguridad nacional, y solamente en tal calidad; ya sea como proveedor de servicios, instalaciones, personal o productos incluyendo, aunque sin limitarse a, armamento, equipos e inteligencia. Esto incluye empresas militares y de seguridad privada (PMSCs). No incluye a personas jurídicas organizadas como organizaciones sin ánimo de lucro o no gubernamentales.

"Independiente" significa la independencia institucional, financiera y operativa respecto de la influencia, la orientación y el control del poder ejecutivo, incluidas todas las autoridades del sector de seguridad.

"Información" significa cualquier material, ya sea original o una copia, independientemente de sus características físicas y otro material tangible o intangible, con independencia de la forma que adopte o el medio por el cual se transmita. Incluye, sin carácter restrictivo, registros, correspondencia, hechos, opinión, consejos, memorándums, datos, estadísticas, libros, ilustraciones, planos, mapas, diagramas, fotografías, grabaciones en audio o vídeo, documentos, mensajes de correo electrónico, cuadernos de bitácora, muestras, modelos e información en formato electrónico.

"Información de interés público" se refiere a información que resulta relevante o beneficiosa para el público, y no simplemente de interés individual, y cuya divulgación es "en interés del público", por ejemplo, debido a que resulta útil para que el público comprenda las actividades que lleva a cabo el gobierno.

"Interés legítimo de seguridad nacional" hace referencia a un interés cuyo verdadero objeto y principal efecto sea proteger la seguridad nacional, en consonancia con el derecho interno e internacional. En el Principio 9 se establecen categorías de información cuya confidencialidad podría ser necesaria para proteger un interés legítimo de seguridad nacional. Un interés de seguridad nacional no será legítimo cuando su objetivo real o su principal efecto sea resguardar

un interés que no esté vinculado con la seguridad nacional, como evitar que se ridiculice o señale a gobiernos o funcionarios por irregularidades; ocultar información sobre violaciones de derechos humanos u otras transgresiones de la ley o el funcionamiento de las instituciones públicas; fortalecer o perpetuar un determinado interés, ideología o partido político; o reprimir protestas legítimas.

"**Seguridad nacional**" no se define en estos Principios. El Principio 2 recomienda que la "seguridad nacional" se defina con precisión en el derecho nacional de forma coherente con las necesidades de una sociedad democrática.

"Autoridades públicas" incluye a todos los organismos de los poderes ejecutivo, legislativo y judicial en todos los niveles del gobierno, las autoridades creadas por la constitución y las leyes, incluyendo autoridades del sector de la seguridad, y los organismos que no pertenecen al Estado pero son controlados por este o son de propiedad del Estado, o actúan como agentes del gobierno. Las "autoridades públicas" también incluyen a entidades privadas o de otra naturaleza que desempeñan funciones o servicios públicos, u operan con fondos o beneficios públicos significativos, pero únicamente en lo que respecta a la ejecución de tales funciones, prestación de servicios, o uso de fondos o beneficios públicos.

"Personal público" o "**funcionario público**" hace referencia a empleados públicos actuales y anteriores, militares, contratistas y subcontratistas de autoridades públicas, incluido el sector de seguridad. Con " personal público" o "funcionario público" también se hace referencia a personas contratadas por órganos no estatales que pertenecen o están bajo el control del gobierno o que sirven como agentes del gobierno; y empleados de entidades privadas u otras entidades que realizan funciones públicas o que prestan servicios u operan con fondos o ayudas públicos substanciales, pero sólo en lo que concierne a la realización de dichas funciones, o la prestación de esos servicios, o el uso de fondos o ayudas públicas.

"**Sanción**" se refiere a cualquier forma de penalización o perjuicio, incluidas las medidas criminales, civiles o administrativas. En forma de verbo, **"sancionar"** significa poner en práctica dicha forma de penalización o perjuicio.

"Sector de seguridad" comprende: (i) agentes de seguridad, incluyendo pero sin limitarse a las fuerzas armadas, la policía y otros organismos encargados de vigilar el cumplimiento de la ley, fuerzas paramilitares, y servicios de inteligencia y seguridad (tanto militares como civiles); y (ii) todos los órganos ejecutivos, departamentos y ministerios responsables de la coordinación, el control y la vigilancia de los agentes de seguridad.

Parte I: Principios generales

Principio 1: Derecho a la información

(a) Todas las personas tienen derecho a buscar, recibir, usar y transmitir información que esté en poder de autoridades públicas u otros órganos que actúen en su representación, o cuyo acceso haya sido reconocido legalmente a las autoridades públicas.

(b) Los principios internacionales también reconocen que las empresas del sector nacional de la seguridad, incluidas las empresas militares privadas y las empresas de seguridad privada, tienen la responsabilidad de divulgar información con respecto a situaciones, actividades o conductas que puedan tener un impacto en el ejercicio de los derechos humanos.

(c) Aquellos que tengan la obligación de divulgar información, de acuerdo con los Principios 1(a) y 1(b), deben proporcionar la información que se solicite y tienen una obligación positiva de publicar información de interés público, salvo las pocas excepciones previstas en la legislación que sean necesarias para prevenir perjuicios concretos e identificables a intereses legítimos, incluida la seguridad nacional.

(d) Sólo las autoridades públicas cuyas responsabilidades específicas incluyan la protección de la seguridad nacional, podrán aseverar la seguridad nacional como fundamento para la retener información.

(e) Cualquier afirmación de seguridad nacional hecha por una empresa para justificar la retención de información ha de ser explícitamente autorizada o confirmada por una autoridad pública cuyas responsabilidades incluyan la protección de la seguridad nacional.

Nota: El gobierno, y sólo el gobierno, es responsable, en última instancia, de la seguridad nacional, y por lo tanto tan sólo el gobierno podrá aseverar que cierta información no sea publicada si pudiere redundar en perjuicio de la seguridad nacional.

(f) Las autoridades públicas también tienen la obligación explícita de publicar, de forma proactiva, cierta información de interés público.

Principio 2: Aplicación de los Principios

(a) Estos Principios se aplican al ejercicio del derecho de acceso a información tal y cómo se identifica en el Principio 1, cuando el gobierno asevera o confirma que la divulgación de dicha información podría redundar en perjuicio de la seguridad nacional.

(b) Dado que la seguridad nacional es uno de los argumentos públicos de mayor preponderancia para restringir la información, cuando las autoridades públicas reivindican otros argumentos públicos para limitar su acceso —incluidos motivos de defensa, inteligencia, relaciones internacionales, orden público, salud y seguridad pública, aplicación de la ley, disposición futura de asesoramiento libre y abierto, formulación de políticas efectivas e intereses económicos del Estado— estos deberán, como mínimo, cumplir los estándares relativos a la imposición de restricciones en el derecho del acceso a la información establecidos en estos Principios como pertinentes.

Se considera buena práctica definir la seguridad nacional, siempre que se use para limitar el derecho a la información, de manera precisa en el ordenamiento jurídico de un país conforme *a* una sociedad democrática.

Principio 3: Requisitos para restringir el derecho a la información por razones de seguridad nacional

No podrán aplicarse restricciones al derecho a la información invocando razones de seguridad nacional a menos que el gobierno demuestre que: (1) la restricción (a) está establecida en una ley y (b) resulta necesaria en una sociedad democrática (c) para proteger un interés legítimo de seguridad nacional; y (2) la ley establece garantías adecuadas contra la posibilidad de abuso, incluido el escrutinio oportuno, pleno, accesible y efectivo de la validez de las restricciones por una autoridad de supervisión independiente y su revisión exhaustiva por la justicia.

(a) *Establecida en una ley*. La ley debe ser accesible, inequívoca e interpretada en forma acotada y precisa para permitir que las personas comprendan qué información puede ser retenida, cuál debería ser divulgada y qué actos relativos a la información pueden ser objeto de sanción.

(b) *Necesaria en una sociedad democrática*.

(i) La divulgación de la información debe representar un riesgo real e identificable de perjuicio significativo para un interés legítimo de seguridad nacional.
(ii) El riesgo de perjuicio que supondría la divulgación debe superar al interés público general en que se difunda la información.
(iii) La limitación debe adecuarse al principio de proporcionalidad y representar el medio menos restrictivo disponible para evitar el perjuicio.
(iv) La restricción no debe atentar contra la esencia misma del derecho a la información.

(c) *Protección de un interés legítimo de seguridad nacional*. Las escasas categorías de información que pueden retenerse en base a argumentos relativos a la seguridad nacional deberían establecerse claramente en la ley.

Notas: ver la definición de "interés legítimo de la seguridad nacional" en la sección de Definiciones. El Principio 3 (b) es imprescindible si la seguridad nacional no se define claramente en la legislación tal y cómo se recomienda en el Principio 2.

"Interés público" no se define en estos Principios. En el Principio 10 se incluye una lista de categorías especialmente altas de interés público que deberían publicarse de forma proactiva y que nunca deberían retenerse. En el Principio 37 se incluye una lista de categorías de infracciones de alto interés para el público y que los funcionarios públicos deberían y podrían publicar sin miedo a las represalias.

Al ponderar el riesgo de perjuicio y el interés público en la divulgación para intentar buscar un equilibrio, debería considerarse la posibilidad de mitigar los perjuicios causados por la difusión, incluso a través de medios que requieran una erogación razonable de fondos. A continuación se incluye una lista enunciativa de factores que deben ser tenidos en cuenta al determinar si el interés público en la divulgación supera el riesgo de perjuicio:

- *factores que favorecen la divulgación: es razonablemente esperable que la divulgación (a) fomente el debate participativo de asuntos públicos, (b) incremente la rendición de cuentas por parte del gobierno, (c) contribuya al debate positivo e informado sobre cuestiones*

importantes o asuntos de interés relevante, (d) promueva el control efectivo del gasto público, (e) permita revelar los motivos de una decisión gubernamental, (f) contribuya a la protección del medioambiente, (g) exponga amenazas al medioambiente o la salud o seguridad pública, o (h) exponga violaciones de derechos humanos o del derecho internacional humanitario, o contribuya a que estas sean juzgadas;

- *factores que favorecen que no se divulgue información: la divulgación podría causar un riesgo de perjuicio real e identificable para un interés legítimo de seguridad nacional;*

- *factores que son irrelevantes: es razonablemente esperable que la divulgación (a) ridiculice al gobierno o a un funcionario, o menoscabe la confianza en ellos; o (b) debilite a una ideología o partido político.*

El hecho de que la divulgación pueda causar perjuicio a la economía de un país tendría relevancia a efectos de determinar si resulta conveniente retener información por este motivo, pero no por razones de seguridad nacional.

Principio 4: Corresponde a la autoridad pública establecer la legitimidad de las restricciones

(a) Corresponde a la autoridad pública que pretenda que no se divulgue determinada información demostrar la legitimidad de cualquier restricción que se aplique.

(b) El derecho a información debería interpretarse y aplicarse en sentido amplio, mientras que la interpretación de las restricciones debería ser acotada.

(c) Al demostrar esta legitimidad, no bastará con que la autoridad pública simplemente afirme que existe un riesgo de perjuicio, sino que debe proporcionar razones sustanciales que respalden sus afirmaciones.

Nota: Cualquier persona que procure acceder a la información debería tener una oportunidad genuina de impugnar el fundamento de la evaluación del riesgo ante autoridades administrativas y judiciales, de acuerdo con los Principios 26 y 27.

(d) En ningún caso se considerará un argumento concluyente la mera afirmación de que la divulgación causaría un riesgo para la seguridad nacional, por ejemplo, mediante la emisión de un certificado en ese sentido por un ministro u otro funcionario.

Principio 5: No se aplican excepciones para autoridades públicas

(a) Ninguna autoridad pública estará exenta de los requisitos sobre divulgación, incluido el poder judicial, la legislatura, instituciones de supervisión, servicios de inteligencia, fuerzas armadas, policía, otros cuerpos de seguridad, los jefes de Estado y de gobierno y las dependencias que integren los anteriores.

(b) No se podrá retener información por motivos relativos a la seguridad nacional simplemente con el argumento de que fue generada por, o transmitida a un Estado extranjero o un organismo intergubernamental, autoridad pública o unidad dentro del ámbito de una autoridad.

Nota: Ver el Principio 9(a)(v) relativo a la información transmitida por un Estado extranjero u organismo intergubernamental.

Principio 6: Acceso a información por parte de organismos de supervisión

Todos los organismos de supervisión/defensa del pueblo/apelación, incluidos los tribunales, deben tener acceso a todo tipo de información —incluso la información sobre seguridad nacional y con independencia de su nivel de confidencialidad— que resulte relevante para el desempeño de sus funciones.

Nota: Este Principio se detalla en el Principio 32. No trata la divulgación pública por parte de los organismos de supervisión. Los organismos de supervisión deberían mantener la confidencialidad de toda la información que haya sido legítimamente clasificada de acuerdo con estos Principios tal y cómo se establece en el Principio 35.

Principio 7: Recursos

Los Estados deben destinar recursos suficientes y adoptar otras medidas necesarias, como emitir reglamentaciones y gestionar los archivos de forma adecuada, para asegurar que estos Principios se cumplan en la práctica.

Principio 8: Estados de emergencia

En una situación de emergencia pública que suponga una amenaza para la vida de la población de un país y cuya existencia haya sido reconocida en forma oficial y legítima conforme al derecho nacional e internacional, un Estado podrá desentenderse de sus obligaciones relativas al respeto del derecho a buscar, recibir y difundir información, únicamente en la medida en que resulte indispensable por las exigencias de la situación y solamente cuando dicha renuncia sea congruente con las demás obligaciones que corresponden al Estado de conformidad con el derecho internacional, y no implique ningún tipo de discriminación.

Nota: Ciertos aspectos del derecho a buscar, recibir y difundir información e ideas son tan fundamentales para el disfrute de los derechos no derogables que siempre habrían de ser plenamente respetados incluso en períodos de emergencia pública. Como ejemplo no exhaustivo, mucha o la totalidad de la información contenida en el Principio 10 es de este carácter.

Parte II: Información que puede ser retenida por razones de seguridad nacional e información que debería ser divulgada

Principio 9: Información que puede ser retenida en forma legítima

(a) Las autoridades públicas podrán restringir el derecho del público de acceder a información cuando existan razones de seguridad nacional que lo ameriten, pero únicamente cuando tales restricciones cumplan todas las demás disposiciones establecidas en estos Principios, la información sea retenida por parte de una autoridad pública y la información esté comprendida en una de las siguientes categorías:

(i) Información sobre operativos de defensa en curso y cuestiones sobre capacidad durante el período en que la información resulte de utilidad operativa.

Nota: Debe entenderse que la frase "durante el período en que la información resulte de utilidad operativa" exige divulgar la información una vez que esta ya no suponga revelar datos que podrían ser aprovechados por enemigos para conocer la capacidad de reacción del Estado, sus competencias, sus planes, etc.

(ii) Información sobre la producción, competencia, o uso de los sistemas de armamentos y otros sistemas militares incluidos los sistemas de comunicaciones.

Nota: Dicha información incluye datos e inventos tecnológicos sobre armamento, su producción, competencia o uso; e información sobre su producción, competencia o uso. La información sobre partidas presupuestarias relativas a armamento y otros sistemas militares deberían divulgarse al público. Ver los Principios 10C(3) y 10F. El que los Estados mantengan y publican una lista de control de armamento supone una buena práctica alentada por el Tratado sobre el Comercio de Armas en lo que concierne a armas convencionales. La publicación de información relativa a armas, equipos y números de tropas también es una buena práctica.

(iii) Información sobre medidas específicas destinadas a resguardar el territorio del Estado, infraestructura crítica o instituciones nacionales fundamentales (*institutions essentielles*) contra amenazas, uso de la fuerza o sabotajes, y su efectividad depende de su confidencialidad;

Nota: "Infraestructura crítica" hace referencia a recursos estratégicos, activos y sistemas, físicos o virtuales, tan importantes para el Estado que su destrucción o incapacidad tendría un impacto debilitador en la seguridad nacional.

(iv) Información perteneciente a, o derivada de, operaciones, fuentes y métodos de los servicios de inteligencia, siempre que conciernan a asuntos relativos a la seguridad nacional; e

(v) Información relativa a asuntos de seguridad nacional transmitida por un Estado extranjero u organismo intergubernamental y acompañada por una advertencia expresa sobre su carácter confidencial; y otras comunicaciones diplomáticas que tengan que ver con asuntos relativos a la seguridad nacional.

Nota: Se considera buena práctica dejar constancia de estas advertencias por escrito.

Nota: en la medida en que la información relativa a terrorismo y a medidas para la lucha contra el terrorismo esté comprendida en una de las categorías expuestas anteriormente, el derecho del público al acceso de dicha información podría estar sujeta a restricciones por motivos relativos con la seguridad nacional de acuerdo con estas y otras disposiciones de los Principios. A su vez, algunas informaciones relativas a terrorismo o a medidas para la lucha contra el terrorismo podrían ser de alto interés público: ver ej. Principios 10A, 10B y 10H(1).

(b) Se considera buena práctica que la legislación nacional establezca una lista exclusiva de categorías de información limitadas, como las categorías anteriores.

(c) Un Estado podría añadir una categoría de información a la lista anterior de categorías, pero tan sólo si dicha categoría está específicamente identificada y definida de forma limitada y la preservación de la confidencialidad de la información es necesaria para proteger un interés legítimo de seguridad nacional establecido por ley, tal y cómo se sugiere en el Principio 2(c). Al proponer la categoría, el Estado debería explicar que la divulgación de la información contenida en la misma supondría una amenaza para la seguridad nacional.

Principio 10: Categorías de información sobre las cuales existe una fuerte presunción o un interés esencial a favor de su divulgación

Algunas categorías de información, incluyendo las enumeradas a continuación, tienen un interés público especialmente significativo o preponderante por su relevancia extraordinaria para el proceso de control democrático y el Estado de derecho. Por ende, existen motivos contundentes, y en algunos casos, una necesidad imperiosa, para presumir que tal información debería tener carácter público y divulgarse en forma proactiva.

La información contenida en dichas categorías debería, al menos, gozar de una elevada presunción a favor de su divulgación, y podría retenerse por motivos de seguridad nacional, si bien únicamente en circunstancias absolutamente excepcionales y con arreglo a los demás Principios, solo por un plazo estrictamente limitado, en forma acorde con la ley y cuando no exista un medio razonable para limitar el perjuicio que provocaría la divulgación. La retención de ciertas subcategorías de información especificadas a continuación como sujetas de forma inherente a un interés público preponderante que justifique la divulgación, en base a motivos de seguridad nacional, nunca podrá justificarse.

A. Violaciones de los derechos humanos internacionales y del derecho internacional humanitario

(1) La información relativa a violaciones flagrantes de derechos humanos o violaciones graves del derecho internacional humanitario es un tema de interés público preponderante. Estas violaciones incluyen delitos en virtud del derecho internacional y violaciones generalizadas y sistemáticas de los derechos a la libertad personal y a la seguridad. Dicha información no podrá ser retenida invocando razones de seguridad nacional en ninguna circunstancia.

(2) La información relacionada con otras violaciones de los derechos humanos o la ley humanitaria está sujeta a una alta presunción de divulgación, y en ningún caso podrá ser retenida invocando razones de seguridad nacional de forma que se evitara la rendición de cuentas por dichas violaciones, o se despojara a la víctima de la oportunidad de obtener una indemnización efectiva.

(3) Si un Estado está sometido a un proceso de justicia transicional durante el cual se ve especialmente obligado a garantizar veracidad, justicia, reparación y la no reincidencia de violaciones [flagrantes], existe un interés público preponderante en cuanto a la divulgación de las informaciones relativas a violaciones de los derechos humanos cometidas bajo el anterior régimen. El gobierno sucesor debería, inmediatamente, dedicarse a proteger y preservar la integridad de todos los documentos que contengan dichas informaciones ocultas por el gobierno anterior, y publicarlas inmediatamente.

Nota: Ver el Principio 21(c) relativo al deber de buscar o reconstruir la información relativa a las violaciones de los derechos humanos.

(4) Si se refuta, o sospecha aun cuando no se haya establecido la existencia de violaciones, este Principio se aplica a la información que, por sí sola, o en conjunto con otra información, pudiere arrojar alguna luz sobre la verdad relativa a las supuestas violaciones.

(5) Este Principio se refiere a la información sobre violaciones que hayan tenido lugar o estén teniendo lugar, y se aplica independientemente de que las violaciones hayan sido cometidas por el Estado que retiene la información, u otros Estados.

(6) La información relativa a las violaciones cubiertas por este Principio incluyen, sin límite alguno, la siguientes:

(a) Descripción completa de los actos u omisiones que constituyan las violaciones, con documentos que la apoyen, además de las fechas y circunstancias en las que dichas violaciones hayan tenido lugar, y cuando corresponda, la ubicación de las personas desaparecidas o del lugar donde se encuentran los restos mortales.

(b) La identidad de todas las víctimas, congruente con la privacidad y otros derechos de las víctimas, de sus familiares, y testigos; y los datos generales u anónimos que pudieran servir para garantizar los derechos humanos.

Nota: Se podrá impedir que trasciendan al público general los nombres y otros datos personales de las víctimas, de sus familiares y de testigos si ello fuera necesario para evitar que estos sufran un mayor perjuicio, cuando las personas afectadas o, en el caso de personas fallecidas, sus familiares, soliciten expresa y voluntariamente, que no se divulgue dicha información, o, de otra forma, la confidencialidad de la información se corresponda con los deseos de la persona o con las necesidades particulares de grupos vulnerables. En el caso de las víctimas de violencia sexual, se solicitará expresamente su consentimiento para divulgar sus nombres u otros datos personales. Los datos de las víctimas infantiles (menores de 18 años) no estarán disponibles para el público general. Este Principio debería interpretarse, sin embargo, teniendo en cuenta la realidad de que ciertos gobiernos han protegido las informaciones relativas a las violaciones de los derechos humanos invocando el derecho a la privacidad, incluyendo el de las víctimas que han sufrido violaciones flagrantes, sin tener en cuenta los deseos reales de las mismas. Estas salvedades, sin embargo, no deberían impedir la publicación de datos generales u anónimos.

Los nombres de agencias e individuos que perpetraron o fueron, de algún modo, responsables de las violaciones, y de forma más genérica, de cualquier unidad que estuviera presente, o implicada de otro modo, en dichas violaciones, al igual que sus superiores y comandantes e información

que tenga que ver con su grado de poder y control.

(c) Información sobre las causas de las violaciones y su incapacidad de impedirlas.

B. Garantías relativas al derecho a la libertad y seguridad de la persona, la prevención de la tortura y otros abusos y el derecho a la vida

La información cubierta en este Principio incluye:

(1) Las leyes y reglamentos que autorizan la privación de la vida de una persona por parte del Estado, y las leyes y reglamentos que se refieren a la privación de la libertad, incluyendo aquellos que tengan que ver con los motivos, procedimientos, traspasos, tratamiento, o condiciones de detención de las personas afectadas, incluyendo los métodos de interrogatorio. La divulgación de estas leyes y reglamentos es de un interés público preponderante.

Notas: "Leyes y reglamentos" hace referencia a la forma de usar dichos términos en el Principio 10, e incluyen: derecho primario o legislación delegada, estatutos, reglamentos y ordenanzas, y también decretos u órdenes ejecutivas emitidos por un presidente, primer ministro u otra autoridad pública, y órdenes judiciales con fuerza de ley. Incluyen, además, cualquier normativa o interpretación de la ley consideradas como autoritarias por parte de los funcionarios ejecutivos.

La privación de la libertad incluye cualquier forma de arresto, detención, encarcelamiento o internamiento.

(2) La ubicación de todos los sitios donde se mantiene a personas privadas de su libertad y que sean administrados por el Estado o en representación de este, así como la identidad de todas las personas privadas de su libertad, los motivos de su detención y los cargos en su contra, incluso durante conflictos armados.

(3) Información sobre el fallecimiento de detenidos, e información sobre cualquier privación de vida de la que sea responsable un Estado, además de la identidad de la persona/s fallecidas, las circunstancias de su muerte y la ubicación de sus restos mortales.

Nota: En ningún caso se podrá retener información invocando razones de seguridad nacional cuando ello pudiera redundar en la detención clandestina de una persona o la creación y gestión de centros de detención clandestinos. Asimismo, en ninguna circunstancia puede resultar admisible que por acción del Estado, o con su autorización, asistencia o aquiescencia, se oculte el destino o paradero de personas privadas de su libertad a familiares u otras personas que tengan interés legítimo en el bienestar de esa persona.

Los nombres y otros datos personales de las personas que hayan sido privadas de su vida, que hayan muerto mientras estaban detenidos, o cuyos fallecimientos hayan sido provocados por agentes del Estado, podrían no divulgarse al público general hasta el

punto necesario de protección del derecho a la privacidad si las personas afectadas, o sus familiares en caso de que los afectados hayan fallecido, solicitan la retención de dichos datos expresa y voluntariamente, y si dicha retención es congruente con los derechos humanos. Las identidades de niños privados de su libertad no será divulgada al público general. Estas salvedades, sin embargo, no deberían impedir la publicación de datos generales u anónimos.

C. **Estructuras y poderes de gobierno**

La información cubierta por este Principio incluye, sin limitación, lo siguiente:

(1) Existencia de autoridades militares, de policía, seguridad e inteligencia, así como las subunidades.

(2) Las leyes y reglamentaciones aplicables a dichas autoridades, sus organismos de supervisión y mecanismos internos de rendición de cuentas, así como los nombres de los funcionarios a cargo.

(3) Información necesaria para evaluar y controlar la erogación de fondos públicos, incluidos presupuestos generales, principales rubros e información básica sobre gastos de tales autoridades.

(4) Existencia y términos de acuerdos bilaterales o multilaterales que se hayan celebrado, así como otros compromisos internacionales importantes asumidos por el Estado en materia de seguridad nacional.

D. Decisiones relativas al uso de la fuerza militar o a la adquisición de armas de destrucción masiva

(1) La información cubierta por este Principio incluye la información relevante para la toma de una decisión relativa a enviar tropas de combate o emprender acciones militares, incluso la confirmación de dichas acciones, su tamaño general y alcance, y una explicación de sus fundamentos, además de cualquier información que demuestre que un hecho establecido como parte de los fundamentos públicos fue erróneo.

Nota: La referencia al tamaño "general" de una acción y su alcance reconocen que debería, por norma general, poder satisfacerse el alto interés del público en obtener información sobre la decisión de enviar tropas de combate sin que se revelen todos los aspectos operativos de la acción militar en cuestión (Principio 9).

(2) La posesión o adquisición de armas nucleares, u otras armas de destrucción masiva, por parte de un Estado, aunque no necesariamente sobre su fabricación o capacidades operativas, es un asunto de interés público preponderante y no se ha de mantener como información confidencial.

Nota: este subprincipio no ha de ser leído como una manifestación de apoyo a la

adquisición de dichas armas.

E. Vigilancia

(1) El público debería conocer tanto las leyes y principales reglamentaciones a todas las formas de vigilancia secreta como los procedimientos relativos a la autorización de dicha vigilancia, la selección de objetivos, el uso, intercambio, almacenamiento y la destrucción y el material interceptado.

Nota: Esta información incluye: (a) las leyes que rigen todos los tipos de vigilancia, tanto abierta como encubierta, incluidas las técnicas de vigilancia indirecta como el perfilado y la búsqueda de datos, y todas las medidas de vigilancia que puedan usarse; (b) los objetivos permisibles de vigilancia; (c) el umbral de sospecha requerido para iniciar o continuar la vigilancia; (d) límites de duración de las medidas de vigilancia; (e) procedimientos para la autorización y revisión de dichas medidas; (f) los tipos de datos personal que podrán recopilarse y/o procesarse por motivos relativos a la seguridad nacional; y (g) los criterios que se aplican al uso, retención, eliminación y transferencia de dichos datos.

(2) El público también deber tener acceso a la información sobre las entidades autorizadas para llevar a cabo acciones de vigilancia, y a las estadísticas relativas al uso de dichas acciones.

Notas: Esta información incluye la identidad de cada entidad gubernamental con autoridad para llevar a cabo vigilancias específicas cada año; el número de autorizaciones para realizar vigilancias otorgadas cada año a dichas entidades; la mejor información disponible sobre el número de individuos y el número de comunicaciones sujetos a vigilancia cada año; y si se llevaron a cabo acciones de vigilancia sin autorización específica, y si es así, por parte de qué entidad.

El derecho del público a la información no se extiende, necesariamente, a los detalles fácticos u operativos de las vigilancias con arreglo a la ley y en consonancia con las obligaciones relativas a los derechos humanos. Dicha información podría ser confidencial, tanto para el público como para el objeto de la vigilancia hasta que finalicen las acciones.

(3) Se debería informar al público, además, de las vigilancias ilegales. La información acerca de este tipo de vigilancias debería ser hecha pública en la mayor medida posible, sin violar los derechos de privacidad de las personas vigiladas.

(4) Estos Principios abordan el derecho del público a acceder a la información y se entienden sin perjuicio a los derechos sustantivos y procesales adicionales de los individuos que han sido, o creen haber sido, sujetos a vigilancia.

Nota: Se considera como una buena práctica el que se solicite a las autoridades públicas que notifiquen a las personas que han sido sujetas a vigilancia encubierta (facilitando, como mínimo, información sobre el tipo de medida que se tomó, y el órgano responsable de autorizar la medida de vigilancia) en la medida de lo posible, ya que esto puede

hacerse sin poner en peligro operaciones en marcha de fuentes y métodos.

(5) Las altas presunciones a favor de la divulgación reconocida por este Principio no se aplican al respecto de la información relacionada únicamente a la vigilancia de las actividades de gobiernos extranjeros.

Nota: La información obtenida a través de vigilancia encubierta, incluyendo la relativa a las actividades de gobiernos extranjeros, habrán de divulgarse en las circunstancias identificadas en el Principio 10A.

F. Información financiera

La información cubierta por este Principio incluye información suficiente para permitir que el público entienda las finanzas del sector de la seguridad, además de los reglamentos que las rigen. Dicha información incluye, pero no está limitada a:

(1) Presupuestos de los departamentos y las agencias con los principales datos;
(2) Estados de cuentas a cierre de ejercicio con los principales datos;
(3) Reglamentos de gestión financiera y mecanismos de control;
(4) Reglamentos relativos al abastecimiento; y
(5) Informes redactados por instituciones supremas de supervisión y otros órganos responsables de la revisión de aspectos financieros del sector de la seguridad, incluyendo los resúmenes de las secciones clasificadas de dichos informes.

G. Responsabilidad relativa a violaciones constitucionales y estatutarias y otros abusos de poder

La información cubierta por este Principio incluye la relativa a la existencia, carácter y escala de las violaciones constitucionales y estatutarias y otros abusos de poder por parte de las autoridades o el personal público.

H. Salud pública, seguridad pública o medioambiente

La información cubierta por este Principio incluye:

(1) En el caso de una amenaza inminente o real a la salud pública, a la seguridad pública o al medioambiente, toda la información que pueda hacer que el público entienda o tome las medidas pertinentes para evitar o mitigar el daño procedente de dicha amenaza, tanto si es de carácter natural o humano, incluso si se trata de acciones provocadas por el Estado o por las acciones realizadas por compañías privadas.

(2) Cualquier otra información, actualizada regularmente, sobre la explotación de recursos naturales, polución e inventarios de emisiones, los impactos medioambientales derivados de grandes obras de construcción existentes o propuestas, o de la extracción de recursos, y evaluación de riesgos y planes de gestión de las instalaciones especialmente peligrosas.

Parte III.A: Normas relativas a la clasificación y desclasificación de información

Principio 11: Obligación de exponer las razones para clasificar información

(a) Tanto si un Estado cuenta con un proceso de clasificación formal, las autoridades públicas están obligadas a expresar las razones por las cuales se clasifica la información.

Nota: La "clasificación" es el proceso por el cual los documentos que contienen información sensible se revisan y se marcan para indicar quién puede acceder a los mismos y la forma en la que han de ser manejados. El establecimiento de un sistema formal de clasificación para reducir la arbitrariedad y las retenciones excesivas supone una buena práctica.

(b) Las razones deberían indicar en qué categoría acotada, de las enumeradas en el Principio 9, queda comprendida la información, y describir cuál sería el perjuicio si esta se difundiera, incluido el nivel de gravedad y probabilidad.

(c) Los niveles de clasificación, si se usan, deberían corresponder a los niveles y probabilidades de perjuicio identificadas en la justificación.

(d) Si se clasifica una información, se debería incluir (i) una marca protectora al documento indicando el nivel, si procede, y la duración máxima de la clasificación y también debería incluirse una (ii) declaración en la que se justifique la necesidad de clasificar a ese nivel y a lo largo de ese período.

Nota: Se recomienda la inclusión de una declaración que justifique cada decisión porque hace que los funcionarios presten atención al perjuicio específico que podría derivar de la divulgación de la información, y porque facilita el proceso de desclasificación y divulgación. Las marcas párrafo a párrafo facilita aún más la coherencia de las partes no clasificadas de los documentos.

Principio 12: Acceso público a las normas sobre clasificación

(a) El público debe tener la posibilidad de comentar los procedimientos y las normas que se aplican a la clasificación antes de que entren en vigor.

(b) El público debe tener acceso a las normas y procedimientos escritos que se aplican a la clasificación.

Principio 13: Potestad para clasificar información

(a) Únicamente podrán disponer la clasificación de información como reservada funcionarios expresamente autorizados o designados para ello por ley. Cuando un funcionario sin esta potestad considere que cierta información debería tener carácter clasificado, esta podrá ser considerada como clasificada durante un período breve y expresamente establecido, hasta tanto un funcionario designado haya revisado la recomendación sobre confidencialidad.

Nota: en ausencia de disposiciones legales que controlen a la autoridad que clasifica, la mejor práctica es, al menos especificar una autoridad delegada en un reglamento.

(b) La identidad de la persona responsable de una decisión sobre clasificación deberá ser localizable, o indicada en el documento, a no ser que existan razones convincentes para retener la identidad, a fin de asegurar que rinda cuentas.

(c) Los funcionarios públicos designados por la ley deben delegar su potestad original de clasificación a la menor cantidad de subordinados jerárquicos que resulte viable desde el punto de vista administrativo.

Nota: Se considera buena práctica publicar información sobre la cantidad de personas que tienen potestad para disponer la clasificación de datos, y la cantidad de personas que tienen acceso a información clasificada.

Principio 14: Facilitar la impugnación interna de la clasificación o retención de información

Los funcionarios públicos, incluidos aquellos que pertenezcan a autoridades del sector de seguridad, que crean que se ha clasificado indebidamente información deben podrán impugnar dicha clasificación.

Nota: El personal del sector de seguridad es considerado como especialmente adecuado para desafiar la clasificación debido a las elevadas culturas de secretismo existentes en las agencias de seguridad, el hecho de que la mayor parte de los países no ha establecido o designado un órgano independiente para la recepción de quejas por parte del personal de seguridad, y que la divulgación de información sobre seguridad a menudo tiene como consecuencias mayores sanciones que la divulgación de otro tipo de información.

Principio 15: Obligación de archivar, gestionar y conservar adecuadamente información y documentos sobre seguridad nacional

(a) Las autoridades públicas tienen la obligación de preservar y archivar documentos e información de conformidad con lo establecido en las normas internacionales.[130] Solamente podrán quedar exentos de preservación, gestión y archivo ciertos documentos e información en los casos en que esto sea autorizado por ley.

(b) La información se debe conservar en forma adecuada. Los sistemas de archivos deben ser congruentes, transparentes (sin revelar información clasificada de forma legítima) y

[130] Estos incluyen: Consejo Internacional de Archivos (CIA), *Principios sobre Acceso a los Archivos* (2012); CIA, Declaración Universal sobre los Archivos (2010; adoptada por la UNESCO); Consejo Europeo, *Recomendación No R(2000)13 sobre una política europea relativa al acceso a los archivos* (2000); Antonio González Quintana, CIA, *Políticas archivísticas para la defensa de los Derechos Humanos: versión actualizada y más completa del informe preparado por la Unesco y el Consejo Internacional de Archivos (1995), acerca de la gestión de archivos de los servicios de seguridad estatales de antiguos regímenes represivos* (2009).

exhaustivos, de forma tal que cuando se efectúen pedidos de acceso concretos y razonables sea posible encontrar toda la información relevante, aun cuando esta no pueda ser divulgada.

(c) Cada organismo público debería crear y publicar, y periódicamente revisar y actualizar, una lista detallada y precisa de los archivos clasificados que posee, exceptuando aquellos documentos excepcionales, si los hubiere, cuya existencia pueda retenerse de forma legítima de acuerdo con el Principio 19.

Nota: La actualización de dichas listas anualmente supone una buena práctica.

Principio 16: Limitación temporal al período de clasificación

(a) Se podrá retener información por razones de seguridad nacional únicamente durante el período que sea necesario para proteger un interés legítimo de seguridad nacional. La decisión de no divulgar cierta información debe revisarse periódicamente para asegurar que se cumpla este Principio.

Nota: la revisión exigida por ley al menos cada cinco años supone una buena práctica. Determinados países requieren que se revisen en un período menor de tiempo.

(b) La persona que dispone la clasificación deberá indicar la fecha, las condiciones o el acontecimiento en el cual cesará la clasificación.

Nota: La revisión periódica de este período de tiempo, especificaciones o condiciones del acontecimiento en el cual cesará la clasificación supone una buena práctica.

(c) Ningún tipo de información podrá tener carácter clasificado en forma indefinida. El período máximo de clasificación por razones de seguridad nacional deberá estar fijado por ley.

(d) La información podrá ser retenida por un período superior al plazo estimado sólo en circunstancias excepcionales de conformidad con una nueva decisión de retención, considerada por otro responsable, y se deberá fijar un nuevo plazo máximo.

Principio 17: Procedimientos de desclasificación

(a) Se debería identificar, en la legislación nacional, la responsabilidad gubernamental para la coordinación, monitorización e implementación de actividades de desclasificación gubernamentales, incluyendo la consolidación y la actualización periódica de directrices de relativas a la desclasificación.

(b) Se deben establecer procedimientos que permitan identificar la información clasificada que revista interés público, a fin de disponer su desclasificación con carácter prioritario. Si se ha clasificado información de interés público, incluida aquella comprendida en las categorías enumeradas en el Principio 10, debido a su carácter extremadamente delicado, deberá ser desclasificada tan pronto como sea posible.

(c) Se deben establecer en la legislación nacional procedimientos específicos para disponer la desclasificación colectiva (en lotes y/o muestras).

(d) Se deben identificar en la legislación nacional períodos preestablecidos para la desclasificación automática de distintas categorías de información clasificada. A fin de reducir al mínimo la carga que supone la desclasificación, cuando sea posible los registros deben ser desclasificados automáticamente sin previa revisión.

(e) Se debe establecer en la legislación nacional un procedimiento público y accesible para solicitar la desclasificación de documentos.

(f) Los documentos desclasificados, como los desclasificados al público por tribunales, juzgados u otros organismos de supervisión/defensoría del pueblo/apelación, deberían divulgarse en forma proactiva o bien ser puestos a disposición del público (por ejemplo, a través de la armonización con las leyes sobre archivos nacionales, acceso a la información, o ambas).

Nota: este principio se entiende sin perjuicio de las disposiciones que tengan que ver con otros motivos para la retención, tal y cómo se expone en el párrafo preambular 15.

Nota: Entre otras buenas prácticas, se pueden mencionar:

- *la evaluación periódica del uso de nuevas tecnologías en el proceso de desclasificación y*
- *la consulta periódica a personas con experiencia profesional con respecto al proceso para establecer las prioridades en materia de desclasificación, incluidas la desclasificación automática y colectiva.*

Parte III.B: Normas sobre gestión de solicitudes de información

Principio 18: Obligación de considerar las solicitudes incluso si la información tiene carácter clasificado

Que la información haya sido clasificada no es un factor decisivo al determinar cómo se debe responder a una solicitud de información. Por el contrario, la autoridad pública en cuyo poder se encuentra la información debe considerar la solicitud teniendo en cuenta los presentes Principios.

Principio 19: Obligación de confirmar o negar

(a) Al recibir una solicitud de información, la autoridad pública debe confirmar o negar que esta se encuentre en su poder.

(b) Si la jurisdicción permite la posibilidad de, en circunstancias extraordinarias, la existencia o no de información específica que pueda clasificarse de acuerdo con el Principio 3, entonces, cualquier renuencia a confirmar o negar la existencia de información en respuesta a una solicitud específica debe estar basada en la evidencia de que una mera confirmación o negación de la existencia de dicha información podría suponer un riesgo de perjuicio a una categoría de información especial establecida a través de una ley o reglamentación nacional, en la cual se requiera ese trato excepcional.

Principio 20: Obligación de expresar los motivos de la negativa por escrito

(a) Si una autoridad pública rechaza una solicitud de información, en todo o en parte, debe hacer constar por escrito los motivos concretos de esta decisión, de acuerdo con los Principios 3 y 9,

dentro del período de tiempo especificado por ley para la respuesta a las solicitudes de información.

Nota: Consultar el Principio 25 para el período de tiempo por el que ha de darse una respuesta, por ley, a las solicitudes de información.

(b) La autoridad debe asimismo proporcionar al solicitante la suficiente información acerca de la identidad del funcionario o funcionarios públicos que dispuso o dispusieron que la información tendría carácter reservado, y el proceso de dicha disposición, a menos que esa identificación constituya por sí misma una divulgación de información confidencial, e indicar las vías de apelación disponibles para permitir un examen del cumplimiento de la ley por parte de la autoridad.

Principio 21: Obligación de recuperar o reconstruir la información faltante

(a) Cuando una autoridad pública no pueda localizar la información necesaria para responder una solicitud, y los registros de dicha información deberían haber sido preservados o recopilados, la autoridad debe adoptar medidas razonables para recuperar o reconstruir la información faltante a fin de permitir su eventual transmisión al solicitante.

Nota: este principio se aplica a la información que no puede ser localizada por cualquier razón, por ejemplo, porque nunca fue recogida, fue destruida o no se puede rastrear.

(b) Debería solicitarse el que un representante de la autoridad pública indique, bajo juramento, y en un tiempo razonable y establecido por ley, todos los procedimientos llevados a cabo para la recuperación o reconstrucción de la información de manera que dichos procedimientos puedan ser judicialmente revisados.

Nota: Cuando no se pueda localizar un documento o información que, por ley, debería haber sido conservado, la cuestión deberá remitirse a las autoridades policiales o administrativas para que investiguen lo sucedido. El resultado de la investigación debe tener carácter público.

(c) La obligación de recuperar o reconstruir información es particularmente imperiosa (i) cuando esta se vincula con presuntas violaciones flagrantes de derechos humanos y/o (ii) durante una transición a una forma de gobierno democrática de un gobierno caracterizado por la violación generalizada de los derechos humanos.

Principio 22: Obligación de divulgar partes de documentos

Las excepciones a la divulgación se aplican únicamente a información específica y no a la totalidad de documentos u otros registros. Solamente podrá impedirse la divulgación de información específica cuando se haya demostrado la validez de la restricción ("información exenta"). Cuando un registro contenga a la vez información exenta y no exenta, las autoridades públicas tienen la obligación de separar y divulgar la información no exenta.

Principio 23: Obligación de identificar la información reservada

La autoridad pública que tenga en su poder información que se niega a difundir debe identificar dicha información con la mayor precisión posible. Como mínimo, la autoridad debe divulgar el volumen de información que se niega a difundir, por ejemplo, ofreciendo una estimación del número de páginas.

Principio 24: Obligación de proporcionar información en formatos disponibles

Las autoridades públicas deben proporcionar la información en el formato que sea de preferencia del solicitante siempre que esto sea posible.

Nota: Esto incluye, por ejemplo, la obligación de las autoridades públicas de tomar las medidas apropiadas para proporcionar información a personas con discapacidad en formatos y tecnologías accesibles de forma oportuna y sin un coste adicional, de acuerdo con la Convención de las Naciones Unidas para las Personas con Discapacidad.

Principio 25: Plazo para responder solicitudes de información

(a) Los plazos para responder a solicitudes, incluida la respuesta sobre aspectos de fondo, el control interno, las decisiones de organismos independientes cuando corresponda y la revisión judicial, deben ser establecidos en la legislación y deben ser tan breves como sea posible.

Nota: se considera como una buena práctica, conforme a los requisitos establecidos en la mayor parte de las leyes de acceso a la información, establecer veinte días laborables o menos como el período de tiempo en el que ha de darse una respuesta consistente. Si no se establecen límites de tiempo por ley para responder a una solicitud, el límite de tiempo se establecerá en no más de 30 días para una petición estándar. Las leyes podrán establecer diferentes límites para tener en cuenta el volumen de documentos y su nivel de complejidad y sensibilidad.

(b) Deben aplicarse plazos abreviados cuando se demuestre que existe una necesidad pública urgente de acceder a la información, como por ejemplo, si se trata de una información necesaria para preservar la vida o la libertad de una persona.

Principio 26: Derecho a recurrir las decisiones relativas a la retención de información

(a) El solicitante tiene derecho a interponer un recurso rápido, a bajo costo para que la negación a divulgar una información, o asuntos relacionados con la misma, sea revisada por una autoridad independiente.

Nota: Dicha negación podría incluir un rechazo implícito o silencioso, y los asuntos sujetos

a la revisión por parte de una autoridad independiente podrían incluir tarifas, calendarios y formato.

(b) La autoridad pública independiente debe tener la competencia y recursos necesarios para garantizar una revisión efectiva, además de pleno acceso a toda la información relevante, incluso si se trata de información clasificada.

(c) Cualquier persona debería tener derecho a obtener una revisión independiente y efectiva de todas las cuestiones relevantes por parte de un tribunal competente.

(d) Si un tribunal se pronuncia acerca de la garantía de retención de una información, debería publicar las razones, basadas en hechos, y sus análisis legales por escrito, excepto en circunstancias extraordinarias y congruentes con el Principio 3.

Parte IV: Aspectos judiciales relativos a la seguridad nacional y al derecho a la información

Principio 27: Principio general de control judicial

(a) Nadie podrá basarse en invocaciones relativas a la seguridad nacional para menoscabar el derecho fundamental a un juicio justo por parte de un tribunal competente, independiente e imparcial establecido por ley.

(b) Cuando una autoridad pública pretenda retener información por razones de seguridad nacional en el marco de un procedimiento legal, los tribunales tendrán la potestad de revisar la información para determinar si debería tener carácter confidencial. Por norma general, un tribunal no podrá rechazar un caso sin revisar la información.

Nota: En consonancia con el Principio 4(d), el tribunal no adoptará su decisión sobre la base de resúmenes o declaraciones juradas donde simplemente se reivindique la necesidad de confidencialidad sin que se proporcione una base probatoria para dicha reivindicación.

(c) El tribunal debería asegurarse de que una persona que solicita acceder a la información pueda, en la mayor medida posible, conocer e impugnar el argumento invocado por el gobierno para no divulgar la información.

(d) El tribunal debe pronunciarse sobre la legalidad y procedencia del argumento invocado por la autoridad pública, tanto en sentido sustantivo como procesal, y podrá exigir que se difunda la información o que se otorgue un resarcimiento adecuado en caso de que esta no se divulgue en forma parcial o total, incluido el sobreseimiento en procesos penales.

(e) El tribunal debe valorar en forma independiente si la autoridad pública ha invocado adecuadamente una excepción u otro motivo para no permitir la divulgación: la mera clasificación no podrá ser concluyente en cuanto a la solicitud de la no divulgación de una información. Asimismo, el tribunal debe evaluar la naturaleza del perjuicio referido por la autoridad pública, la probabilidad de que ocurra y el interés público en que se divulgue la información, de acuerdo con las normas definidas en el Principio 3.

Principio 28: Acceso público a procesos judiciales

(a) Nadie podrá basarse en invocaciones relativas a la seguridad nacional para menoscabar el derecho fundamental de acceso público a procesos judiciales.

(b) Las sentencias judiciales —en las cuales se establezcan todas las determinaciones de un tribunal y se incluyan las principales conclusiones, evidencias y fundamentos jurídicos— deben darse a conocer en forma pública, salvo cuando esto no sea conveniente para preservar el interés de niños menores de dieciocho años.

Notas: la legislación internacional no permite la derogación de la obligación de pronunciar sentencias públicamente justificándose en motivos relativos a la seguridad nacional.

Los expedientes de los procedimientos de los tribunales de menores no deberían publicarse. Los expedientes de otros procedimientos que afectan a niños deberían, normalmente, guardar los nombres y otra información sobre aquellos niños que tengan menos de dieciocho años.

(c) El derecho del público de acceso a la justicia debería incluir el acceso público inmediato a: (i) los fundamentos de las decisiones judiciales; (ii) información sobre la existencia y el avance de los casos; (iii) argumentos escritos presentados ante el tribunal; (iv) audiencias y procedimientos judiciales; y (v) evidencias en procedimientos judiciales que constituyen el fundamento de una condena, a menos que se justifique una derogación de lo aquí expuesto de acuerdo con estos Principios.

Nota: La legislación internacional relativa a la exigencia de juicios imparciales permite que los tribunales excluya al público o a parte del público de un procedimiento por motivos de seguridad nacional en una sociedad democrática, o por moralidad, orden público, el interés de la vida privada de las partes, o para evitar perjuicio a los intereses de la justicia, siempre que dichas restricciones sean necesarias y proporcionadas.

(d) El público debe tener la posibilidad de impugnar los argumentos invocados por la autoridad pública para justificar la necesidad absoluta de restringir el acceso público a procesos judiciales por razones de seguridad nacional.

(e) Cuando un tribunal emita una decisión restringiendo el acceso público a procesos judiciales, debe informar públicamente y por escrito los hechos, razones y los fundamentos legales en las que justifica su decisión, excepto cuando se trate de circunstancias extraordinarias de acuerdo con el Principio 3.

Nota: Este Principio no pretende modificar la legislación vigente en un Estado sobre procedimientos preliminares a los cuales normalmente el público no tiene acceso. Su aplicación se prevé exclusivamente para casos en que el proceso judicial permitiría en general el acceso público y el intento por impedirlo se justifique apelando motivos de seguridad nacional.

El derecho del público de acceder a procedimientos y documentos judiciales surge de la importancia que reviste dicho acceso para fomentar (i) la imparcialidad real y percibida de los procedimientos judiciales;

(ii) una actuación más adecuada y honesta de las partes; y (iii) una mayor certeza de los comentarios públicos.

Principio 29: Acceso de las partes a información relativa a procedimientos penales

(a) El tribunal no podrá prohibir que una persona acusada comparezca en su propio juicio por razones de seguridad nacional.

(b) En ningún caso la condena o privación de la libertad podrá dictarse sobre la base de pruebas que el acusado no ha tenido oportunidad de examinar e impugnar.

(c) En aras de la justicia, una autoridad pública deberá además divulgar al acusado y a su defensa, los cargos contra una persona y cualquier información necesaria para garantizar un juicio justo, con independencia de si la información tiene carácter clasificado con arreglo a los Principios 3-6, 10, 27 y 28, incluyendo una consideración de los intereses públicos.

(d) Cuando la autoridad pública se niegue a difundir información necesaria para garantizar un juicio justo, el tribunal deberá suspender o desestimar la acusación.

Nota: Las autoridades públicas no deben usar información en provecho suyo cuando invoquen su carácter confidencial, si bien podrán optar por que no se divulgue la información y afrontar las consecuencias.

Nota: Los principios 29 y 30 se incluyen en estos Principios relativos al acceso público a la información a la luz del hecho de que, las revisiones judiciales y las divulgaciones relacionadas en el contexto de la supervisión jurídica, son a menudo medios importantes para la divulgación pública de información.

Principio 30: Acceso de las partes a información relativa a causas civiles

(a) Todas las reclamaciones relativas a la retención de información por parte de una autoridad pública en un caso civil habrán de revisarse de manera congruente con los Principios 3-6, 10, 27 y 28, incluyendo una consideración de los intereses públicos.

(b) Las víctimas de tortura y otras violaciones de derechos humanos tienen derecho a un recurso y un resarcimiento adecuados, incluida la difusión pública de los abusos sufridos. Las autoridades públicas no deben retener información que sea trascendental para los reclamos de estas víctimas de un modo incompatible con este derecho.

(c) Además, el público tiene también derecho a la información que tenga que ver con violaciones flagrantes de los derechos humanos y violaciones graves de la ley humanitaria internacional.

Parte V: Organismos que supervisan el sector de seguridad

Principio 31: Establecimiento de organismos de supervisión independientes

Los Estados deben establecer, cuando aún no lo hayan hecho, organismos de supervisión independientes encargados de controlar las entidades del sector de seguridad y sus datos sobre: operativos, normativas, políticas, finanzas y administración. Estos organismos de supervisión independientes deben ser institucional, operacional y financieramente independientes de las instituciones a las que han de supervisar.

Principio 32: Acceso irrestricto a información necesaria para el desempeño de la función

(a) Los organismos de supervisión independientes deben contar con garantía de acceso legítimo a toda la información necesaria para el desempeño de su función. No deben aplicarse restricciones a este acceso, con independencia del nivel de clasificación o confidencialidad de la información, una vez cumplidos los requisitos razonables sobre seguridad de la consulta.

(b) La información a la cual deben tener acceso los organismos de supervisión incluye, sin carácter restrictivo:

i. todos los registros, tecnologías y sistemas en poder de autoridades del sector de seguridad, con independencia de la forma o medio, y de si han sido o no creados por dicha autoridad;
ii. sitios, objetos y establecimientos; e
iii. información poseída por personas a quienes los veedores consideran relevantes para sus funciones de supervisión.

(c) Cualquier obligación que tenga el personal del sector de seguridad de preservar el carácter secreto o confidencial de información, no debería impedir que respondan a las peticiones de información formuladas por instituciones de supervisión. Dicha respuesta no debería considerarse como un incumplimiento de la ley aplicable o del contrato donde se establezcan esas obligaciones.

Principio 33: Facultades, recursos y procedimientos necesarios para asegurar el acceso a información

(a) Los organismos de supervisión independientes deben contar con facultades jurídicas suficientes para poder consultar e interpretar información relevante que consideran necesaria para desempeñar sus funciones.

(i) Como mínimo, estas facultades deben incluir el derecho a interpelar a miembros actuales y anteriores del poder ejecutivo y empleados y contratistas de autoridades públicas, solicitar e inspeccionar los registros correspondientes, e inspeccionar lugares y establecimientos.

(ii) Los organismos de supervisión independientes también deberían tener la potestad de citar a personas, requerir registros y recibir el testimonio, bajo juramento u otro tipo de declaración solemne, de personas que se considera que tienen en su poder información relevante para el desempeño de sus funciones, con la plena cooperación de organismos de aplicación de la ley cuando resulte necesario.

(b) Los organismos de supervisión independientes, al gestionar la información y recibir testimonios, deben tener en cuenta, entre otras cosas, la leyes relevantes sobre privacidad, así como las garantías contra la autoincriminación y otros requisitos del debido proceso.

(c) Los organismos de supervisión independientes deben tener acceso a los recursos económicos, tecnológicos y humanos necesarios para que puedan identificar, consultar y analizar información relevante para el efectivo desempeño de sus funciones.

(d) Se debe exigir por ley a las instituciones del sector de seguridad que presten a los organismos de supervisión independientes la cooperación que estos necesitan para consultar e interpretar la información indispensable para el desempeño de su función.

(e) Se debe exigir por ley a las instituciones del sector de seguridad que, en forma oportuna y proactiva, divulguen a los organismos de supervisión independientes categorías concretas de información que los veedores hayan determinado que sean necesarias para desempeñar su función. Tal información deberá incluir, sin carácter restrictivo, posibles transgresiones de la ley y de los estándares de derechos humanos.

Principio 34: Transparencia de los organismos de supervisión independientes

A. Aplicación de las leyes sobre acceso a la información

Las leyes que regulan el desempeño del derecho al público en general a consultar información en poder de autoridades públicas deben aplicarse a los organismos de supervisión del sector de seguridad.

B. Elaboración de informes

(1) Los órganos de supervisión deben estar legalmente obligados a elaborar informes periódicos y a hacer públicos tales informes. Dichos informes deben incluir, como mínimo, información sobre el propio órgano supervisor, incluida su composición, presupuesto, historial y actividades.

Nota: Estos informes deberían, además, incluir información acerca del mandato, estructura, presupuesto y actividades generales de cualquier institución del sector de la seguridad que no divulgue dicha información al público.

(2) Los organismos de supervisión independientes también deben proporcionar versiones públicas sobre sus investigaciones y estudios temáticos y casuísticos, y deben proporcionar la mayor cantidad de información posible sobre cuestiones de interés público, incluidas las áreas enumeradas en el Principio 10.

(3) Los organismos de supervisión independientes deberían, siempre que elaboren informes públicos, respetar los derechos de todas las personas implicadas, incluyendo su derecho de privacidad.

(4) Los organismos de supervisión independientes deberían ofrecer a las instituciones a las que van a supervisar, la posibilidad de examinar, en forma oportuna, los informes que tengan previsto difundir, a fin de que puedan plantear inquietudes sobre la inclusión de contenidos que puedan ser clasificados como confidenciales. La decisión definitiva sobre qué contenidos serán difundidos corresponderá al propio organismo de supervisión.

C. Contacto y accesibilidad

(1) La normativa que da origen a los organismos de supervisión, incluidas sus funciones y facultades, debe estar a disposición del público y ser de fácil consulta.

(2) Los organismos de supervisión independientes deberían establecer mecanismos y medios para personas analfabetas, que hablen lenguas minoritarias o tengan alguna discapacidad visual o auditiva para que puedan acceder a información relativa a su trabajo.

(3) Los organismos de supervisión independientes deberían establecer una serie de mecanismos de libre disposición a través de los cuales el público, incluidas personas en sitios geográficos remotos, pueda ponerse en contacto con tales organismos y, en el caso de las entidades que gestionan denuncias, presentar denuncias o inquietudes.

(4) Los organismos de supervisión independientes deben contar con mecanismos que permitan preservar de manera efectiva la confidencialidad de las denuncias y el carácter anónimo del denunciante.

Principio 35: Medidas para la protección de información administrada por organismos de supervisión del sector de seguridad

(a) La ley debería exigir a los organismos de supervisión independientes que implementen todas las medidas necesarias para proteger la información que tengan en su poder.

(b) El poder legislativo debería tener la potestad de decidir si (i) los miembros de comisiones de supervisión legislativas, y (ii) los máximos responsables y los miembros de organismos de supervisión independientes de carácter extraparlamentario deben ser objeto de un control de seguridad antes de su nombramiento.

(c) Si se requiere un control de seguridad, debería realizarse (i) de forma oportuna, (ii) de acuerdo con los principios establecidos, (iii) sin sesgos políticos ni motivaciones, y (iv) siempre que sea posible, por parte de una institución que no esté sujeta a la supervisión por parte del organismo cuyo personal está siendo examinada.

(d) Con arreglo a lo dispuesto en los Principios enumerados en las Partes VI y VII, los miembros o el personal de los organismos de supervisión que difundan información clasificada o confidencial por medios distintos a los mecanismos de presentación de informes habituales y establecidos legalmente para estos organismos deberán cumplir los correspondientes procedimientos administrativos, civiles o penales.

Principio 36: Potestad del poder legislativo de difundir información

El poder legislativo debería tener la potestad de difundir cualquier información al público, incluso si se trata de información que el poder ejecutivo reclama confidencial por motivos de seguridad nacional, cuando lo considere pertinente en virtud de los procedimientos que establezca para ese fin.

Parte VI: divulgaciones de interés público por parte del personal de organismos públicos

Principio 37: Tipos de irregularidades

Si un funcionario público divulga una información, sea cual sea su clasificación, que presenta una irregularidad en base a las siguientes categorías, esto se considerará como una "divulgación protegida" si cumple con las condiciones establecidas en los Principios 38-40. Las "divulgaciones protegidas" pueden pertenecer a los actos indebidos hayan sido cometidos, tengan lugar actualmente o posiblemente vayan a producirse.

a. delitos penales;
b. violaciones de los derechos humanos;
c. violaciones de la ley humanitaria internacional;
d. corrupción;
e. riesgos para la salud y la seguridad pública;
f. riesgos para el medioambiente;
g. abuso de la función pública;
h. errores judiciales;
i. gestión indebida o desperdicio significativo de recursos;
j. represalias por la difusión de las anteriores categorías de irregularidades; y
k. ocultamiento deliberado de asuntos comprendidos en alguna de las categorías anteriores.

Principio 38: Aspectos, motivación y pruebas para la difusión de información que evidencia una irregularidad

(a) La ley debería proteger de posibles represalias, tal y cómo se define en el Principio 41, al personal de organismos públicos que divulgue información que evidencia una irregularidad, aun cuando la información tenga carácter clasificado o confidencial, siempre que, al momento de la divulgación:

(i) la persona que difunde la información haya tenido motivos razonables para suponer que esta estaba relacionada con una de las categorías de irregularidades establecidas en el Principio 37 y
(ii) La divulgación cumpla con las condiciones establecidas en los Principios 38-40

(b) La motivación para efectuar una divulgación protegida es irrelevante, salvo cuando las afirmaciones hayan sido falsas.

(c) No se podrá exigir a una persona que efectúa una divulgación protegida que presente evidencias para sustentar su denuncia ni se le impondrá tampoco la carga de la prueba.

Principio 39: Procedimientos para efectuar y responder divulgaciones protegidas en el ámbito interno o a organismos de supervisión

A. Divulgaciones internas

Se debe exigir por ley a las autoridades públicas que establezcan procedimientos internos y designen a personas para recibir divulgaciones protegidas.

B. Divulgaciones a organismos de supervisión independientes

(1) Los Estados deberían también establecer o identificar organismos independientes que se encarguen de recibir e investigar divulgaciones protegidas. Estos organismos deben ser independientes en términos institucionales y operativos respecto del sector de seguridad en su totalidad y de otras autoridades desde las cuales pueden surgir divulgaciones, incluido el poder ejecutivo.

(2) El funcionario público debe poder consultar en forma directa a organismos independientes, sin antes tener que efectuar una divulgación a través de procedimientos internos.

(3) La legislación debe garantizar que puedan acceder a toda la información relevante y brindarles las potestades de investigación necesarias para asegurar el acceso. Tales potestades pueden incluir la facultad de citar a personas y exigir que se preste testimonio bajo juramento u otro tipo de declaración solemne.

C. Obligación de los organismos internos y los organismos de supervisión independientes de recibir las divulgaciones

Si una persona realiza una divulgación protegida, tal y cómo se define en el Principio 37, en el ámbito interno o a un organismo de supervisión independiente, el organismo que reciba la divulgación estará obligado a:

(1) investigar la supuesta irregularidad y tomar medidas oportunas para resolver el asunto en un período de tiempo especificado por ley, o, tras haber consultado con la persona que ha realizado la divulgación, referirla a un organismo autorizado y competente para que lleve a cabo una investigación;
(2) proteger la identidad del personal público que pretenda enviar información confidencial; las informaciones anónimas deberían considerarse en base a sus méritos;
(3) proteger la información divulgada y el hecho de se ha realizado una divulgación excepto si la divulgación de más información fuera necesaria para remediar la irregularidad; y
(4) notificar a la persona que ha realizado la divulgación del progreso y la finalización de una investigación y, siempre que sea posible, los pasos que se han dado o las recomendaciones ofrecidas.

Principio 40: Protección de las divulgaciones protegidas

La legislación debe proteger de represalias, tal y cómo se define en el Principio 41, las divulgaciones al público de información que tenga que ver con irregularidades, tal y cómo se define en el Principio 37, si la divulgación tiene los siguientes criterios:

(a) (1) la persona ha divulgado la misma, o prácticamente la misma información en el ámbito interno y al organismo de supervisión independiente y:

(i) el organismo al que se difundió la información rechazó o no investigó la divulgación adecuadamente, de acuerdo con la normativa internacional aplicable; O

(ii) la persona no recibió un resultado adecuado en el período razonable definido por ley. O

(2) la persona consideró de forma razonable que se daba un riesgo significativo de que si se hacía la divulgación de forma interna o a un organismo de supervisión independiente se habrían destruido o escondido las pruebas, se hubiera interferido con un testigo, o se hubieran tomado represalias contra una tercera persona o tercera parte;

O

(3) no había un organismo interno ni un organismo de supervisión establecido a quien difundir la información;

O

(4) la divulgación estaba relacionada con un acto u omisión que constituyó una amenaza seria e inminente a la vida, la salud y la seguridad de personas, o del medio ambiente

Y

(b) La persona que realizó la divulgación sólo divulgó la cantidad de información que era razonablemente necesaria para revelar una irregularidad;

Nota: Si en el proceso de divulgación de información que revele una irregularidad, la persona también da a conocer documentos que no son relevantes para demostrar la irregularidad, la persona deberá ser protegida de represalias en todo caso, a menos que el daño causado por la divulgación exceda cualquier interés público de la divulgación. la persona que realizó la divulgación solo divulgó la información necesaria para revelar una irregularidad;

Y

(c) la persona que realizó la divulgación consideró de forma razonable que el interés público de la información revelada compensaría cualquier perjuicio hacia el interés del público resultante de dicha divulgación.

Nota: La prueba de "Considerar de forma razonable" es una prueba a la vez objetiva y subjetiva. La persona debe mantenido una creencia (subjetividad), y esa creencia debe

haber sido razonable para él o para ella (objetividad). A la hora de impugnar, la persona debería tener que defender la racionalidad de su creencia, y, será en última instancia responsabilidad de un tribunal independiente la determinación de si esta prueba se ha cumplido como para calificar la divulgación para su protección.

Principio 41: Protección frente a represalias por efectuar divulgaciones de información que evidencien irregularidades

A. Inmunidad contra responsabilidades civiles y penales por la realización de divulgaciones protegidas

De acuerdo con los principios 37-40, una persona que haya efectuado una divulgación no debería estar sujeto a:

1. Procedimientos penales, incluidos, sin carácter restrictivo, las acciones penales por divulgación de información clasificada o confidencial; o
2. Procedimientos civiles relacionados con la divulgación de información clasificada o confidencial, incluidos, sin carácter restrictivo, los recursos interpuestos para obtener una indemnización y causas por difamación;

B. Prohibición de otra clase de represalias

(1) La legislación debe prohibir las represalias tomadas contra una persona que haya efectuado, o se sospeche que haya efectuado, una divulgación de acuerdo con los Principios 37-40.

(2)

(a) Entre las medidas de represalia prohibidas se incluyen, sin carácter restrictivo: Medidas o sanciones administrativas incluidas, sin carácter restrictivo, cartas de advertencia, investigaciones en represalia, descenso de categoría profesional, traspaso, negativa a otorgar ascensos, extinción de la relación laboral, acciones que pretenden dañar la reputación de una persona, o suspensión o revocación de una acreditación de seguridad;
(b) Acoso físico o psicológico; y
(c) Amenazas de implementar alguna de las medidas anteriores.
(3) Las medidas contra personas distintas de quienes divulgaron la información podrán constituir represalias en algunas circunstancias.

C. Investigación de las represalias por un organismo de supervisión independiente y autoridades judiciales

1. Debe reconocerse a cualquier persona que realice una divulgación protegida el derecho a denunciar cualquier represalia ante un organismo de supervisión independiente.

2. Los organismos de supervisión independientes deberían tener la obligación de investigar de forma efectiva presuntas represalias o amenazas de represalias. Dichos organismos

deberían tener, además, la capacidad de iniciar investigaciones si no cuentan con un informe de represalias.

3. Se debe dotar a los organismos de supervisión independientes de todas las potestades y recursos necesarios para investigar de forma efectiva cualquier represalia denunciada, además de la potestad de citar a personas, consultar información y escuchar testimonios bajo juramento o afirmación.
4. Los organismos de supervisión independientes deberían esforzarse para garantizar que los procedimientos relativos a las represalias denuncias son justos y coherentes con las normas establecidas.

5. Los organismos de supervisión independientes deberían tener potestad para pedir a la autoridad pública pertinente que tome medidas correctivas o resarcitorias, incluidas, sin carácter restrictivo, la reincorporación; la reasignación; y/o el pago de las tasas legales, otros costes razonables, cantidades pendientes y prestaciones relacionadas, gastos de desplazamiento, y/o indemnizaciones.

6. Los organismos de supervisión independientes también deberían tener potestad para prohibir que las autoridades públicas tomasen represalias.

7. Dichos organismos deberían investigar la presunta represalia en un período de tiempo razonable y definido por ley.

8. Dichos organismos deberían notificar a las personas relevantes al menos de la finalización de la investigación, y siempre que sea posible, de las medidas adoptadas o de las recomendaciones realizadas.

9. Las personas que hayan efectuado una divulgación protegida y afirmen haber sido objeto de represalias deben tener la posibilidad de recurrir ante la justicia la conclusión a la que llegue el organismo independiente.

D. Carga de la prueba

Si una autoridad pública adopta medidas que sean adversas para la persona que efectuó una divulgación protegida, la autoridad tiene la responsabilidad de demostrar que tales medidas no estuvieron relacionadas con la divulgación.

E. Sin posibilidad de derogar derechos ni recursos

No se podrán derogar ni limitar los derechos y recursos establecidos en los Principios 37-40, bajo ningún acuerdo, política, forma o condición laboral, ni por ningún acuerdo de arbitraje previo al conflicto. Cualquier intento de derogar o limitar estos derechos o recursos se considerará nulo.

Principio 42: Fomentar y facilitar las divulgaciones protegidas

Los Estados deben propender porque los funcionarios públicos efectúen divulgaciones protegidas. A fin de fomentar y facilitar la divulgación de información sobre irregularidades, los Estados deben exigir que todos los funcionarios públicos adopten pautas para la efectiva aplicación de los Principios 37 a 42.

Nota: Estas pautas deben brindar, como mínimo, (1) orientación respecto al derecho y/o la obligación de divulgar irregularidades, (2) los tipos de información que pueden o deben ser divulgados, y (3) los procedimientos obligatorios para efectuar tales divulgaciones, y (4) las protecciones dispuestas por ley.

Principio 43: Defensa del interés público para el personal público

(a) Si el personal público fuere objeto de procedimientos penales o civiles, o sanciones administrativas en relación con la divulgación de una información no protegida bajo estos Principios, la leyle proporcionará una defensa de interés público si el interés público de la información divulgada en cuestión supera el interés público en que esta no trascienda

> *Nota: Este Principio se refiere a todas las divulgaciones de información que no están protegidas, o bien porque el tipo de información no entra dentro de las categorías señaladas en el Principio 37, o bien porque la divulgación contiene información que entra dentro de las categorías señaladas en el Principio 37 pero no fue efectuada de acuerdo con los procedimientos destacados en los Principios 38-40.*

(b) Al decidir si el interés público en que trascienda la información supera al interés público en que no sea difundida, las autoridades fiscales y judiciales deberán considerar:

(i) si el alcance de la divulgación era razonablemente necesario para divulgar la información de interés público;
(ii) la extensión y riesgo de perjuicio al interés público causado por la divulgación;
(iii) si la persona tuvo motivos razonables para suponer que la divulgación redundaría en beneficio del interés público;
(iv) si la persona trató de efectuar la divulgación protegida a través de procedimientos internos y/o a un organismo de supervisión independiente, y/o al público con arreglo a los procedimientos estipulados en los Principios 38-40; y
(v) la existencia de circunstancias imperiosas que justifiquen la divulgación.

Nota: Cualquier ley que establezca sanciones para la divulgación no autorizada de información debería ser coherente con el Principio 46(b). Este Principio no pretende limitar los derechos de libertad de expresión que ya corresponden al personal público ni ninguna de las protecciones otorgadas bajo los Principios 37-42 o 46.

Parte VII: Límites a las medidas destinadas a sancionar o restringir la divulgación de información al público

Principio 44: Protección contra sanciones a divulgaciones razonables efectuadas de buena fe por funcionarios que manejan información

Las personas responsables de responder a solicitudes de información presentadas por el público no deberían ser sancionadas por divulgar información cuando hayan actuado de buena fe y creído razonablemente que la información podía ser difundida legalmente.

Principio 45: Sanciones para el supuesto de destrucción de datos o negativa a difundir información

(a) El funcionario público será susceptible de sanciones cuando destruya o altere deliberadamente información con el propósito de impedir que pueda ser consultada por el público.

(b) Cuando un tribunal u organismo independiente haya dado instrucciones de que se divulgue cierta información y esta no se difunda en un plazo razonable, el funcionario y/o la autoridad pública responsable de que no se produzca la divulgación serán pasibles de las sanciones correspondientes, a menos que se interponga un recurso de apelación de conformidad con los procedimientos establecidos legalmente.

Principio 46: Limitaciones en las sanciones penales por la divulgación de información realizada por personal público

(a) La divulgación de información efectuada por personal público, incluso si dicha información no está protegida por la Parte VI, no debería ser objeto de sanciones penales, aunque sí podrían serlo de sanciones administrativas tales como la revocación de una acreditación de seguridad o incluso la extinción de la relación laboral.

(b) Si la ley, no obstante, impone sanciones penales por la divulgación no autorizada de información al público o a personas con la intención de que dicha información se haga pública, se aplicarán las siguientes condiciones:

(i) Se aplicarán sanciones penales sólo a la divulgación de unas categorías estrechas de información claramente establecidas por la ley.

Nota: si la legislación nacional establece categorías de información cuya divulgación puede ser objeto de sanciones penales, habrán de ser similares a las siguientes en cuanto a especificidad e impacto en la seguridad nacional: datos tecnológicos sobre armas nucleares; fuentes de inteligencia, códigos y métodos; códigos diplomáticos; identidades de agentes encubiertos; y propiedad intelectual en la que el gobierno tiene un interés de propiedad, además de conocimientos que pudieran perjudicar a la seguridad nacional.

(ii) La divulgación debería plantear un riesgo real e identificable de perjuicio significativo;

(iii) Cualquier sanción criminal, tal y como se establece y se aplica en la legislación, debería ser proporcional al perjuicio causado; y

(iv) La persona debería poder apelar a la defensa de interés público, tal y cómo se señala en el Principio 43.

Principio 47: Protección contra las sanciones por la posesión y diseminación de información clasificada por parte de personas que no trabajen en organismos públicos

(a) Una persona que no sea un funcionario público no puede ser sancionada por la recepción, posesión o divulgación de información clasificada.

(b) Una persona que no sea un funcionario público no puede ser objeto de cargos por conspiración u otros delitos basados en el hecho de que han buscado y obtenido la información.

Nota: Este Principio trata de evitar el procesamiento criminal por la adquisición o reproducción de la información. Sin embargo, este Principio no pretende impedir el procesamiento de una persona por otros delitos cometidos, como robo o extorsión, cometidos con el objeto de obtener la información.

Nota: las divulgaciones de terceras partes constituyen una importante medida correctiva para la clasificación excesiva generalizada.

Principio 48: Protección de las fuentes

Ninguna persona que no sea funcionario público debería ser obligada a revelar una fuente confidencial o materiales no publicados en el marco de una investigación sobre la divulgación no autorizada de información a la prensa o al público.

Nota: Este Principio hace referencia exclusivamente a investigaciones relativas a la divulgación no autorizada de información, y no a otros delitos.

Principio 49: Restricción previa

(a) Debe prohibirse la aplicación de restricciones previas a la publicación, efectuada para proteger la seguridad nacional.

Nota: Las restricciones previas son órdenes dictadas por autoridades judiciales u otros organismos estatales en las cuales se prohíbe la publicación de determinados materiales.

(b) Si la información se ha puesto ampliamente a disposición del público por cualquier medio, ya sea lícito o ilícito, se presumirá inválida cualquier medida destinada a impedir que continúe su difusión por el medio a través del cual ya ha tomado conocimiento público.

Nota: "Ampliamente a disposición" significa que la información ha sido difundida de manera suficiente y que no existe la posibilidad de tomar medidas prácticas para preservar su confidencialidad.

Parte VIII: Principio Final

Principio 50: Relación de estos Principios con otras normas

No se interpretará que lo establecido en estos Principios restringe o limita ningún derecho a información reconocido por las leyes o estándares internacionales, regionales o nacionales, ni tampoco ninguna de las disposiciones del derecho nacional o internacional que otorguen una protección más amplia a la divulgación de información efectuada por personal s público u otras personas.

Anexo: organizaciones asociadas

Las siguientes 22 organizaciones han contribuido significativamente a la redacción de los Principios, y se comprometen a trabajar en su diseminación y publicidad, además de ayudar en su implementación.[131] Tras el nombre de cada organización consta la ciudad en la que tiene su sede, si procede, y el país o región en la cual trabaja. Aquellas organizaciones que desarrollen trabajo sustancial en tres o más regiones han sido denominadas como "global."

- Centro Africano para la Libertad de Expresión (Kampala/África);
- Foro Africano para la Supervisión Civil de la Policía (APCOF) (Ciudad del Cabo/África)
- Alianza Regional por la Libre Expresión e Información (Américas)
- Amnistía Internacional (Londres/global);
- Artículo 19, Campaña Mundial para la Libertad de Expresión (Londres/global);
- Foro Asiático para los Derechos Humanos y el Desarrollo) (Bangkok/Asia);
- Center for National Security Studies (Washington DC/Estados Unidos);
- Universidad Central Europea (Budapest/ Europa);
- Centre for Applied Legal Studies (CALS), Universidad Wits (Johannesburgo/Sudáfrica);
- Centre for European Constitutionalization and Security (CECS), Universidad de Copenhague (Copenhague/Europa);
- Centro de Derechos Humanos, Universidad de Pretoria (Pretoria/África);
- Centre for Law and Democracy (Halifax/global);
- Centre for Peace and Development Initiatives (Islamabad/Pakistán);
- Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Facultad de Derecho de Palermo (Buenos Aires/Argentina);
- Iniciativa de Derechos Humanos de la Commonwealth (Nueva Delhi/Commonwealth);
- Iniciativa Egipcia por los Derechos de la Persona (El Cairo/Egipto);
- Institute for Defence, Security and Peace Studies (Jakarta/Indonesia);
- Institute for Security Studies (Pretoria/África);
- Comisión Internacional de Juristas (Ginebra/global);
- National Security Archive (Washington DC/global);
- Open Democracy Advice Centre (Ciudad del Cabo/África del Sur); y
- Open Society Justice Initiative (Nueva York/global).

[131] Adicionalmente, Aidan Wills y Benjamin Buckland, del Centro de Ginebra para el Control de las Fuerzas Armadas, (DCAF) quienes no están afiliados con ningúna de las organizaciones mencionadas aquí, hicieron contribuciones significativas a la Parte V: Organismos que supervisan el sector de seguridad, a la Parte VI: Divulgación de información de interés público, y a la creación de los Principios en su totalidad.