PRINCÍPIOS GLOBAIS SOBRE SEGURANÇA NACIONAL E O DIREITO À INFORMAÇÃO

("OS PRINCÍPIOS DE TSHWANE")

concluídos em Tshwane, África do Sul
emitidos a 12 de Junho de 2013

INTRODUÇÃO

Estes Princípios foram desenvolvidos com o objectivo de fornecer orientação aos envolvidos na elaboração, revisão ou implementação de leis ou disposições relativas à autoridade do Estado para reter informações por razões de segurança nacional ou para punir a divulgação dessas informações.

Estes baseiam-se na legislação internacional (incluindo regional) e nacional, nas normas, boas práticas e nos escritos de especialistas.

Os Princípios abordam a segurança nacional – contrariamente a fornecer motivos para reter informações. Todas as outras razões públicas para limitar o acesso deverão pelo menos satisfazer estas normas.

Estes Princípios foram elaborados por 22 organizações e centros académicos (indicados no Anexo), em consulta com mais de 500 especialistas de mais de 70 países, em 14 reuniões realizadas em todo o mundo, facilitadas pela Open Society Justice Initiative (Iniciativa de Justiça de Sociedade Aberta) e em consulta com os quatro relatores especiais para a liberdade de expressão e/ou liberdade de imprensa e o relator especial para o anti-terrorismo e direitos humanos:

- o Relator Especial das Nações Unidas (ONU) para a Liberdade de Opinião e Expressão,
- o Relator Especial da ONU para o anti-terrorismo e os Direitos Humanos,
- o Relator Especial da Comissão Africana dos Direitos Humanos e dos Povos (ACHPR) para a Liberdade de Expressão e Acesso à Informação,
- o Relator Especial da Organização dos Estados Americanos (OAS) para a Liberdade de Expressão, e
- o Representante da Organização para a Segurança e a Cooperação na Europa (OSCE) para a Liberdade dos Meios de Comunicação Social.

CONTEXTO E FUNDAMENTAÇÃO

A segurança nacional e o direito do público a ser informado são muitas vezes vistos como interesses de sentidos opostos. Embora, por vezes, exista uma tensão entre o desejo de um governo em manter secretas as informações por razões de segurança nacional e o direito do público à informação detida pelas autoridades públicas, uma análise lúcida da história recente sugere que os interesses legítimos para a segurança nacional são, na prática, melhor protegidos quando o público está bem informado sobre as actividades do Estado, incluindo as realizadas para proteger a segurança nacional.

O acesso à informação, permitindo o escrutínio público da acção do Estado, não só protege contra o abuso por parte das autoridades públicas mas também permite que o povo desempenhe um papel na determinação das políticas do Estado e, deste modo, constitui um componente essencial da verdadeira segurança nacional, participação democrática e elaboração de políticas válidas. Para proteger o pleno exercício dos direitos humanos, em determinadas circunstâncias, pode ser necessário manter a informação em segredo para proteger os interesses legítimos relativos à segurança nacional.

Atingir o equilíbrio certo é um cenário tornado ainda mais complicado pelo facto dos tribunais de muitos países demonstrarem uma menor independência e uma maior deferência às reivindicações dos governos quando é invocada a segurança nacional. Esta deferência é reforçada por disposições na legislação sobre segurança de muitos países que activam excepções ao direito à informação, bem como às regras comuns do ónus da prova e dos direitos do acusado, perante uma demonstração mínima, ou mesmo a mera afirmação por parte do governo, de um risco para a segurança nacional. A invocação excessiva de preocupações de segurança nacional por parte de um governo pode comprometer seriamente as principais salvaguardas institucionais contra os abusos do governo: a independência dos tribunais, o Estado de Direito, a supervisão legislativa, a liberdade de imprensa e a abertura governamental.

Estes Princípios respondem aos desafios de longa data descritos acima, bem como ao facto de que, nos últimos anos, um número significativo de países por todo o mundo ter começado a adoptar ou a rever os regimes de classificação e as leis relacionadas. Esta tendência foi, por sua vez, provocada por diversos desenvolvimentos. Talvez o mais significativo tenha sido a rápida adopção das leis de acesso à informação, a partir da queda do Muro de Berlim, com o resultado de, à data de emissão destes Princípios, mais de 5,2 mil milhões de pessoas em 95 países por todo o mundo desfrutarem do direito de acesso à informação – pelo menos em termos legais, se não em termos práticos. As pessoas nesses países estão – muitas vezes pela primeira vez – a debater-se com a questão se, e em que circunstâncias, a informação pode ser mantida em segredo. Outros desenvolvimentos que contribuem para um aumento da legislação sobre segredos de Estado proposta foram as respostas dos governos contra o terrorismo ou a ameaça de terrorismo e um interesse na regulamentação por lei dos segredos de Estado no contexto dos processos de transição democrática.

PRINCÍPIOS GLOBAIS SOBRE SEGURANÇA NACIONAL E O DIREITO À INFORMAÇÃO

("OS PRINCÍPIOS DE TSHWANE")

concluídos em Tshwane, África do Sul
emitidos a 12 de Junho de 2013

PREÂMBULO

As organizações e os indivíduos envolvidos na elaboração dos presentes Princípios:

Relembrando que o acesso à informação detida pelo Estado é um direito de qualquer pessoa e, como tal, que esse direito deverá estar protegido por leis elaboradas com precisão, e com excepções estritamente concebidas, e pela supervisão desse direito por parte de tribunais independentes, entidades de supervisão parlamentar e outras entidades independentes;

Reconhecendo que os Estados podem ter um interesse legítimo em reter determinadas informações, incluindo por razões de segurança nacional, e destacando que atingir o equilíbrio adequado entre a divulgação e a retenção de informações é vital para uma sociedade democrática e essencial para a sua segurança, progresso, desenvolvimento e bem-estar, e para o pleno gozo dos direitos humanos e das liberdades fundamentais;

Afirmando que é imperativo, para que as pessoas possam ser capazes de monitorizar a conduta dos seus governos e participarem plenamente numa sociedade democrática, que tenham acesso à informação detida pelas autoridades públicas, incluindo informações relacionadas com a segurança nacional;

Observando que estes Princípios se baseiam na legislação e normas internacionais relacionadas com o direito do público ao acesso à informação detida pelas autoridades públicas e com outros direitos humanos, envolvendo a prática do Estado (como evidenciado, *inter alia*, nos julgamentos

em tribunais internacionais e nacionais), nos princípios gerais do direito reconhecidos pela comunidade das nações e nos escritos de especialistas;

Tendo em consideração as disposições relevantes da Declaração Universal dos Direitos Humanos, o Pacto Internacional sobre os Direitos Civis e Políticos, a Carta Africana dos Direitos Humanos e dos Povos, a Convenção Americana sobre Direitos Humanos, a Convenção Europeia sobre Direitos Humanos e a Convenção do Conselho da Europa sobre o Acesso a Documentos Oficiais;

Tendo igualmente em consideração a Declaração de Princípios sobre Liberdade de Expressão da Comissão Interamericana de Direitos Humanos; a Lei Modelo Interamericana sobre o Acesso à Informação Pública, a Declaração de Princípios sobre a Liberdade de Expressão em África e a Lei Modelo sobre o Acesso à Informação para África;

Relembrando a Declaração Conjunta de 2004 do Relator Especial da ONU para a Liberdade de Opinião e Expressão, do Representante da OSCE para a Liberdade dos Meios de Comunicação Social e do Relator Especial da Comissão Interamericana de Direitos Humanos para a Liberdade de Expressão; as Declarações Conjuntas de 2006, 2008, 2009 e 2010 destes três especialistas e do Relator Especial da Comissão Africana dos Direitos Humanos e dos Povos para a Liberdade de Expressão e Acesso à Informação; a Declaração Conjunta sobre o WikiLeaks de Dezembro de 2010 dos Relatores Especiais da ONU e Interamericanos; e o Relatório sobre Medidas Anti-terrorismo e Direitos Humanos, adoptado pela Comissão de Veneza em 2010;

Relembrando ainda os Princípios de Joanesburgo sobre a Segurança Nacional, Liberdade de Expressão e Acesso à Informação adoptados por um grupo de especialistas convocados pelo Artigo 19 em 1995, e os Princípios de Supervisão e Responsabilidade pelos Serviços de Segurança numa Democracia Constitucional elaborados em 1997 pelo Centro para os Estudos sobre Segurança Nacional (CNSS) e a Fundação de Helsínquia para os Direitos Humanos;

Observando que existem princípios internacionais — tal como os incluídos na Lei Modelo sobre o Acesso à Informação para África, os Princípios Orientadores da ONU sobre Empresas e os Direitos Humanos ("Princípios de Ruggie"), o Tratado sobre o Comércio de Armas, as Orientações da OCDE para as Empresas Multinacionais, e o Documento de Montreux sobre as obrigações legais internacionais e boas práticas relevantes para os Estados relativas a operações de empresas privadas militares e de segurança durante conflitos armados — que reconhecem a importância crítica do acesso à informação de, ou relacionada com, empresas comerciais em determinadas circunstâncias; e que alguns abordam expressamente a necessidade das empresas militares e de segurança privadas que operam no sector da segurança nacional tornarem pública determinada informação;

Observando que estes Princípios não se referem a normas concretas para a recolha de informações secretas, gestão de dados pessoais ou partilha de informações secretas que são abordadas pelas "boas práticas relativas aos quadros jurídicos e institucionais para os serviços de informações secretas e sua supervisão"[1] emitidas em 2010 por Martin Scheinin, à altura Relator Especial da ONU para a promoção e protecção dos direitos humanos e das liberdades fundamentais durante a luta contra o terrorismo, a pedido do Conselho dos Direitos Humanos da ONU;

1 Nota do tradutor: os textos indicados através de hiperligação poderão estar redigidos na língua inglesa.

Reconhecendo a importância da partilha eficaz de informações secretas entre os Estados, conforme sugerido pela Resolução 1373 do Conselho de Segurança da ONU;

Reconhecendo ainda que as barreiras à supervisão pública independente, criadas em nome da segurança nacional, aumentam o risco de poderem ocorrer condutas ilegais, corruptas e fraudulentas e não serem descobertas; e que violações de privacidade e de outros direitos individuais ocorrem frequentemente sob o manto de sigilo da segurança nacional;

Preocupados com os custos para a segurança nacional relativos ao excesso de classificação, incluindo a obstrução à partilha de informação entre agências governamentais e os seus aliados, a incapacidade de proteger segredos legítimos, a incapacidade de encontrar informação importante no meio da confusão, recolha repetitiva de informação por diversas agências e a sobrecarga dos responsáveis pela segurança;

Enfatizando que os Princípios se concentram no direito do público à informação, e que estes abordam os direitos à informação dos detidos, vítimas de violações dos direitos humanos e outras pessoas com acentuadas reivindicações a informações, apenas na medida em que esses direitos estejam intimamente relacionados com o direito do público à informação;

Reconhecendo que determinada informação, que não deverá ser retida por razões de segurança nacional, pode, apesar disso, ser potencialmente retida por várias outras razões reconhecidas pelo direito internacional – incluindo, por exemplo, as relações internacionais, a equidade dos processos judiciais, os direitos dos litigantes e a privacidade pessoal – sempre sujeitos ao princípio de que a informação só pode ser retida quando o interesse público em manter o sigilo da informação compensar claramente o interesse público no acesso à informação;

Desejando proporcionar orientações práticas para os governos, entidades legislativas e regulamentares, autoridades públicas, elaboradores de legislação, os tribunais, outras entidades de supervisão e a sociedade civil, relativamente a algumas das questões mais complicadas na intersecção da segurança nacional e do direito à informação, em particular aqueles que envolvem o respeito pelos direitos humanos e a responsabilidade democrática;

Esforçando-se por elaborar Princípios que tenham valor e aplicação universais;

Reconhecendo que os Estados enfrentam desafios muito diversos para equilibrar os interesses públicos na divulgação e a necessidade de sigilo para proteger os interesses legítimos para a segurança nacional, e que, embora os Princípios sejam universais, a sua aplicação prática pode responder às realidades locais, incluindo diversos sistemas jurídicos;

Recomendam que as entidades adequadas ao nível nacional, regional e internacional tomem medidas para disseminar e debater estes Princípios, e endossar, adoptar e/ou implementá-los, na medida do possível, com o objectivo de obter progressivamente a plena implementação do direito à informação, conforme estabelecido no Princípio 1.

DEFINIÇÕES

Nestes Princípios, salvo se o contexto o determinar de outro modo:

"**Empresa comercial no sector da segurança nacional**" significa uma pessoa jurídica que exerce ou exerceu qualquer transacção ou negócio no sector da segurança nacional, mas apenas nessa capacidade; quer como contratante ou prestador de serviços, instalações, pessoal ou produtos incluindo, entre outros, armamento, equipamento e informação secreta. Isto inclui empresas privadas militares e de segurança (PMSCs). Não inclui pessoas jurídicas organizadas como organizações sem fins lucrativos ou não governamentais.

"**Independente**" significa livre, em termos institucionais, financeiros e operacionais, da influência, orientação ou controlo do Executivo, incluindo todas as autoridades do sector da segurança.

"**Informação**" significa qualquer original ou cópia de material documental, independentemente das suas características físicas, e qualquer outro material corpóreo ou incorpóreo, apesar da forma ou do meio em que seja detido. Inclui, entre outros, os registos, correspondências, factos, opiniões, conselhos, memorandos, dados, estatísticas, livros, desenhos, planos, mapas, diagramas, fotografias, gravações audiovisuais, documentos, mensagens de e-mail, livros de registos, amostras, modelos e dados guardados em qualquer formato electrónico.

"**Informação de interesse público**" refere-se a informações que sejam de preocupação ou benefício para o público, não só do interesse individual e cuja divulgação seja "do interesse do público", por exemplo, porque é útil para a compreensão pública das actividades governamentais.

"**Interesse legítimo para a segurança nacional**" refere-se a um interesse, cujo objectivo genuíno e impacto principal é a protecção da segurança nacional, de modo compatível com a legislação internacional e nacional. (As categorias de informação cuja retenção possa ser necessária para proteger um interesse legítimo para a segurança nacional são estabelecidas no Princípio 9). Um interesse para a segurança nacional não é legítimo se o seu objectivo real ou impacto principal for proteger um interesse não relacionado com a segurança nacional, tal como a protecção do governo ou de funcionários em relação a embaraços ou à exposição de irregularidades; ocultação de informação sobre violações dos direitos humanos, qualquer outra violação das leis ou o funcionamento das instituições públicas; reforço ou perpetuar de um interesse, partido ou ideologia política em particular; ou a supressão de protestos legítimos.

"**Segurança nacional**" não é definido nestes Princípios. O Princípio 2 inclui uma recomendação de que a "segurança nacional" deve ser definida com precisão na legislação nacional, de modo consistente com as necessidades de uma sociedade democrática.

"**Autoridades públicas**" inclui todas as entidades dentro dos ramos executivo, legislativo e judicial em todos os níveis de governo, autoridades constitucionais e estatutárias, incluindo autoridades do sector da segurança; e entidades não-estatais que sejam propriedade ou controladas pelo governo, ou que sirvam como agentes do governo. O termo "Autoridades públicas" também inclui entidades privadas ou outras que realizem funções ou serviços públicos, ou operem com financiamento ou benefícios públicos substanciais, mas apenas

relativamente ao desempenho dessas funções, prestação de serviços ou utilização de financiamento ou benefícios públicos.

"**Funcionário público**" ou "**funcionário do Estado**" refere-se a actuais ou antigos empregados do Estado, contratantes e subcontratantes de autoridades públicas, incluindo no sector da segurança. "Funcionário público" ou "funcionário do Estado" também inclui pessoas empregadas por entidades não-estatais que são propriedade ou controladas pelo governo ou que funcionam como agentes do governo; e empregados de entidades privadas ou outras que realizem funções ou serviços públicos, ou operem com financiamento ou benefícios públicos substanciais, mas apenas relativamente ao desempenho dessas funções, prestação de serviços ou utilização de financiamento ou benefícios públicos.

"**Sanção**", quando usado como substantivo, refere-se a qualquer forma de punição ou prejuízo, incluindo medidas criminais, civis e administrativas. Quando usado como verbo, "sancionar" significa levar a cabo essa forma de punição ou prejuízo.

"**Sector da segurança**" é definido para incluir: (i) prestadores de serviços de segurança, incluindo, entre outros, as forças armadas, polícia e outras entidades de aplicação da lei, forças paramilitares e serviços de informações secretas e segurança (tanto militares como civis); e (ii) todas as entidades executivas, departamentos e ministérios responsáveis pela coordenação, controlo e supervisão dos prestadores de serviços de segurança.

PARTE I: PRINCÍPIOS GERAIS

Princípio 1: Direito à informação

(a) Todas as pessoas têm o direito de procurar, receber, usar e transmitir informações detidas ou em nome das autoridades públicas, ou a que as entidades públicas tenham o direito por lei a ter acesso.

(b) Os princípios internacionais também reconhecem que as empresas comerciais dentro do sector da segurança nacional, incluindo empresas privadas militares e de segurança, têm a responsabilidade de divulgar informações relativas às situações, actividades ou condutas de que se possam esperar, de modo razoável, ter impacto sobre o exercício dos direitos humanos.

(c) Todos os que tenham a obrigação de divulgar informação, de acordo com os Princípios 1(a) e 1(b), devem disponibilizar as informações mediante pedido, sujeito apenas às excepções limitadas determinadas por lei e necessárias para evitar danos específicos e identificáveis aos interesses legítimos, incluindo a segurança nacional.

(d) Apenas as autoridades públicas cujas responsabilidades específicas incluam a protecção da segurança nacional podem reivindicar a segurança nacional como fundamento para a retenção de informação.

(e) Qualquer reivindicação por parte de uma empresa comercial de segurança nacional para justificar a retenção de informação deve ser explicitamente autorizada ou confirmada por uma autoridade pública encarregada de proteger a segurança nacional.

Nota: o governo, e apenas o governo, tem a responsabilidade final pela segurança nacional e, sendo assim, só o governo pode impor que essa informação não deva ser divulgada se esta prejudicar a segurança nacional.

(f) As autoridades públicas também têm a obrigação de publicar, de forma proactiva, determinada informação de interesse público.

Princípio 2: Aplicação destes Princípios

(a) Estes Princípios aplicam-se ao exercício do direito de acesso à informação conforme identificado no Princípio 1, em que o governo afirme ou confirme que a divulgação de tal informação pode causar danos à segurança nacional.

(b) Dado que a segurança nacional é uma das razões públicas com maior peso para limitar a informação, quando as autoridades públicas reivindicam outras razões públicas para limitar o acesso – incluindo as relações internacionais, a ordem pública, a saúde e a segurança pública, a aplicação da lei, a futura disponibilização de aconselhamento gratuito e aberto, a formulação eficaz de políticas e os interesses económicos do Estado – devem, pelo menos, satisfazer as normas para a imposição de limitações ao direito de acesso à informação, estabelecidas nestes Princípios como relevantes.

(c) É uma boa prática para a segurança nacional, quando usada para limitar o direito à informação, que esteja definida com precisão no enquadramento jurídico de um país, de modo consistente com uma sociedade democrática.

Princípio 3: Requisitos para Limitar o Direito à Informação por Razões de Segurança Nacional

Nenhuma limitação ao direito à informação por razões de segurança nacional pode ser imposta, a menos que o governo possa demonstrar que: (1) a limitação (a) é determinada por lei e (b) é necessária numa sociedade democrática (c) destina-se a proteger um interesse legítimo para a segurança nacional; e (2) a lei proporciona as salvaguardas adequadas contra abusos, incluindo o escrutínio rápido, completo, acessível e eficaz da validade da limitação, por uma autoridade supervisora independente e com uma análise integral por parte dos tribunais.

(a) *Determinado por lei*. A lei deve ser acessível, inequívoca e elaborada de modo estrito e preciso para permitir que os indivíduos compreendam que informação pode ser retida, qual a que deve ser divulgada e que acções relacionadas com a informação se encontram sujeitas a sanções.

(b) *Necessário numa sociedade democrática*.

(i) A divulgação da informação deve implicar um risco verdadeiro e identificável de danos significativos para um interesse legítimo para a segurança nacional.
(ii) O risco de danos derivados da divulgação deve superar o interesse público na divulgação.
(iii) A limitação deve estar em conformidade com o princípio da proporcionalidade e deve ser o meio menos limitador disponível para protecção contra os danos.
(iv) A limitação não deve comprometer a própria razão de ser do direito à informação.

(c) *Protecção de um interesse legítimo para a segurança nacional*. As categorias restritas de informação que podem ser retidas por razões de segurança nacional deverão estar claramente dispostas na lei.

Notas: consulte a definição de "interesse legítimo para a segurança nacional" na secção de Definições acima. O Princípio 3(b) é tanto mais importante se a segurança nacional não for claramente definida na lei, conforme recomendado no Princípio 2.

"*Interesse público*" *não é definido nestes Princípios. Uma lista das categorias de interesse público particularmente elevado que devem ser publicadas, de forma proactiva, e nunca deverão ser retidas é estabelecida no Princípio 10. Uma lista de categorias de irregularidades que são de elevado interesse para o público, e que os funcionários do Estado devem e podem divulgar sem medo de retaliações, encontra-se estabelecida no Princípio 37.*

Ao equilibrar o risco de danos contra o interesse público na divulgação, deve ser tida em consideração a possibilidade de mitigar qualquer dano de divulgação, incluindo através dos meios que exijam as despesas razoáveis de financiamento. A seguir encontra-se uma lista de factores ilustrativa a ser tida em consideração para decidir se o interesse público na divulgação supera o risco de danos:

- *factores que favorecem a divulgação: a divulgação espera-se razoavelmente que (a) promova a discussão aberta de assuntos públicos, (b) reforce a responsabilidade governamental, (c) contribua para um debate positivo e informado sobre questões importantes ou assuntos de grande interesse, (d) promova a supervisão eficaz de despesas de financiamento público, (e) revele os motivos para uma decisão governamental, (f) contribua para a protecção do ambiente, (g) revele ameaças para a saúde ou segurança pública, ou (h) revele, ou ajude a estabelecer a responsabilidade por, violações dos direitos humanos ou do direito humanitário internacional.*
- *factores que favorecem a não-divulgação: a divulgação implicaria um risco verdadeiro e identificável de danos para um interesse legítimo para a segurança nacional;*
- *factores que são irrelevantes: a divulgação espera-se razoavelmente que (a) cause constrangimento a, ou uma perda de confiança no governo ou num funcionário, ou (b) enfraqueça um partido político ou ideologia.*

O facto que a divulgação pode causar danos para a economia de um país seria relevante para determinar se a informação pode ser retida por essa razão, mas não por razões de segurança nacional.

Princípio 4: Sobrecarga para a Autoridade Pública para Estabelecer a Legitimidade de Qualquer Limitação

(a) A sobrecarga na demonstração da legitimidade de qualquer limitação recai sobre a autoridade pública que procura reter a informação.

(b) O direito à informação deve ser interpretado e aplicado amplamente e quaisquer limitações devem ser interpretadas de forma restrita.

(c) Ao assumir esta sobrecarga, não é suficiente para uma autoridade pública simplesmente reivindicar que existe um risco de danos; a autoridade está obrigada ao dever de proporcionar razões específicas e concretas, para apoiar as suas reivindicações.

Nota: qualquer pessoa que procure o acesso à informação deverá ter uma oportunidade justa de contestar a base da reivindicação para uma avaliação do risco perante uma autoridade, tanto administrativa como judicial, de acordo com os Princípios 26 e 27.

(d) Em caso algum, a mera afirmação, tal como a emissão de um certificado por um ministro ou outro funcionário, no sentido de que a divulgação poderia causar danos à segurança nacional, pode ser considerada conclusiva em relação ao ponto para o qual ela é feita.

Princípio 5: Falta de Isenção por Parte de Qualquer Autoridade Pública

(a) Nenhuma autoridade pública – incluindo as instituições judiciárias, legislativas e de supervisão, as agências de informações secretas, forças armadas, polícia, outras agências de segurança, os gabinetes do chefe de Estado e do Governo e qualquer elemento dos gabinetes indicados – pode ser dispensada das exigências de divulgação.

(b) A informação não pode ser retida por razões de segurança nacional, simplesmente com base no facto de ter sido gerada por, ou partilhada com, um Estado ou entidade intergovernamental estrangeiros, ou uma autoridade pública específica ou uma unidade dentro de uma autoridade.

Nota: em relação à informação gerada por um Estado ou entidade intergovernamental estrangeiros, consulte o Princípio 9(a)(v).

Princípio 6: Acesso à Informação por Parte das Entidades de Supervisão

Todas as entidades de supervisão, provedoria e de recurso, incluindo os tribunais, deverão ter acesso a todas as informações, incluindo a informação sobre a segurança nacional, independentemente do nível de classificação, relevante para a sua capacidade de assumir as suas responsabilidades.

Nota: este Principio é desenvolvido no Princípio 32. Não se refere à divulgação ao público pelas entidades de supervisão. As entidades de supervisão deverão manter o sigilo sobre todas as informações que tenham sido legitimamente classificadas de acordo com estes Princípios, conforme estabelecido no Princípio 35.

Princípio 7: Recursos

Os Estados devem devotar os recursos adequados e adoptar outros passos necessários, tal como a emissão de regulamentos e a devida gestão dos arquivos, para garantir que estes Princípios são aplicados na prática.

Princípio 8: Estados de Emergência

Em casos de emergência pública, que ameacem a vida da nação e cuja existência esteja proclamada, de forma oficial e legal, em conformidade com o direito nacional e internacional, um Estado pode derrogar as suas obrigações relativas ao direito de procurar, receber e transmitir

informações apenas na medida do que for estritamente exigido pelas exigências da situação e apenas quando, e durante o tempo em que, a derrogação é consistente com as outras obrigações do Estado, nos termos do direito internacional, e não envolve qualquer tipo de discriminação.

Nota: determinados aspectos do direito de procurar, receber e transmitir informações e ideias são tão fundamentais para o exercício dos direitos inalienáveis, que deveriam ser sempre integralmente respeitados, mesmo em casos de emergência pública. Como exemplo não exaustivo, parte ou a totalidade da informação no Princípio 10 seria desta natureza.

PARTE II: INFORMAÇÃO QUE PODE SER RETIDA POR RAZÕES DE SEGURANÇA NACIONAL E INFORMAÇÃO QUE DEVE SER DIVULGADA

Princípio 9: Informação que Pode ser Retida Legitimamente

(a) As autoridades públicas podem limitar o direito do público ao acesso à informação por razões de segurança nacional do público, mas apenas se essas limitações estiverem de acordo com todas as restantes disposições destes Princípios, se a informação for detida por uma autoridade pública, e se a informação se enquadrar numa das seguintes categorias:

(i) Informação sobre planos de defesa e operações em curso, e capacidades durante o período de tempo em que a informação tem utilidade operacional.

Nota: a frase "durante o período de tempo em que a informação tem utilidade operacional" destina-se a exigir a divulgação de informação assim que essa informação deixar de revelar algo que possa ser usado pelos inimigos para entender a prontidão, capacidade ou planos do Estado.

(ii) Informação sobre a produção, capacidades ou utilização de sistemas de armamento e outros sistemas militares, incluindo sistemas de comunicações.

Nota: esta informação inclui dados tecnológicos e invenções, e informação sobre a produção, capacidades ou utilização. Informação sobre as rubricas orçamentais relativas a armamento e outros sistemas militares deve ser disponibilizada ao público. Consulte os Princípios 10C(3) e 10F. Para os Estados, é uma boa prática manter e publicar uma lista de controlo de armamento, conforme recomendado pelo Tratado sobre o Comércio de Armas em relação às armas convencionais. Também é uma boa prática publicar informação sobre armamento, equipamentos e número de tropas.

(iii) Informação sobre medidas específicas para proteger o território do Estado, as infra-estruturas essenciais ou as instituições nacionais essenciais (*institutions essentielles*) de ameaças ou do uso da força ou sabotagem, cuja eficiência depende do sigilo;

Nota: "Infra-estruturas críticas" refere-se a recursos, activos e sistemas estratégicos, físicos ou virtuais, tão vitais para o Estado que a destruição ou a incapacidade desses recursos, activos ou sistemas teria um impacto debilitante em termos de segurança nacional.

(iv) Informação respeitante, ou derivada, das operações, fontes e métodos dos serviços de informações secretas, na medida em que digam respeito a questões de segurança nacional; e

(v) Informação relativa a questões de segurança nacional que foi proporcionada por um Estado ou entidade intergovernamental estrangeiros, com uma expectativa expressa de confidencialidade; e outras comunicações diplomáticas, na medida em que dizem respeito a questões de segurança nacional.

Nota: é uma boa prática que essas expectativas sejam registadas por escrito.

Nota: na medida em que a informação específica sobre o terrorismo, e as medidas anti-terrorismo, é coberta por uma das categorias mencionadas acima, o direito do público ao acesso a essa informação pode estar sujeito a limitações por razões de segurança nacional, de acordo com esta e outras disposições dos Princípios. Ao mesmo tempo, alguma informação relativa ao terrorismo ou às medidas anti-terrorismo pode ter um interesse público particularmente elevado: consultar, por exemplo, os Princípios 10A, 10B e 10H(1).

(b) Para o Direito nacional, é uma boa prática o estabelecimento de uma lista exclusiva de categorias de informação que seja elaborada, pelo menos, de forma tão estrita como as categorias acima.

(c) Um Estado pode acrescentar uma categoria de informação à lista de categorias acima, mas apenas se a categoria for especificamente identificada e estritamente definida e a preservação do sigilo de informação for necessária para proteger um interesse legítimo para a segurança nacional, que está estabelecido na lei, conforme sugerido no Princípio 2(c). Ao propor a categoria, o Estado deverá explicar como a divulgação de informação na categoria causaria danos para a segurança nacional.

Princípio 10: Categorias de Informação com um Interesse Superior ou de Elevada Presunção a Favor da Divulgação

Algumas categorias de informação, incluindo as indicadas em baixo, têm um interesse público particularmente elevado, dada a sua especial importância para o processo de supervisão democrática e o Estado de Direito. Deste modo, existe uma presunção muito forte e, em alguns casos, um imperativo superior, que esta informação deva ser pública e divulgada de forma proactiva.

A informação nas categorias seguintes deverá beneficiar, pelo menos, de uma elevada presunção em favor da divulgação, e poderá ser retida por razões de segurança nacional, apenas nas circunstâncias mais excepcionais, e de um modo consistente com os restantes princípios, apenas por um período de tempo limitado, apenas nos termos da lei, e apenas se não existirem meios razoáveis através dos quais se consiga limitar os danos que estariam associados à divulgação. Para determinadas subcategorias de informação, especificadas abaixo como intrinsecamente sujeitas a um interesse público superior na divulgação, a retenção por razões de segurança nacional nunca pode ser justificada.

A. Violações dos Direitos Humanos ou do Direito Humanitário Internacional

(1) Existe um interesse público superior na divulgação de informação relativa a graves violações dos direitos humanos ou violações sérias do direito humanitário internacional, incluindo crimes de direito internacional e as violações sistemáticas e generalizadas dos direitos à liberdade e segurança pessoais. Essa informação não pode, em circunstância alguma, ser retida por razões de segurança nacional.

(2) A informação relativa a outras violações dos direitos humanos ou do direito humanitário está sujeita a uma elevada presunção da divulgação, e em qualquer caso, não pode ser retida por razões de segurança nacional, de uma forma que impediria a responsabilização pelas violações ou privar a vítima do acesso a uma solução eficaz.

(3) Quando um Estado está a passar por um processo transitório em termos de justiça, durante o qual é particularmente necessário que o Estado garanta a verdade, justiça, reparação e garantias de ausência de reincidência, existe um interesse público superior na divulgação para a sociedade como um todo de informação relativa às violações dos direitos humanos cometidas no regime anterior. Um governo sucessor deverá proteger e preservar imediatamente a integridade dos registos, e divulgar sem demora, todos os que contenham a informação que foi escondida por um governo anterior.

Nota: consulte o Princípio 21(c) relativo ao dever de procurar ou reconstruir informação sobre violações dos direitos humanos.

(4) No caso da existência de violações ser contestada ou suspeita, em vez de já ter sido estabelecida, este Princípio aplica-se à informação que, por si só ou em conjunto com outra informação, lance luz sobre a verdade relativamente às alegadas violações.

(5) Este Princípio aplica-se à informação sobre violações que ocorreram ou estejam a ocorrer, e aplica-se independentemente de as violações terem sido cometidas pelo Estado que detém a informação ou por outros.

(6) A informação relativa a violações abrangidas por este Princípio inclui, sem limitação, o seguinte:

(a) Uma descrição completa e todos os registos que mostrem os actos ou omissões que constituem as violações, bem como as datas e circunstâncias em que ocorreram, e, quando aplicável, a localização de todas as pessoas desaparecidas ou restos mortais.

(b) A identidade de todas as vítimas, desde que consistentes com os direitos de privacidade e outros direitos das vítimas, dos seus familiares e das testemunhas; e dados anónimos agregados e outros relativos aos seus números e características que possam ser relevantes para a salvaguarda dos direitos humanos.

Nota: os nomes e outros dados pessoais das vítimas, dos seus familiares e das testemunhas podem ser retidos da divulgação para o público em geral, conforme necessário para evitar que lhes sejam infligidos mais danos, se as pessoas em causa ou, no caso de pessoas falecidas, os seus familiares, solicitarem a retenção de modo expresso e voluntário, ou a retenção for, de outro modo, manifestamente compatível com os desejos da própria pessoa ou as necessidades específicas de grupos vulneráveis. Em relação a vítimas de violência sexual, deve ser solicitada a sua autorização expressa para a divulgação dos seus nomes e

outros dados pessoais. As vítimas menores (com idade inferior a 18 anos) não deverão ser identificadas para o público em geral. Este Princípio deverá ser interpretado tendo em consideração, no entanto, a realidade de que diversos governos, em várias ocasiões, ocultaram as violações dos direitos humanos do conhecimento público, invocando o direito à privacidade, incluindo o dos próprios indivíduos cujos direitos estão a ser ou foram violados de forma grosseira, sem ter em conta os verdadeiros desejos dos indivíduos afectados. Estas ressalvas, no entanto, não deverão impedir a publicação de dados agregados ou, de outra forma, anónimos.

(c) Os nomes das agências e indivíduos que cometeram ou foram, de outra forma, responsáveis pelas violações e, de um modo mais geral, quaisquer unidades do sector da segurança presentes no momento, ou de outra forma implicadas nas violações, bem como os seus superiores e comandantes, e informação relativa ao alcance do seu comando e controlo.

(d) Informação sobre as causas das violações e a falha na sua prevenção.

B. Salvaguardas para o Direito à Liberdade e Segurança da Pessoa, a Prevenção da Tortura e Outros Maus-Tratos e o Direito à Vida

A informação abrangida por este Princípio inclui:

(1) Leis e regulamentos que autorizem a privação da vida de uma pessoa por parte do Estado, e leis e regulamentos relativos à privação de liberdade, incluindo as que abordam as razões, procedimentos, transferências, tratamento ou condições de detenção das pessoas afectadas, incluindo os métodos de interrogatório. Existe um interesse público superior na divulgação dessas leis e regulamentos.

Notas: "Leis e regulamentos", como usado ao longo de todo o Princípio 10, inclui toda a legislação primária ou delegada, estatutos, regulamentos e portarias, bem como decretos ou ordens executivas emitidas por um presidente, primeiro-ministro, ministro ou outra autoridade pública, e as decisões judiciais, que possuam força de lei. O termo "Leis e regulamentos" também inclui todas as regras ou interpretações da lei que sejam consideradas como autorizadas pelos representantes executivos.

A privação de liberdade inclui qualquer forma de prisão, detenção, encarceramento ou internamento.

(2) A localização de todos os locais onde as pessoas foram privadas da sua liberdade, operados por ou em nome do Estado, bem como a identidade, e as acusações contra, ou os motivos para a detenção, de todas as pessoas privadas da sua liberdade, incluindo durante o conflito armado.

(3) Informação relativa à morte de qualquer pessoa sob detenção, e informação relativa a qualquer outra privação da vida de que um Estado seja responsável, incluindo a identidade da pessoa ou pessoas mortas, as circunstâncias da(s) sua(s) morte(s) e a localização dos seus restos mortais.

Nota: em circunstância alguma pode a informação ser retida por razões de segurança nacional, resultando na detenção secreta de uma pessoa, ou o estabelecimento e operação de locais de detenção secretos ou execuções secretas. Também não existem quaisquer circunstâncias em que o destino ou paradeiro de alguém privado da sua liberdade pelo, ou com a autorização, apoio ou consentimento do, Estado possa ser ocultado, ou de outra forma negado, dos familiares da pessoa ou de outras pessoas com um interesse legítimo no bem-estar da pessoa.

Os nomes e outros dados pessoais relativos a pessoas que foram privadas da sua liberdade, que morreram sob detenção, ou cujas mortes tenham sido causadas por agentes do Estado, podem ser retidos da divulgação para o público em geral, conforme for necessário para proteger o direito à privacidade se as pessoas em causa, ou os seus familiares no caso de pessoas falecidas, solicitarem a retenção de modo expresso e voluntário, e se a retenção for, de outra forma, consistente com os direitos humanos. A identidade das crianças que estão a ser privadas da liberdade não deve ser disponibilizada ao público em geral. Estas ressalvas, no entanto, não deverão impedir a publicação de dados agregados ou, de outra forma, anónimos.

C. Estruturas e Poderes do Governo

A informação abrangida por este Princípio inclui, sem limitação, o seguinte:

(1) A existência de todas as autoridades e subunidades militares, policiais, de segurança e dos serviços de informações secretas.

(2) As leis e regulamentos aplicáveis a essas autoridades, às suas entidades de supervisão e mecanismos de responsabilidade a nível interno e os nomes dos oficiais que lideram essas autoridades.

(3) A informação necessária para avaliar e controlar a despesa de financiamento público, incluindo os orçamentos globais brutos, as principais rubricas e a informação básica sobre despesas para essas autoridades.

(4) A existência e os termos de acordos bilaterais e multilaterais celebrados, e outros importantes compromissos internacionais assumidos pelo Estado em matéria de segurança nacional.

D. Decisões de Utilizar a Força Militar ou Adquirir Armas de Destruição Maciça

(1) A informação abrangida por este Princípio inclui as informações relevantes para uma decisão de enviar tropas de combate ou realizar outra acção militar, incluindo a confirmação do facto de realizar essa acção, a sua dimensão e âmbito gerais, e uma explicação sobre a fundamentação da mesma, bem como qualquer informação que demonstre que um facto indicado como parte da fundamentação pública estava errado.

Nota: a referência à dimensão e âmbito "gerais" de uma acção reconhece que, de um modo geral, deveria ser possível satisfazer o elevado interesse do público em ter acesso à informação relevante para a decisão de enviar tropas de combate sem revelar todos os pormenores dos aspectos operacionais da acção militar em questão (consultar Princípio 9).

(2) A posse ou aquisição de armas nucleares ou de outras armas de destruição maciça, por parte de um Estado, embora não necessariamente os pormenores sobre o seu fabrico ou capacidades operacionais, é uma questão de interesse público superior e não deve ser mantida em segredo.

Nota: este subprincípio não deve ser lido como aprovando, de modo algum, a aquisição dessas armas.

E. Vigilância

(1) O enquadramento jurídico global relativo à vigilância de todos os tipos, bem como os procedimentos a serem seguidos para autorizar a vigilância, a selecção dos alvos de vigilância e a utilização, partilha, armazenamento e destruição do material interceptado, devem estar acessíveis ao público.

Nota: esta informação inclui: (a) as leis que regem todas as formas de vigilância, tanto discreta como explícita, incluindo a vigilância indirecta, como através da elaboração de perfis e de extracção de dados, e os tipos de medidas de vigilância que podem ser usados; (b) os objectivos admissíveis da vigilância; (c) o limiar de suspeita necessário para iniciar ou continuar a vigilância; (d) as limitações na duração das medidas de supervisão; (e) os procedimentos de autorização e análise da utilização dessas medidas; (f) os tipos de dados pessoais que podem ser recolhidos e/ou processados para efeitos de segurança nacional; e (g) os critérios que se aplicam à utilização, retenção, eliminação e transferência destes dados.

(2) O público também deverá ter acesso à informação sobre entidades autorizadas a proceder à vigilância e estatísticas sobre a utilização de tal vigilância.

Notas: esta informação inclui a identificação de cada entidade governamental a quem é concedida uma autorização específica para realizar uma determinada vigilância todos os anos; o número de autorizações de vigilância atribuídas todos os anos a cada uma dessas entidades; a melhor informação disponível relativa ao número de indivíduos e ao número de comunicações sujeitas a vigilância todos os anos; e se qualquer vigilância foi realizada sem autorização específica e, se for o caso, por que entidade governamental.

O direito do público a ser informado não se estende necessariamente ao facto, ou aos pormenores operacionais, da vigilância realizada nos termos da lei e consistente com as obrigações em matéria de direitos humanos. Essa informação pode ser retida do público e das pessoas sujeitas à vigilância, pelo menos, até à conclusão do período de vigilância.

(3) Além disso, o público deverá ser plenamente informado em relação a qualquer vigilância ilegal. A informação sobre tal vigilância deve ser divulgada ao máximo, sem violar os direitos à privacidade das pessoas que foram sujeitas a vigilância.

(4) Estes Princípios abordam o direito de acesso à informação por parte do público e são, sem prejuízo dos direitos substantivos e processuais adicionais dos indivíduos que tenham sido, ou que acreditem que possam ter sido, sujeitos a vigilância.

Nota: é uma boa prática que as autoridades públicas sejam obrigadas a notificar as pessoas que foram submetidas a vigilância discreta (proporcionando, pelo menos, informação sobre o

tipo de medida que foi usada, as datas e a entidade responsável pela autorização da medida de vigilância), na medida em que isto pode ser feito sem colocar em risco as operações em curso, as fontes e os métodos.

(5) As elevadas presunções a favor da divulgação reconhecida por este Princípio não se aplicam em relação a informação que diga respeito exclusivamente à vigilância das actividades de governos estrangeiros.

Nota: a informação obtida através da vigilância discreta, incluindo as actividades de governos estrangeiros, deve ser objecto de divulgação nas circunstâncias identificadas no Princípio 10A.

F. Informação Financeira

A informação abrangida por este Princípio inclui informação suficiente para permitir que o público compreenda o lado financeiro do sector da segurança, bem como as regras que regem as finanças do sector da segurança. Esta informação deve incluir, entre outros:

(1) Orçamentos dos departamentos e agências com títulos de artigos;
(2) Demonstrações financeiras anuais com títulos de artigos;
(3) Regras e mecanismos de controlo de gestão financeira**;**
(4) Regras de aquisição; e
(5) Relatórios elaborados por instituições superiores de auditoria e outras entidades responsáveis por analisar os aspectos financeiros do sector da segurança, incluindo resumos de cada secção desses relatórios que são classificados (sigilosos).

G. Responsabilidade Relativa a Violações Constitucionais e Estatutárias e Outros Abusos de Poder

A informação abrangida por este Princípio inclui a informação sobre a existência, carácter e extensão das violações constitucionais ou estatutárias e de outros abusos de poder realizados pelas autoridades ou funcionários públicos.

H. Saúde Pública, Segurança Pública ou o Ambiente

A informação abrangida por este Princípio inclui:

(1) No caso de uma ameaça iminente ou real para a saúde pública, a segurança pública ou para o ambiente, toda a informação que possa permitir ao público compreender ou tomar medidas para impedir ou mitigar os danos decorrentes dessa ameaça, quer esta se deva a causas naturais ou a actividades humanas, incluindo por acções do Estado ou por acções de empresas privadas.

(2) Outra informação, actualizada periodicamente, sobre a exploração de recursos naturais, a poluição e os inventários de emissões, impactos ambientais de grandes obras públicas propostas ou existentes ou extracções de recursos e a avaliação de riscos e os planos de gestão para instalações particularmente perigosas.

PARTE III.A: REGRAS RELATIVAS À CLASSIFICAÇÃO E DESCLASSIFICAÇÃO DE INFORMAÇÃO

Princípio 11: Dever de Fundamentação para a Classificação de Informação

(a) Quer um Estado tenha ou não um processo de classificação formal, as autoridades públicas têm a obrigação de fundamentar a classificação de informação.

Nota: "Classificação" é o processo pelo qual os registos que contêm informação sensível são analisados e classificados para indicar quem pode ter acesso e como o registo deve ser tratado. É uma boa prática instituir um sistema formal de classificação, com o objectivo de reduzir a arbitrariedade e o excesso de retenções.

(b) As razões devem indicar a categoria estrita de informação, correspondendo a uma das categorias indicadas no Princípio 9 a que a informação pertence, e descrever os danos que poderiam resultar da divulgação, incluindo o seu nível de gravidade e o grau de probabilidade.

(c) Os níveis de classificação, se usados, deverão corresponder aos níveis e à probabilidade de danos identificados na justificação.

(d) Quando a informação é classificada, (i) deve ser afixada uma marca de protecção no registo que indica o nível, caso exista, e a duração máxima da classificação, e (ii) deve ser incluída uma declaração, justificando a necessidade de classificar a esse nível e durante esse período.

Nota: fornecer uma declaração a justificar cada decisão de classificação é recomendado porque faz com que os funcionários prestem atenção aos danos específicos que possam resultar da divulgação e porque facilita o processo de desclassificação e divulgação. A marcação parágrafo por parágrafo facilita ainda mais a consistência na divulgação de partes não classificadas de documentos.

Princípio 12: Acesso Público às Regras de Classificação

(a) O público deve ter a oportunidade de comentar sobre os procedimentos e normas que regem a classificação antes de estes entrarem em vigor.

(b) O público deve ter acesso aos procedimentos escritos e normas que regem a classificação.

Princípio 13: Autoridade para Classificar

(a) Apenas responsáveis especialmente autorizados ou designados, conforme definido na lei, podem classificar as informações. Se um funcionário não especificado acreditar que a informação deve ser classificada, a informação pode ser considerada como classificada por um período de tempo breve e expressamente definido, até que um funcionário especificado reveja a recomendação para classificação.

Nota: na ausência de disposições jurídicas que controlem a autoridade em termos de classificação, é uma boa prática, pelo menos, especificar essa autoridade de delegação num regulamento.

(b) A identidade da pessoa responsável por uma decisão de classificação deve ser detectável ou indicada no documento, a menos que existam razões convincentes para reter a identidade, para garantir a responsabilização.

(c) Estes responsáveis especificados pela lei deverão atribuir a autoridade de classificação original ao menor número de subordinados seniores que seja eficiente em termos administrativos.

Nota: é uma boa prática publicar informação sobre o número de pessoas que têm autoridade para classificar e o número de pessoas que têm acesso a informação classificada.

Princípio 14: Facilitar a Contestação Interna à Classificação

Os funcionários públicos, incluídos os associados ao sector da segurança, que acreditam que certa informação foi indevidamente classificada podem contestar a classificação dessa informação.

Nota: os funcionários do sector da segurança são assinalados como merecendo um incentivo especial para confrontar a classificação, devido à cultura acrescida de sigilo nas agências de segurança. O facto da maioria dos países não ter estabelecido ou indicado uma entidade independente para receber as queixas dos funcionários da segurança e a divulgação de informação sobre segurança resulta frequentemente em penalidades maiores do que a divulgação de outras informações.

Princípio 15: Dever de Preservar, Gerir e Manter a Informação sobre Segurança Nacional

(a) As autoridades públicas têm o dever de preservar, gerir e manter a informação de acordo com as normas internacionais.[2] A informação pode estar isenta de preservação, gestão e manutenção apenas de acordo com a lei.

(b) A informação deverá ser submetida a manutenção adequada. Os sistemas de arquivo deverão ser consistentes, transparentes (sem revelar informação legitimamente classificada) e abrangentes, para que pedidos de acesso específicos localizem toda a informação relevante, mesmo que a informação não seja divulgada.

(c) Cada entidade pública deverá criar e tornar pública, bem como rever e actualizar periodicamente, uma lista detalhada e precisa dos registos classificados que detém, salvo os documentos excepcionais, caso existam, cuja própria existência possa legitimamente ser retida em conformidade com o Princípio 19.

---

[2] Estas incluem: Conselho Internacional de Arquivos (ICA), *Princípios de Acesso aos Arquivos* (2012); ICA, *Declaração Universal sobre os Arquivos* (2010; subscrita pela UNESCO); Conselho da Europa, *Recomendação N.º R(2000)13 sobre uma política europeia de acesso aos arquivos* (2000); Antonio González Quintana, ICA, *Políticas de arquivo na protecção dos direitos humanos: uma versão actualizada e ampliada do relatório preparado pela UNESCO e o Conselho Internacional de Arquivos (1995), relacionada com a gestão de arquivos dos serviços de segurança do Estado de antigos regimes repressivos* (2009).

Nota: é uma boa prática actualizar estas listas anualmente.

Princípio 16: Prazos para Período de Classificação

(a) A informação pode ser retida por razões de segurança nacional apenas durante o tempo que for necessário para a protecção de um interesse legítimo para a segurança nacional. As decisões de reter informação devem ser revistas periodicamente para garantir que este Princípio é cumprido.

Nota: é uma boa prática que uma revisão seja exigida por lei, pelo menos a cada cinco anos. Diversos países exigem uma revisão após períodos mais curtos.

(b) O classificador deverá especificar a data, condições ou evento em que a classificação deverá prescrever.

Nota: é uma boa prática que este prazo, ou especificação de condições ou evento em que a classificação prescreva, seja sujeito a uma revisão periódica.

(c) Nenhuma informação pode permanecer como classificada por tempo indeterminado. O período máximo de classificação presumido por razões de segurança nacional deverá ser estabelecido por lei.

(d) A informação pode ser retida para além do prazo presumido apenas em circunstâncias excepcionais, em conformidade com uma nova decisão de retenção, feita por outro decisor, e estabelecendo um prazo alterado.

Princípio 17: Processos de Desclassificação

(a) A legislação nacional deverá identificar a responsabilidade do governo de coordenar, supervisionar e implementar as actividades de desclassificação do governo, incluindo a consolidação e a actualização periódica de orientações de desclassificação.

(b) Os procedimentos devem ser colocados em prática para identificar informação classificada de interesse público para desclassificação prioritária. Se a informação de interesse público, incluindo a informação que se enquadre nas categorias indicadas no Princípio 10, for classificada devido a excepcional sensibilidade, deve ser desclassificada o mais rapidamente possível.

(c) A legislação nacional deverá estabelecer os procedimentos para a desclassificação *em bloco* (em massa e/ou por amostragem).

(d) A legislação nacional deverá identificar períodos fixos para a desclassificação automática de diferentes categorias de informação classificada. Para minimizar o peso da desclassificação, os registos devem ser desclassificados automaticamente, sem revisão, sempre que possível.

(e) A legislação nacional deverá estabelecer um procedimento acessível e público para solicitar a desclassificação de documentos.

(f) Os documentos desclassificados, incluindo os que são desclassificados pelos tribunais ou por outras entidades de supervisão, provedoria ou de recurso, deverão ser divulgados de forma

proactiva, ou de outra forma disponibilizadas ao público (por exemplo, através da harmonização com a legislação nos arquivos nacionais, o acesso à informação ou ambos).

Nota: este Princípio não prejudica o pressuposto relativo a outras razões para reter informação, estabelecidas no parágrafo 15 no preâmbulo.

Nota: outras boas práticas incluem o seguinte:

- *consideração periódica da utilização de novas tecnologias nos processos de desclassificação; e*
- *consulta periódica com pessoas de competência profissional relativa ao processo de estabelecimento de prioridades de desclassificação, incluindo as desclassificações automáticas e* em bloco*.*

PARTE III.B: REGRAS RELATIVAS AO TRATAMENTO DOS PEDIDOS DE INFORMAÇÃO

Princípio 18: Dever de Considerar o Pedido Mesmo se a Informação Tiver Sido Classificada

O facto de a informação ter sido classificada não é decisivo na determinação de como responder a um pedido por essa informação. Pelo contrário, a autoridade pública que retém a informação deverá considerar o pedido de acordo com estes Princípios.

Princípio 19: Dever de Confirmar ou Negar

(a) Após a recepção de um pedido de informação, uma autoridade pública deverá confirmar ou negar se detém a informação solicitada.

(b) Se uma jurisdição permitir a possibilidade de, em circunstâncias extraordinárias, a própria existência ou não-existência de determinada informação poder ser classificada de acordo com o Princípio 3, então qualquer recusa em confirmar ou negar a existência da informação, em resposta a um pedido específico deverá basear-se numa demonstração de que a mera confirmação ou negação da existência da informação constituiria um risco de danos para uma categoria de informação distinta, especificada numa lei ou regulamento nacional como necessitando desse tratamento excepcional.

Princípio 20: Dever de Fundamentação para a Recusa por Escrito

(a) No caso de uma autoridade pública negar um pedido de informação, na totalidade ou parcialmente, deverá estabelecer, por escrito, as razões específicas para o fazer, de modo consistente com os Princípios 3 e 9, dentro do período de tempo especificado na lei para a resposta aos pedidos de informação.

Nota: consulte o Princípio 25 para o requisito de que o prazo para que uma resposta seja dada deverá estar estabelecido por lei.

(b) A autoridade também deverá fornecer ao requerente informação suficiente relativa ao(s) funcionário(s) que autorizou(autorizaram) a não divulgação e o processo para o fazer, a menos que fazê-lo acabaria por divulgar a informação classificada por si só e as vias de recurso, para permitir um exame de adesão da lei por parte da autoridade.

Princípio 21: Dever de Recuperar ou Reconstituir a Informação em Falta

(a) Quando uma autoridade pública é incapaz de localizar a informação em resposta a um pedido, e os registos que contêm essa informação deveriam ter sido mantidos, recolhidos ou produzidos, a autoridade deverá fazer os esforços razoáveis para recuperar ou reconstituir a informação em falta para uma potencial divulgação para o requerente.

Nota: este Princípio aplica-se a informação que não possa ser localizada, por qualquer razão, por exemplo por nunca ter sido recolhida, ter sido destruída ou não ser localizável.

(b) Um representante da autoridade pública deverá ser obrigado a indicar, sob juramento, e dentro de um período especificado estatutariamente e razoável, todos os procedimentos realizados para tentar recuperar ou reconstituir a informação para que esses procedimentos possam ser sujeitos a revisão judicial.

Nota: quando a informação que, por exigência da lei, deveria ser mantida não puder ser encontrada, a questão deve ser encaminhada para a polícia e as autoridades administrativas para investigação. O resultado da investigação deverá ser tornado público.

(c) O dever de recuperar ou reconstituir informação é particularmente forte (i) quando a informação é relativa a violações dos direitos humanos alegadamente grosseiras ou sistemáticas, e/ou (ii) durante uma transição para uma forma de governo democrática a partir de um governo caracterizado por violações generalizadas dos direitos humanos.

Princípio 22: Dever de Divulgar Partes de Documentos

As isenções de divulgação aplicam-se apenas a informação específica e não a documentos, ou outros registos, inteiros. Apenas a informação específica para a qual a validade de uma limitação tenha sido demonstrada ("informação isenta") pode ser retida. Quando um registo contém tanto informação isenta, como não-isenta, as autoridades públicas têm a obrigação de separar e divulgar a informação não-isenta.

Princípio 23: Dever de Identificar a Informação Retida

Uma autoridade pública que detenha informação que se recusa a divulgar deverá identificar essa informação da forma mais específica possível. No mínimo, a autoridade deverá divulgar a quantidade de informação que se recusa a divulgar, por exemplo, pela estimativa de um número de páginas.

Princípio 24: Dever de Fornecer Informação em Formatos Disponíveis

As autoridades públicas deverão fornecer informação no formato preferido do requerente, na medida do possível.

Nota: isto inclui, por exemplo, a obrigação das autoridades públicas tomarem as medidas adequadas para fornecer informação às pessoas com deficiência, em formatos e tecnologias acessíveis, atempadamente e sem custos adicionais, de acordo com a Convenção da ONU sobre as Pessoas com Deficiência.

Princípio 25: Prazos para Responder aos Pedidos de Informação

(a) Os prazos para responder aos pedidos, incluindo sobre o mérito, revisão interna, decisão por uma entidade independente (se disponível) e revisão judicial, deverão ser estabelecidos por lei e deverão ser tão curtos quanto seja possível em termos práticos.

Nota: é considerada uma boa prática, manter os requisitos estabelecidos por lei na maioria dos acessos às leis da informação, com prescrição após vinte dias úteis ou menos, conforme o prazo em que deva ser dada uma resposta substantiva. Quando os prazos para a resposta aos pedidos não forem estabelecidos por lei, o prazo não deverá ser superior a 30 dias para um pedido normal. As leis podem prever prazos diferentes, com o objectivo de ter em conta diferentes volumes e níveis de complexidade e a sensibilidade dos documentos.

(b) Prazos acelerados deverão aplicar-se quando existe uma necessidade demonstrada por informação com carácter de urgência, tal como onde a informação é necessária para proteger a vida ou a liberdade de uma pessoa.

Princípio 26: Direito a Reavaliar uma Decisão de Retenção de Informação

(a) Um requerente tem o direito a obter uma reavaliação rápida e de baixo custo, feita por uma autoridade independente, relativa a uma recusa em divulgar informação ou em questões relacionadas com o pedido.

Nota: uma recusa pode incluir uma recusa implícita ou silenciosa. As matérias sujeitas a uma revisão por uma autoridade independente incluem taxas, prazos e formatos.

(b) A autoridade independente deverá ter a competência e os recursos necessários para assegurar uma revisão eficaz, incluindo o pleno acesso a toda a informação relevante, mesmo no caso de informação classificada.

(c) Uma pessoa deverá ter o direito de obter a revisão independente e eficaz de todas as questões relevantes, feita por um tribunal competente.

(d) No caso de o tribunal proferir uma decisão de que reter informação é justificado, deverá disponibilizar publicamente os motivos específicos e a sua análise jurídica por escrito, salvo em circunstâncias extraordinárias, de modo consistente com o Princípio 3.

PARTE IV: ASPECTOS JUDICIAIS DA SEGURANÇA NACIONAL E DO DIREITO À INFORMAÇÃO

Princípio 27: Princípio Geral de Supervisão Judicial

(a) As invocações de segurança nacional não podem ser tidas em conta para comprometer o direito fundamental a um julgamento justo por um tribunal competente, independente e imparcial, estabelecido por lei.

(b) Quando uma autoridade pública procura reter informação invocando razões de segurança nacional, em qualquer processo jurídico, o tribunal deverá ter o poder de examinar a

informação para determinar se esta informação pode ser retida. Normalmente, um tribunal não deverá afastar uma contestação sem examinar a informação.

Nota: em conformidade com o Princípio 4(d), o tribunal não deverá confiar em resumos ou depoimentos que simplesmente afirmem a necessidade de sigilo, sem fornecer uma base de fundamentação para a afirmação.

(c) O tribunal deve assegurar que a pessoa que procura obter acesso pode, na medida do possível, conhecer e contestar o caso avançado pelo governo para reter a informação.

(d) Um tribunal deverá julgar a legalidade e propriedade da reivindicação de uma autoridade pública e pode obrigar à divulgação ou ordenar as medidas apropriadas no caso de uma não-divulgação parcial ou total, incluindo a dispensa de acusações em processos penais.

(e) O tribunal deverá avaliar de forma independente se a autoridade pública invocou devidamente qualquer base para a não divulgação; o facto de a classificação não dever ser conclusiva quanto ao pedido de não-divulgação da informação. Da mesma forma, o tribunal deverá avaliar a natureza de quaisquer danos reivindicados pela autoridade pública, a sua probabilidade de ocorrência e o interesse público na divulgação, em conformidade com as normas definidas no Princípio 3.

Princípio 28: Acesso Público aos Processos Judiciais

(a) A invocação de segurança nacional não pode ser tida em conta para comprometer o direito fundamental do público de acesso aos processos judiciais.

(b) Acórdãos do tribunal – estabelecendo todas as ordens de um tribunal e incluindo as conclusões essenciais, provas e fundamentação jurídica – deverão ser tornados públicos, salvo quando o interesse das crianças com idade inferior a dezoito anos exigir o contrário.

Notas: o direito internacional não permite a derrogação por razões de segurança nacional da obrigação de pronunciar as sentenças publicamente.

Os registos de processos do tribunal de menores não devem ser tornados públicos. Os registos de outros processos judiciais que envolvam crianças deverão normalmente eliminar os nomes e outras informações identificativas das crianças com idade inferior a dezoito anos.

(c) O direito do público de acesso à justiça deverá incluir o acesso público imediato a (i) fundamentação judicial, (ii) informação sobre a existência e a evolução dos casos, (iii) argumentos escritos apresentados em tribunal, (iv) audiências em tribunal e julgamentos, e (v) provas nos processos judiciais que formem a base de uma condenação, a menos que uma derrogação da mesma seja justificada de acordo com estes Princípios.

Nota: o direito internacional relativo às exigências de um julgamento justo permite aos tribunais excluírem a totalidade ou parte do público de uma audiência, por razões de segurança nacional numa sociedade democrática, bem como da moral, ordem pública, interesse da vida privada das partes ou para evitar o prejuízo dos interesses da justiça, desde que essas limitações sejam sempre necessárias e proporcionais.

(d) O público deverá ter a oportunidade de contestar qualquer reivindicação avaliada pela autoridade pública de que uma limitação no acesso do público aos processos judiciais seja estritamente necessária por razões de segurança nacional.

(e) No caso de o tribunal proferir uma decisão de que uma limitação ao livre acesso aos processos judiciais é justificada, este deverá disponibilizar publicamente os motivos específicos e a sua análise jurídica por escrito, salvo em circunstâncias extraordinárias, de modo consistente com o Princípio 3.

Notas: este Princípio não se destina a alterar a lei existente de um Estado em relação aos procedimentos preliminares a que o público normalmente não tem acesso. Aplica-se apenas quando o processo judicial permitiria, de outra forma, o acesso público e a tentativa de negar que o acesso se baseia numa alegação de segurança nacional.

O direito do público de acesso aos processos judiciais e aos materiais decorre da importância do acesso à promoção (i) da justiça e imparcialidade, real e percebida, dos processos judiciais, (ii) da conduta adequada e mais honesta das partes; e (iii) da maior precisão do comentário público.

Princípio 29: Acesso de Partes à Informação em Processos Penais

(a) O tribunal não pode proibir um arguido de comparecer ao seu julgamento por razões de segurança nacional.

(b) Em caso algum deverá uma condenação ou privação de liberdade ser baseada em provas que o acusado não tenha tido a oportunidade de analisar e refutar.

(c) No interesse da justiça, a autoridade pública deverá divulgar ao arguido e ao advogado do arguido as acusações contra uma pessoa e toda a informação necessária para garantir um julgamento justo, independentemente de a informação ser classificada, de modo consistente com os Princípios 3-6, 10, 27 e 28, incluindo uma consideração dos interesses públicos.

(d) Quando a autoridade pública se recusa a divulgar a informação necessária para garantir um julgamento justo, o tribunal deve suspender ou indeferir as acusações.

Nota: as autoridades públicas não deverão confiar em informação em seu benefício quando alegarem sigilo, embora possam decidir manter a informação em segredo e sofrer as consequências.

Nota: Os Princípios 29 e 30 estão incluídos nestes Princípios relativos ao acesso do público à informação, à luz do facto de que a revisão judicial, e respectivas divulgações no contexto da supervisão judicial, muitas vezes são meios importantes para a divulgação pública da informação.

Princípio 30: Acesso de Partes à Informação em Processos Civis

(a) Todas as queixas de retenção de informação por parte de uma autoridade pública num processo civil devem ser revistas, de um modo consistente com os Princípios 3-6, 10, 27 e 28, incluindo a consideração pelos interesses públicos.

(b) As vítimas de violações dos direitos humanos têm o direito a um recurso e reparação eficazes, incluindo a divulgação pública dos abusos sofridos. As autoridades públicas não deverão reter material informativo para as suas reivindicações de modo incompatível com este direito.

(c) O público também tem o direito à informação relativa a violações graves dos direitos humanos e violações sérias do direito humanitário internacional.

PARTE V: ENTIDADES QUE SUPERVISIONAM O SECTOR DA SEGURANÇA

Princípio 31: Estabelecimento de Entidades de Supervisão Independentes

Os Estados devem estabelecer, se ainda não o tiverem feito, as entidades de supervisão independentes para supervisionar as entidades do sector da segurança, incluindo as suas operações, regulamentos, políticas, finanças e administração. Essas entidades de supervisão deverão ser independentes em termos institucionais, operacionais e financeiros das instituições que estão mandatadas para supervisionar.

Princípio 32: Acesso Ilimitado à Informação Necessária para o Cumprimento do Mandato

(a) As entidades de supervisão independentes deverão ter acesso garantido legalmente a todas as informações necessárias para o cumprimento dos seus mandatos. Não deverão existir limitações a esse acesso, independentemente do nível de classificação ou da confidencialidade da informação, mediante a satisfação dos requisitos de segurança razoáveis do acesso.

(b) A informação a que as entidades de supervisão deveriam ter acesso inclui, mas não está limitada a:

(i) todos os registos, tecnologias e sistemas na posse das autoridades do sector de segurança, independentemente da forma ou meio, e se eles foram ou não criados por essa autoridade.
(ii) locais físicos, objectos e instalações; e
(iii) informação detida por pessoas que os supervisores consideram ser relevantes para as suas funções de supervisão.

(c) Qualquer obrigação dos funcionários públicos em manter o sigilo ou a confidencialidade não deverá impedi-los de fornecer informações para as instituições de supervisão. A prestação dessa informação não deve ser considerada uma violação de qualquer lei ou contrato que imponha essas obrigações.

Princípio 33: Poderes, Recursos e Procedimentos Necessários para Assegurar o Acesso à Informação

(a) As entidades de supervisão independentes devem ter os poderes legais adequados, para serem capazes de aceder e interpretar qualquer informação relevante que considerem necessária para cumprir os seus mandatos.

(i) No mínimo, esses poderes devem incluir o direito de questionar os membros actuais e antigos do ramo executivo e funcionários e contratantes das autoridades públicas, solicitar e inspeccionar os registos relevantes e inspeccionar os locais físicos e as instalações.

(ii) Também deve ser atribuído às entidades de supervisão independentes a competência para intimar essas pessoas e os registos e ouvir o depoimento sob juramento ou afirmação das pessoas consideradas como possuindo informação que é relevante para o cumprimento dos seus mandatos, com a plena cooperação das agências de aplicação da lei, quando necessário.

(b) As entidades de supervisão independentes, no tratamento da informação e de testemunhos convincentes, devem ter em consideração, *inter alia*, as leis de privacidade relevantes, bem como as protecções contra a auto-incriminação e outros requisitos do processo legal aplicável.

(c) As entidades de supervisão independentes devem ter acesso aos recursos financeiros, tecnológicos e humanos necessários que lhes permita identificar, aceder e analisar a informação que é relevante para o desempenho eficaz das suas funções.

(d) A lei deverá exigir às instituições do sector da segurança que prestem às entidades de supervisão independentes a cooperação que estas precisem para aceder e interpretar a informação requerida para o cumprimento das suas funções.

(e) A lei deverá exigir às entidades de supervisão independentes que façam divulgações proactivas e atempadas às instituições do sector da segurança sobre as categorias de informação específicas que os supervisores tenham determinado serem necessárias para a realização dos seus mandatos. Esta informação deverá incluir, entre outras, possíveis violações do direito e das normas de direitos humanos.

Princípio 34: Transparências das Entidades de Supervisão Independentes

A. Aplicabilidade do Acesso às Leis de Informação

As leis que regulam o cumprimento do direito público relativo ao acesso a informação detida por autoridades públicas deverão aplicar-se às entidades de supervisão do sector da segurança.

B. Elaboração de relatórios

(1) Deverá ser exigido por lei que as entidades de supervisão independentes produzam relatórios periódicos e que disponibilizem publicamente estes relatórios. Estes relatórios deverão incluir, no mínimo, a informação sobre a própria entidade de supervisão, incluindo o seu mandato, membros, orçamento, desempenho e actividades.

Nota: estes relatórios também deverão incluir informação sobre o mandato, estrutura, orçamento e actividades gerais de qualquer instituição do sector da segurança que não disponibilize, ela própria, essa informação publicamente.

(2) As entidades de supervisão independentes também deverão proporcionar versões públicas dos seus relatórios relativos aos estudos e investigações temáticos e específicos de cada caso, e deverão fornecer o máximo de informação possível relativamente a assuntos de interesse público, incluindo em relação às áreas indicadas no Princípio 10.

(3) Na elaboração dos seus relatórios públicos, as entidades de supervisão independentes deverão respeitar os direitos de todos os indivíduos interessados, incluindo o seu direito à privacidade.

(4) As instituições de supervisão independentes devem dar às instituições sujeitas à sua supervisão a oportunidade de reverem, atempadamente, todos os relatórios que devam ser tornados públicos, de forma a permitir que levantem preocupações sobre a inclusão de material que possa ser classificado. A decisão final relativa ao que deverá ser publicado deve caber à própria entidade de supervisão.

C. Cobertura e Acessibilidade

(1) A base jurídica para as entidades de supervisão, incluindo os seus mandatos e poderes, deverá estar disponível publicamente e facilmente acessível.

(2) As entidades de supervisão independentes deverão criar mecanismos e instalações para que pessoas analfabetas, que falem línguas minoritárias ou tenham deficiência visual ou auditiva acedam à informação sobre o seu trabalho.

(3) As entidades de supervisão independentes deverão proporcionar uma série de mecanismos de acesso livre através dos quais o público, incluindo pessoas em locais geograficamente remotos, possam ter facilidade em estabelecer contacto com elas e, no caso de entidades que tratem de queixas, apresentar queixas ou registar preocupações.

(4) As entidades de supervisão independentes deverão ter mecanismos que possam preservar eficazmente a confidencialidade das queixas e o anonimato do queixoso.

Princípio 35: Medidas para Proteger Informação Tratada pelas Entidades de Supervisão do Sector da Segurança

(a) A lei deve exigir às entidades de supervisão independentes que implementem todas as medidas necessárias para proteger a informação na sua posse.

(b) Os legisladores deverão ter o poder de decidir se (i) os membros das comissões de supervisão legislativa, e (ii) os líderes e membros de entidades de supervisão não-legislativa independentes devem estar sujeitos a uma verificação de segurança antes da sua nomeação.

(c) Sempre que seja solicitada uma verificação de segurança, esta deve ser realizada (i) atempadamente, (ii) de acordo com os princípios estabelecidos, (iii) livre de todas as tendências ou motivações políticas, e (iv) sempre que possível, por uma instituição que não esteja sujeita a supervisão pela entidade cujos membros/funcionários estão a ser verificados.

(d) Sujeito aos Princípios das Partes VI e VII, os membros ou funcionários das entidades de supervisão independentes que divulguem material classificado ou, de outra forma, confidencial fora do âmbito dos mecanismos de elaboração de relatórios normais da entidade, deverão ser sujeitos aos processos administrativos, civis ou penais adequados.

Princípio 36: Autoridade do Legislador para Tornar Pública a Informação

O legislador deverá ter o poder de divulgar qualquer informação ao público, incluindo informação de que o ramo executivo reivindique o direito de reter por razões de segurança nacional, caso considere apropriado fazê-lo de acordo com os procedimentos que deverá estabelecer.

PARTE VI: DIVULGAÇÕES DE INTERESSE PÚBLICO POR FUNCIONÁRIOS PÚBLICOS

Princípio 37: Categorias de Irregularidades

A divulgação de informação por funcionários públicos, independentemente da sua classificação, que denuncie irregularidades que se enquadrem numa das seguintes categorias deve ser considerada como tratando-se de uma "divulgação protegida" se estiver em conformidade com as condições estabelecidas nos Princípios 38-40. Uma divulgação protegida pode referir irregularidades que tenham ocorrido, estejam a ocorrer ou seja provável que ocorram.

(a) delitos penais;
(b) violações dos direitos humanos;
(c) violações do direito humanitário internacional;
(d) corrupção;
(e) perigos para a saúde e segurança públicas;
(f) perigos para o ambiente;
(g) abuso de cargo público;
(h) erros judiciais;
(i) má gestão ou desperdício de recursos;
(j) retaliação pela divulgação de quaisquer irregularidades das categorias indicadas acima; e
(k) ocultação deliberada de qualquer questão que se enquadre numa das categorias anteriores.

Princípio 38: Razões, Motivação e Provas para Divulgações de Informação Denunciando Irregularidades

(a) A lei deverá proteger da retaliação, conforme definido no Princípio 41, os funcionários públicos que façam divulgações de informação que denunciem irregularidades, independentemente de a informação ser classificada ou, de outra forma, confidencial, desde que, no momento da divulgação:

(i) a pessoa que faz a divulgação tivesse motivos razoáveis para acreditar que a informação divulgada parecia mostrar irregularidades que se enquadram numa das categorias estabelecidas no Princípio 37; e
(ii) a divulgação está em conformidade com as condições estabelecidas nos Princípios 38-40.

(b) A motivação para a divulgação protegida é irrelevante, salvo se for provado que a divulgação é conscientemente falsa.

(c) Não deverá ser exigido a uma pessoa que faz uma divulgação protegida que apresente provas ou que suporte o ónus da prova em relação à divulgação.

Princípio 39: Procedimentos para Fazer e Responder a Divulgações Protegidas Internamente ou a Entidades de Supervisão

A. Divulgações Internas

A lei deve exigir que as autoridades públicas estabeleçam procedimentos internos e designem pessoas para a recepção de divulgações protegidas.

B. Divulgações a Entidades de Supervisão Independentes

(1) Os Estados devem também estabelecer ou identificar entidades independentes para receber e investigar as divulgações protegidas. Essas entidades devem ser independentes, em termos institucionais e operacionais, do sector da segurança e de outras autoridades relativamente às quais possam ser feitas as divulgações, incluindo do ramo executivo.

(2) Os funcionários públicos deverão ser autorizados a fazer divulgações protegidas às entidades de supervisão independentes ou a outra entidade competente para investigar o assunto sem antes precisar de fazer a divulgação internamente.

(3) A lei deverá garantir que as entidades de supervisão independentes tenham acesso a toda a informação relevante e dar-lhes os poderes de investigação necessários para garantir esse acesso. Estes poderes deverão incluir os poderes de intimação e o poder de exigir que o depoimento seja dado sob juramento ou afirmação.

C. Obrigações das Entidades Internas e das Entidades de Supervisão Independentes que Recebem as Divulgações

Se uma pessoa fizer uma divulgação protegida, conforme definido no Princípio 37, internamente ou a uma entidade de supervisão independente, a entidade que receber a divulgação deve ser obrigada a:

(1) investigar a alegada irregularidade e tomar medidas imediatas com o objectivo de resolver os assuntos num período de tempo legalmente determinado, ou, após ter consultado a pessoa que fez a divulgação, encaminhá-la para uma entidade que esteja autorizada e seja competente para a investigar;
(2) proteger a identidade do funcionário público que procure fazer envios confidenciais; os envios anónimos deverão ser considerados pelos seus méritos;

(3) proteger a informação divulgada e o facto de uma divulgação ter sido feita, salvo na medida em que seja necessária uma divulgação adicional de informação para resolver a irregularidade; e
(4) notificar a pessoa que faz a divulgação da evolução e conclusão de uma investigação e, na medida do possível, os passos dados ou as recomendações feitas.

Princípio 40: Protecção de Divulgações ao Público

A lei deverá proteger da retaliação, conforme definido no Princípio 41, as divulgações ao público de informação relativa a irregularidades, conforme definido no Princípio 37, se a divulgação cumprir os seguintes critérios:

(a) (1) A pessoa fez uma divulgação da mesma informação, ou de informação substancialmente semelhante, internamente e/ou a uma entidade de supervisão independente, e:
(i) a entidade a que a divulgação foi feita recusou-se ou falhou em investigar a divulgação de forma eficaz, em conformidade com as normas internacionais aplicáveis; ou
(ii) a pessoa não recebeu um resultado razoável e adequado dentro de um período de tempo razoável e definido por lei.

OU

(2) A pessoa acreditava razoavelmente que existia um risco significativo de, ao fazer a divulgação internamente e/ou a uma entidade de supervisão independente, isso resultasse na destruição ou ocultação de provas, interferência com uma testemunha, ou retaliação contra a pessoa ou terceiros;

OU

(3) Não houve uma entidade interna ou entidade de supervisão independente estabelecida a que pudesse ter sido feita uma divulgação;

OU

(4) A divulgação relacionada com um acto ou omissão que constituiu um risco de perigo sério e iminente para a vida, a saúde e a segurança das pessoas ou para o ambiente.

E

(b) A pessoa que faz a divulgação só divulgou a quantidade de informação que era razoavelmente necessária para revelar a irregularidade.

Nota: se, durante o processo de divulgação da informação denunciando irregularidades, uma pessoa também divulgar documentos que não sejam relevantes para a denúncia da irregularidade, essa pessoa deverá, ainda assim, ser protegida da retaliação, a menos que os danos da divulgação superem qualquer interesse público na divulgação.

E

(c) A pessoa que faz a divulgação acreditou razoavelmente que o interesse público em ter a informação revelada superou quaisquer danos para o interesse público que resultariam do facto de ter sido feita a divulgação.

Nota: o teste de "acreditar razoavelmente" é um teste misto objectivo-subjectivo. A pessoa deve realmente ter tido a convicção (subjectivamente) e deve ter-lhe sido razoável fazê-lo (objectivamente). Se contestada, a pessoa pode precisar de defender a razoabilidade da sua convicção e, em última instância, cabe a um tribunal independente determinar se este teste foi satisfeito, de modo a classificar a divulgação para protecção.

Princípio 41: Protecção contra a Retaliação por Fazer a Divulgação de Informação Denunciando Irregularidades

A. Imunidade da Responsabilidade Civil e Criminal para Divulgações Protegidas

Uma pessoa que tenha feito uma divulgação, em conformidade com os Princípios 37-40, não deverá ser sujeita a:

(1) Processos penais, incluindo, entre outros, um processo pela divulgação de informação classificada ou, de outra forma, confidencial; ou
(2) Processos cíveis relacionadas com a divulgação de informação classificada ou, de outra forma, confidencial, incluindo, entre outras, as tentativas de reivindicar acções de indemnização e de difamação.

B. Proibição de Outras Formas de Retaliação

(1) A lei deverá proibir a retaliação contra qualquer pessoa que tenha feito, seja suspeito de ter feito, ou possa fazer uma divulgação, em conformidade com os Princípios 37-40.

(2) As formas proibidas de retaliação incluem, entre outras, o seguinte:

(a) As medidas administrativas ou punições, incluindo, entre outros: cartas de reprimenda, investigações de retaliação, despromoção, transferência, reatribuição de tarefas, não-promoção, despedimento do funcionário, acções prováveis ou destinadas a prejudicar a reputação de uma pessoa, ou a suspensão ou revogação de uma autorização de segurança;
(b) Danos ou assédio físico ou moral; ou
(c) Ameaças de qualquer um dos indicados acima.

(3) As medidas tomadas contra indivíduos que não a pessoa que fez a divulgação podem, em determinadas circunstâncias, constituir uma retaliação proibida.

C. Investigação de Retaliação por uma Entidade de Supervisão Independente e as Autoridades Judiciais

(1) Qualquer pessoa deverá ter o direito de denunciar a uma entidade de supervisão independente e/ou a uma autoridade judicial qualquer medida de retaliação, ou a ameaça de retaliação, relacionada com divulgações protegidas.

(2) As entidades de supervisão independentes devem ser obrigadas a investigar uma retaliação ou a ameaça de retaliação denunciada. Essas entidades também devem ter a capacidade de lançar investigações na ausência de uma denúncia de retaliação.

(3) As entidades de supervisão independentes deverão ter os poderes e recursos para investigar, de modo eficaz, qualquer retaliação reivindicada, incluindo os poderes para intimar pessoas e registos e ouvir testemunhos sob julgamento ou afirmação.

(4) As entidades de supervisão independentes devem fazer todos os esforços para garantir que os processos referentes à retaliação são justos e de acordo com as normas de processo adequadas.

(5) As entidades de supervisão independentes deverão ter a autoridade para exigir que a autoridade pública relevante tome medidas correctivas ou de restauração, incluindo, entre outras, a reintegração; reafectação; e/ou o pagamento dos honorários de advogados, outros custos razoáveis, salários retroactivos e benefícios associados, despesas de viagem, e/ou indemnizações compensatórias.

(6) As entidades de supervisão independentes também deverão ter a autoridade para ordenar a uma autoridade pública que adopte medidas de retaliação.

(7) Essas entidades deverão completar a sua investigação sobre a retaliação denunciada, num período de tempo razoável e definido por lei.

(8) Essas entidades deverão notificar as pessoas relevantes, pelo menos, para a conclusão de uma investigação e, na medida do possível, os passos dados ou as recomendações feitas.

(9) As pessoas também poderão recorrer perante uma autoridade judicial relativamente a uma determinação de que as acções de resposta à divulgação não constituem uma retaliação, ou relativamente a medidas correctivas ou de restauração efetuadas pela entidade de supervisão independente.

D. Ónus da Prova

Se uma autoridade pública tomar qualquer acção adversa contra qualquer pessoa, cabe à autoridade o ónus de demonstrar que a acção não estava relacionada com a divulgação.

E. Sem Renúncia a Direitos e Meios de Recurso

Os direitos e meios de recurso previstos ao abrigo dos Princípios 37-40 não podem ser renunciados ou limitados por qualquer acordo, política, formas ou condições de emprego, incluindo por qualquer acordo de arbitragem pré-litigioso. Qualquer tentativa de renunciar ou limitar esses direitos e meios de recurso deverá ser considerada nula.

Princípio 42: Incentivar e Facilitar Divulgações Protegidas

Os Estados devem incentivar os funcionários públicos a fazerem divulgações protegidas. Para facilitar essas divulgações, os Estados devem exigir a todas as autoridades públicas que emitam directrizes para dar efeito aos Princípios 37-42.

Nota: tais directrizes deverão proporcionar, no mínimo: (1) conselhos relativos aos direitos e/ou responsabilidades para divulgar as irregularidades; (2) os tipos de informação que devem ou podem ser divulgados; (3) procedimentos necessários para fazer essas divulgações; e (4) protecções estabelecidas por esta lei.

Princípio 43: Defesa do Interesse Público por Funcionários Públicos

(a) Sempre que os funcionários públicos possam estar sujeitos a processos penais ou civis, ou sanções administrativas, relacionadas com o facto de terem feito uma divulgação de informação de outra forma não protegida ao abrigo destes Princípios, a lei deverá estipular uma defesa do interesse público se o interesse público na divulgação da informação em questão superar o interesse público na não-divulgação.

Nota: este Princípio aplica-se a todas as divulgações de informação que ainda não estejam protegidas, seja pelo facto da informação não se enquadrar em nenhuma das categorias sublinhadas no Princípio 37 ou pela divulgação conter informações que se enquadram numa das categorias destacadas no Princípio 37, mas não foi feito de acordo com os procedimentos descritos nos Princípios 38-40.

(b) Ao decidir se o interesse público na divulgação supera o interesse público na não-divulgação, as autoridades de acusação e judiciais deverão ter em conta:

(i) se o grau de divulgação foi o razoavelmente necessário para divulgar a informação de interesse público;
(ii) o grau e o risco de danos para o interesse público causados pela divulgação;
(iii) se a pessoa tinha motivos razoáveis para acreditar que a divulgação seria do interesse público;
(iv) se a pessoa tentou fazer uma divulgação protegida através dos procedimentos internos e/ou de uma entidade de supervisão independente e/ou para o público, em conformidade com os procedimentos descritos nos Princípios 38-40; e
(v) a existência de circunstâncias exigentes que justifiquem a divulgação.

Nota: qualquer lei que estabeleça sanções penais para a divulgação não autorizada de informação deverá ser consistente com o Princípio 46(b). Este Princípio não se destina a limitar quaisquer direitos de liberdade de expressão já disponíveis para os funcionários públicos ou qualquer das protecções concedidas nos termos dos Princípios 37-42 ou 46.

PARTE VII: LIMITES SOBRE MEDIDAS PARA SANCIONAR OU LIMITAR A DIVULGAÇÃO DE INFORMAÇÃO AO PÚBLICO

Princípio 44: Protecção Contra Penalidades pela Divulgação Razoável e de Boa-fé por Responsáveis pela Informação

Pessoas com a responsabilidade de responder aos pedidos de informação do público não devem ser sancionadas por divulgarem informação que acreditem, de modo razoável e em boa-fé, poder ser divulgada em conformidade com a lei.

Princípio 45: Penalidades pela Destruição de, ou Recusa em Divulgar, Informação

(a) Os funcionários públicos devem estar sujeitos a penalidades por destruírem ou interferirem deliberadamente com a informação com a intenção de negar o acesso público à mesma.

(b) Se um tribunal ou entidade independente tiver ordenado que a informação seja divulgada, e a informação não for divulgada dentro de um prazo razoável, a autoridade oficial e/ou pública responsável pela não-divulgação deverá estar sujeita às sanções apropriadas, a menos que seja interposto um recurso em conformidade com os procedimentos estabelecidos por lei.

Princípio 46: Limitações de Penalidades Criminais para a Divulgação de Informação por Funcionários Públicos

(a) A divulgação pública da informação por funcionários públicos, mesmo se não estiver protegida pela Parte VI, não deve estar sujeita a penalidades penais, embora possa estar sujeita a sanções administrativas, tal como a perda da autorização de segurança ou mesmo a rescisão do trabalho.

(b) Se, no entanto, a lei impõe penalidades penais para a divulgação não autorizada de informação ao público, ou a pessoas com a intenção de que a informação será tornada pública, as seguintes condições deverão aplicar-se:

(i) As penalidades penais deverão ser aplicadas apenas para a divulgação de categorias estritas de informação que estão claramente estabelecidas na lei;

Nota: se o direito nacional prever categorias de informação cuja divulgação pudesse estar sujeita a penalidades criminais, deveriam ser semelhantes ao seguinte em termos de especificidade e impacto para a segurança nacional: dados tecnológicos sobre as armas nucleares; fontes, códigos e métodos de informações secretas; códigos diplomáticos; identidades de agentes secretos; e propriedade intelectual em que o governo tem um interesse de propriedade e conhecimento do que poderia provocar danos para a segurança nacional.

(ii) A divulgação deve implicar um risco verdadeiro e identificável de causar danos significativos;

(iii) Qualquer penalidade criminal, conforme estabelecida pela lei e conforme aplicada, deve ser proporcional aos danos causados; e

(iv) A pessoa deveria poder invocar a defesa do interesse do público, conforme destacado no Princípio 43.

Princípio 47: Protecção Contra Sanções pela Posse e Disseminação de Informação Classificada por Pessoas que não são Funcionários Públicos

(a) Uma pessoa que não seja um funcionário do Estado não pode ser sancionada pela recepção, posse ou divulgação ao público de informação classificada.

(b) Uma pessoa que não seja um funcionário do Estado não pode ser sujeita a acusações de conspiração ou outros crimes, com base no facto de ter procurado ou divulgado a informação.

Nota: este Princípio tem como objectivo impedir acções penais pela aquisição ou reprodução de informação. No entanto, este Princípio não pretende impedir a acusação de uma pessoa por outros crimes, como roubo ou chantagem, cometidos no decorrer da procura ou obtenção da informação.

Nota: a divulgação a terceiros funciona como um importante correctivo para a sobreclassificação disseminada.

Princípio 48: Protecção das Fontes

Nenhuma pessoa que não seja um funcionário do Estado deverá ser forçada a revelar uma fonte confidencial ou materiais não publicados em qualquer investigação relacionada com a divulgação não autorizada de informação à imprensa ou ao público.

Nota: este Princípio refere-se apenas a investigações relativas à divulgação não autorizada de informação e não a outros crimes.

Princípio 49: Restrição Anterior

(a) As restrições anteriores contra a publicação, no interesse de proteger a segurança nacional, deverão ser proibidas.

Nota: as restrições anteriores são ordens emitidas por entidades judiciais ou outros organismos estatais, proibindo a publicação de material específico já na posse de uma pessoa que não seja um funcionário público.

(b) Se a informação tem sido de um modo geral disponibilizada ao público, por qualquer meio, quer seja legal ou não, qualquer tentativa para tentar impedir uma publicação posterior da informação, no formato em que já é do domínio público, é presumivelmente inválida.

Nota: "Geralmente disponível" é entendido como significando que a informação foi suficientemente divulgada e que não existem medidas práticas que pudessem ser tomadas para manter a informação em segredo.

PARTE VIII: CONCLUSÃO DOS PRINCÍPIOS

Princípio 50: Relação Destes Princípios com Outras Normas

Nada nos presentes Princípios deve ser interpretado como restringindo ou limitando qualquer direito à informação reconhecido pela legislação ou normas internacionais, regionais ou nacionais, ou por quaisquer disposições de legislação nacional ou internacional, que dariam uma maior protecção para a divulgação de informação por parte de funcionários públicos ou outros intervenientes.

Anexo: Organizações Parceiras

As seguintes 22 organizações contribuíram significativamente para a elaboração dos Princípios, e estão empenhadas em trabalhar para divulgar, publicitar e ajudar a implementá-los.[3] Depois do nome de cada uma das organizações está a cidade, se for caso, em que estas estão sediadas e o país ou região em que trabalham. As organizações que realizem trabalhos substanciais em três ou quatro regiões encontram-se listadas como "global".

- Centro Africano de Liberdade de Informação (Kampala/África);
- Fórum de Supervisão Civil da Polícia Africana (APCOF) (Cidade do Cabo/África);
- Alianza Regional por la Libre Expresión e Información (Américas);
- Amnistia Internacional (Londres/global);
- Artigo 19, a Campanha Global pela Liberdade de Expressão (Londres/global);
- Fórum Asiático para os Direitos Humanos e o Desenvolvimento (Fórum Ásia) (Banquecoque/Ásia);
- Centro para os Estudos sobre Segurança Nacional (Washington DC/Estados Unidos);
- Universidade Central Europeia (Budapeste/Europa);
- Centro para Estudos Jurídicos Aplicados (CALS), Universidade de WITS (Joanesburgo/África do Sul);
- Centro para a Constitucionalização e a Segurança Europeias (CECS), Universidade de Copenhaga (Copenhaga/Europa);
- Centro para os Direitos Humanos, Universidade de Pretória (Pretória/África);
- Centro para a Lei e a Democracia (Halifax/global);
- Centro para as Iniciativas de Paz e Desenvolvimento (Islamabad/Paquistão);
- Centro para Estudos sobre a Liberdade de Expressão e o Acesso à Informação (CELE), Faculdade de Direito da Universidade de Palermo (Buenos Aires/Argentina);
- Iniciativa para os Direitos Humanos da Commonwealth (Nova Deli/Commonwealth);
- Iniciativa Egípcia para os Direitos Pessoais (Cairo/Egipto);
- Instituto para a Defesa, Segurança e Estudos da Paz (Jacarta/Indonésia);
- Instituto de Estudos de Segurança (Pretória/África);
- Comissão Internacional de Juristas (Genebra/global);
- Arquivo de Segurança Nacional (Washington DC/global);
- Centro de Aconselhamento para a Democracia Aberta (Cidade do Cabo/África do Sul); e
- Iniciativa de Justiça de Sociedade Aberta (Nova Iorque/global).

[3] Além disso, Aidan Wills e Benjamin Buckland, do Centro de Genebra para o Controlo Democrático das Forças Armadas (DCAF) mas não associados a nenhuma das organizações parceiras, também deram contributos especialmente significativos para a Parte V, sobre Entidades de Supervisão, e a Parte VI, sobre Divulgações de Interesse Público, bem como para os Princípios como um todo.