NECESSÁRIO E PROPORCIONAL

PRINCÍPIOS INTERNACIONAIS DE APLICAÇÃO DA LEI DOS DIREITOS HUMANOS À VIGILÂNCIA DAS COMUNICAÇÕES

Créditos

Os "Princípios Internacionais de Direitos Humanos sobre Vigilância das Comunicações" foram escritos colaborativamente por organizações de privacidade e ativistas do mundo inteiro, incluindo, mas não limitado a **Access, Article 19, Asociación Civil por la Igualdad y la Justicia, Asociación por los Derechos Civiles, Association for Progressive Communications, Bits of Freedom, Center for Internet & Society India, Comision Colombiana de Juristas, Electronic Frontier Foundation, European Digital Rights, Fundación Karisma, Fundación Vía Libre, Open Net Korea, Open Rights Group, Privacy International**, e o **Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.** Além disso, também queremos agradecer **IP Justice, IFEX Network, SHARE Foundation - SHARE Defense** *e* **Instituto NUPEF** para ajudar a conectar os grupos interessados.

For more information, visit

necessaryandproportionate.org/text

Acontecimento

O processo de elaboração destes Princípios começou em outubro de 2012, em uma reunião de mais de 40 especialistas de segurança e privacidade em Bruxelas. Após uma vasta consulta inicial, que incluiu uma segunda reunião no Rio de Janeiro em dezembro de 2012, a Access, a EFF e a Privacy International lideraram um processo de elaboração colaborativa que contou com a experiência de especialistas em direitos humanos e direitos digitais em todo o mundo. A primeira versão dos Princípios foi concluída em 10 de julho de 2013 e lançada oficialmente no Conselho de Direitos Humanos da ONU em Genebra, em setembro de 2013. O sucesso retumbante e a adoção global dos Princípios por mais de 400 organizações em todo o mundo exigiram uma série de alterações específicas, principalmente alterações textuais superficiais na linguagem dos Princípios, a fim de garantir a sua interpretação consistente e aplicação em várias jurisdições. De março a maio de 2013, realizou-se mais uma consulta para verificar e retificar esses problemas textuais e atualizar os Princípios de acordo comes se trabalho. O efeito e a intenção dos Princípios não foram alterados por essas mudanças. Esta versão é o produto final desses processos e é a versão oficial dos Princípios.

Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações

VERSÃO FINAL MAIO DE 2014*

Enquanto as tecnologias que facilitam a vigilância estatal das comunicações têm avançado, os Estados não têm cumprido seu dever de assegurar que leis, regulamentos, atividades, poderes e autoridades relacionados à Vigilância das Comunicações cumpram os padrões e leis de direitos humanos internacionais. Este documento tenta esclarecer como a lei internacional dos direitos humanos se aplica no atual ambiente digital, especialmente tendo em conta o aumento e as alterações técnicas e tecnológicas da Vigilância das Comunicações. Estes princípios podem oferecer a grupos da sociedade civil, empresas, Estados e a outros atores um instrumento para avaliar se as leis e práticas atuais ou propostas sobre monitoramento são consistentes ou não com os direitos humanos.

Estes princípios são o resultado de uma consulta global com grupos da sociedade civil, da indústria e especialistas inter-

nacionais em questões jurídicas, políticas e tecnológicas relacionadas à Vigilância das Comunicações.

PREÂMBULO

A privacidade é um direito humano fundamental para a manutenção de sociedades abertas e democráticas. É essencial à dignidade humana e reforça outros direitos, tais como a liberdade de expressão e de informação e a liberdade de associação, sendo reconhecida pela lei internacional dos direitos humanos.[1] A Vigilância das Comunicações interfere no direito à privacidade, dentre vários outros direitos humanos. Como resultado, pode ser justificada apenas quando determinada pela lei, necessária para atingir um fim legítimo e proporcional ao fim almejado.[2]

Antes da adoção pública da internet, princípios jurídicos bem estabelecidos e encargos logísticos inerentes ao monitoramento das comunicações limitavam a Vigilância das Comunicações por parte dos Estados. Nas últimas décadas, porém, essas barreiras logísticas para vigilância diminuíram e a aplicação dos princípios jurídicos em novos contextos tecnológicos tornou-se nebulosa. A explosão de conteúdo de comunicação digital—informações sobre as comunicações ou a utilização de dispositivos eletrônicos por parte de um indivíduo—e o barateamento do custo de armazenagem e mineração de grandes quantidades de dados, além da oferta de conteúdos pessoais por parte de provedores particulares, possibilitam a Vigilância das Comunicações por parte dos Estados em uma escala sem precedentes.[3] Ao mesmo tempo, os conceitos usuais de direitos humanos já existentes não acompanharam a modernização e as mudanças nas tecnologias e técnicas de Vigilância das Comunicações pelo Estado, nem a capacidade desse ator em organizar informações adquiridas por meio de diversas técnicas de monitoramento, ou a crescente sensibilidade da informação passível de ser acessada.

A frequência com que os Estados estão buscando acessar tanto o conteúdo de comunicações quanto os metadados está aumentando drasticamente, sem fiscalização adequada.[4] Os metadados de comunicações podem criar um perfil de vida do indivíduo, incluindo questões médicas, pontos de vista políticos e religiosos, associações, interações e interesses, revelando tantos detalhes quanto—ou ainda mais—do que seria perceptível a partir do conteúdo das comunicações.[5] Apesar do vasto potencial de intromissão na vida do indivíduo e do efeito desencorajador ("chilling effect") sobre a associação política e de outra natureza, as leis, regulamentos, atividades, poderes ou autoridades frequentemente atribuem aos metadados de comunicações um nível de proteção menor e não impõem restrições suficientes a como eles podem ser usados posteriormente pelos Estados.

ÂMBITO DE APLICAÇÃO

Os Princípios e o Preâmbulo são holísticos e auto-referenciais—cada princípio e o preâmbulo devem ser lidos e interpretados como parte de um quadro mais amplo e, lidos em conjunto, cumprem um objetivo singular: assegurar que as leis, políticas e práticas relacionadas à Vigilância das Comunicações sigam os padrões e leis internacionais de direitos humanos, além de protegerem adequadamente direitos humanos individuais tais como privacidade e liberdade de expressão. Assim, para que os Estados possam cumprir seus deveres no que diz respeito à Vigilância das Comunicações, devem obedecer a cada um dos princípios abaixo.

Estes princípios se aplicam a vigilância realizada dentro de um Estado ou extraterritorialmente. Os princípios também se aplicam independentemente do propósito do monitoramento—seja ele o cumprimento da lei, a proteção da segurança nacional, o recolhimento de dados de inteligência ou alguma função governamental. Eles também se aplicam tanto à obrigação do Estado de respeitar e cumprir os direitos

humanos dos indivíduos quanto à obrigação de proteger os direitos humanos individuas de abuso por parte de atores não-estatais, incluindo empresas.[6] As empresas têm a responsabilidades de respeitar a privacidade de um indivíduo e outros direitos humanos, particularmente tendo em conta o papel chave que desempenham no planejamento, desenvolvimento e difusão de tecnologias; na habilitação e oferecimento de serviços de comunicação; e na facilitação de determinadas atividades de vigilância estatal.[7] No entanto, estes Princípios articulam os deveres e obrigações dos Estados ao se envolver na vigilância das comunicações.

MUDANÇAS TECNOLÓGICAS E DEFINIÇÕES

"Vigilância das comunicações" no ambiente contemporâneo abrange o monitoramento, interceptação, coleta, obtenção, análise, uso, preservação, retenção, interferência em, acesso a ou ações semelhantes com relação às informações que incluem, refletem, derivam de ou dizem respeito às comunicações de uma pessoa no passado, presente ou futuro.

"Comunicações" incluem atividades, interações e transações transmitidas através de meios eletrônicos, tais como conteúdo de comunicações, a identidade das partes para as informações de rastreamento do local, de comunicações, incluindo endereços IP, o tempo e a duração das comunicações e identificadores de equipamentos de comunicação utilizados nas comunicações.

"Informações protegidas" são informações que incluem, refletem, decorrem de ou referem-se a comunicações de uma pessoa e não estejam prontamente disponíveis e facilmente acessíveis ao público em geral. Tradicionalmente a intrusão da Vigilância das Comunicações tem sido avaliada com base em categorias artificiais e formalistas. Os ordenamentos jurídicos existentes distinguem entre "conteúdo" e "não conteúdo", "informações do assinante" ou "metadados", dados guardados ou

dados em trânsito, dados mantidos em casa ou sob a posse de um terceiro provedor de serviço.[7] No entanto, tais distinções não são mais apropriadas para se avaliar o grau de intrusão que a Vigilância das Comunicações faz na vida privada e nas associações do indivíduo. Embora exista desde há muito um consenso no sentido de que o conteúdo das comunicações merece proteção significativa por parte da lei por conta de sua capacidade de revelar informações sensíveis, agora é evidente que outras informações extraídas das comunicações—metadados e outras formas de dados sem conteúdo—podem revelar ainda mais sobre uma pessoa do que o próprio conteúdo, e assim merecem proteção equivalente. Hoje em dia, cada um desses tipos de informação pode, sozinho ou analisado coletivamente, revelar a identidade de uma pessoa, seu comportamento, associações da qual faz parte, condições físicas ou médicas, raça, cor, orientação sexual, nacionalidade ou pontos de vista; ou permitir o mapeamento de sua localização, movimento e interações ao longo do tempo[8], ou mesmo de todas as pessoas de uma certa localidade, incluindo em manifestações públicas ou outro evento político. Como resultado, todas as Informações Protegidas devem receber a mais alta proteção legal.

Para avaliar o grau de intrusão da Vigilância Estatal das Comunicações, é necessário considerar tanto o potencial de se revelar a Informação Protegida quanto o propósito para o qual tal informação é buscada pelo Estado. Qualquer Vigilância das Comunicações é uma interferência nos direitos humanos, portanto deve ser regida pela lei de direitos humanos. A Vigilância das Comunicações que possivelmente levem à revelação de Informações Protegidas que possam colocar uma pessoa em risco de investigação, discriminação ou violação de direitos humanos constituirá uma grave violação de seu direito à privacidade, e também enfraquecerá o gozo de outros direitos fundamentais, tais como o de liberdade de expressão, associação e participação política. Isso ocorre porque esses direitos exigem que as pessoas possam comunicar-se sem o efeito desencora-

jador colocado pela vigilância do governo. Uma determinação tanto do caráter quanto dos usos potenciais da informação buscada, portanto, será necessária em cada caso específico.

Ao adotar uma nova técnica de Vigilância das Comunicações ou ao expandir o escopo de uma técnica já existente, o Estado deve verificar se a informação a ser procurada se encaixa dentro do âmbito de Informação Protegida antes da busca em si, e deve submeter-se à análise do Poder Judiciário ou de outro mecanismo de controle democrático. Ao considerar se a informação obtida por meio da Vigilância das Comunicações se encaixa no nível de Informação Protegida, tanto a forma quanto o escopo e a duração da vigilância são fatores relevantes. Já que o monitoramento universal ou sistemático, bem como as técnicas invasivas usadas para realizar a Vigilância das Comunicações, têm a capacidade de revelar informação privada que em muito excede cada uma de suas partes constituintes, ele pode elevar a vigilância de informação não-protegida a um nível de intrusão que necessita de forte proteção aplicável às Informações Protegidas.[9]

A determinação sobre se o Estado pode conduzir a Vigilância das Comunicações no que tange às Informações Protegidas deve atender aos princípios abaixo.

OS 13 PRINCÍPIOS

OS 13 PRINCÍPIOS

Legalidade

Qualquer limitação aos direitos humanos deve ser disposta em lei. O Estado não deve adotar ou implementar uma medida que interfere no direito à privacidade na ausência de um dispositivo legal disponível ao público e que atinja um nível de precisão e clareza suficientes para garantir que indivíduos possam prever sua aplicação. Dada a velocidade das mudanças tecnológicas, as leis que autorizam limitações ao direitos humanos devem ser sujeitas a revisão periódica por meio de um processo legislativo ou regulamentar participativo.

Fim Legítimo

As leis só devem permitir a Vigilância das Comunicações por autoridades estatais específicas para atingir um interesse legítimo de suma importância que corresponda a um interesse necessário em uma sociedade democrática. Qualquer medida não pode ser aplicada de forma discriminatória com base em raça, cor, sexo, língua, religião, opiniões políticas e demais opiniões, nacionalidade ou origem social, propriedade, nascimento ou qualquer estado.

Necessidade

As leis, regulamentos, atividades, poderes ou autoridades de vigilância devem se limitar ao que é estrita e comprovadamente necessário para atingir um fim legítimo. A Vigilância das Comunicações só deve ser conduzida quando for a única forma de atingir um fim legítimo, ou, caso haja múltiplas formas, que seja a forma de menor impacto aos diretos humanos. O ônus de estabelecer esta justificativa recai sempre sobre o Estado.

Adequação

Qualquer instância de Vigilância das Comunicações autorizada por lei deve ser apropriada para realizar o Fim Legítimo identificado.

Proporcionalidade

A Vigilância das Comunicações deve ser considerada um ato altamente intrusivo que interfere nos direitos humanos, ameaçando os fundamentos de uma sociedade democrática. As decisões sobre a Vigilância das Comunicações devem envolver uma consideração sobre a sensibilidade da informação e a gravidade da infração aos direitos humanos e outros interesses concorrentes.

Isso requer que um Estado, no mínimo, estabeleça os seguintes pontos à Autoridade Judicial Competente, antes de realizar a Vigilância das Comunicações com o objetivo de cumprir a lei, proteger a segurança nacional ou recolher dados de inteligência:

1. existe uma alta probabilidade de que um crime grave ou ameaça específica a um Fim Específico foi ou será cometido, e;

2. existe alta probabilidade de que evidências ou materiais relevantes para tal crime grave ou ameaça específica a um Fim Legítimo seriam obtidos acessando as Informações Protegidas procuradas, e;

3. outras técnicas menos invasivas foram esgotadas ou seriam inúteis, de forma que as técnicas utilizadas sejam a opção menos invasiva, e;

4. as informações acessadas serão limitadas ao que é relevante e essencial ao crime grave ou ameaça específica ao Fim Legítimo alegado; e

5. quaisquer informações coletadas a mais não serão mantidas, mas, pelo contrário, serão prontamente destruídas ou devolvidas; e

6. as informações serão acessadas somente pela autoridade especificada e usadas apenas para a finalidade e pela duração para as quais foi concedida a autorização.

7. as atividades de vigilância solicitadas e técnicas propostas não comprometem a essência do direito à privacidade ou as liberdades fundamentais.

Autoridade Judicial Competente

As determinações relativas à Vigilância das Comunicações devem ser expedidas por uma autoridade judicial competente que seja imparcial e independente. Essa autoridade deve ser:

1. separada e independente das autoridades que realizam a Vigilância das Comunicações;

2. familiarizada com os assuntos relacionados e competente para expedir decisões judiciais sobre a legalidade da Vigilância das Comunicações, as tecnologias utilizadas e os direitos humanos; e

3. ter recursos adequados ao exercer as funções que lhes são atribuídas.

Devido Processo Legal

O devido processo legal requer que Estados respeitem e garantam os direitos humanos de uma pessoa ao assegurar que os procedimentos legais que interferem nos direitos humanos sejam feitos de acordo com a lei, e que esta seja respeitada e esteja disponível para o público em geral. Especificamente no que diz respeito aos direitos humanos do indivíduo, todos têm direito a uma audiên-

cia pública e justa dentro de um tempo razoável realizada em um tribunal independente, competente e imparcial estabelecido por lei,[10] excetuando-se os casos de emergência nos quais há risco ou perigo iminente para a vida humana. Em tais casos, devem ser buscadas autorizações retroativas dentro de um período razoável e cabível. O mero risco de perecimento ou destruição de evidências nunca deve ser considerado como suficiente para justificar autorização retroativa.

Notificação Do Usuário

Aqueles cujas comunicações estão sendo vigiadas devem ser notificados da decisão que autoriza a Vigilância das Comunicações dentro de um tempo suficiente e ter informações necessárias para permitir-lhes o recurso contra as decisões ou a busca de outras medidas, e devem ter acesso a materiais apresentados juntamente com o pedido da autorização. O atraso na notificação só é justificado nas seguintes circunstâncias:

1. A notificação tornaria totalmente inepto o propósito para o qual a Vigilância das Comunicações é autorizada, ou em caso de haver perigo iminente à vida humana, e/ou;

2. A autorização para o atraso na notificação for autorizada pelo Órgão Judicial Competente; e

3. O Usuário afetado seja notificado o mais cedo possível quando o risco cessar ou quando determinado pela Autoridade Judicial Competente.

A obrigação para a notificação recai sobre o Estado, mas os provedores de serviços de comunicação estarão livres para notificar indivíduos sobre a Vigilância de Comunicações, voluntariamente ou se forem assim requisitados.

Transparência

Os Estados devem ser transparentes sobre o uso e o escopo das leis, regulamentos, atividades, poderes ou autoridades de Vigilância das Comunicações. Eles devem publicar, no mínimo, informações agregadas sobre número de pedidos aprovados e rejeitados, um detalhamento dessa informação por provedor de serviços e autoridade investigatória, tipo, propósito e número específico de indivíduos afetados por cada um desses pedidos. Os Estados devem fornecer aos indivíduos informações suficientes que lhes deem a capacidade de compreender plenamente o escopo, natureza e aplicação da legislação que permite a Vigilância das Comunicações. Os Estados não devem interferir nos esforços empreendidos por provedores de serviço para publicar os procedimentos que aplicam para avaliar e cumprir as exigências estatais para com a Vigilância das Comunicações, além de aderir a esses procedimentos e publicar arquivos dos pedidos de Vigilância de Comunicações por parte do Estado.

Escrutínio Público

Os Estados devem estabelecer mecanismos de fiscalização independente para garantir a transparência e responsabilização da Vigilância das Comunicações.[11] Esses órgãos fiscalizadores devem ter autorização: para acessar toda informação potencialmente relevante sobre ações do Estado, incluindo, quando apropriado, acesso a informações secretas ou confidencias; discernir se o Estado está fazendo uso legítimo de suas atribuições legais; avaliar se o Estado está publicando corretamente informações sobre o uso e escopo de suas técnicas e poderes de Vigilância das Comunicações de acordo com suas obrigações de Transparência; publicar relatórios periódicos e outras informações relevantes sobre a Vigilância das Comunicações; e divulgar as determinações quanto à legalidade dessas ações, incluindo até que ponto eles aderem a estes Princípios. Os

mecanismos de supervisão independentes devem fixar-se além de qualquer supervisão já fornecida através de outro ramo do governo.

Integridade Das Comunicações E Sistemas

Para garantir a integridade, a segurança e a privacidade dos sistemas de comunicações e em reconhecimento do fato de que comprometer a segurança por causa de propósitos estatais quase sempre fragiliza a segurança de forma geral, os Estados não devem compelir provedores de serviços ou fornecedores de hardware e software a embutir capacidade de vigilância ou monitoramento em seus sistemas, ou a coletar ou reter informações particulares apenas para propósitos de Vigilância das Comunicações por parte do Estado. A retenção de dados a priori ou sua coleta nunca deve ser exigida de provedores de serviços. Os indivíduos têm o direito de se expressar anonimamente e, dessa forma, os Estados devem abster-se de obrigar a identificação do usuário.[12]

Salvaguardas Para A Cooperação Internacional

Em resposta às mudanças nos fluxos de informação e em serviços e tecnologias de comunicação, os Estados podem precisar buscar assistência de prestadores de serviços estrangeiros e de outros estados. Nesse sentido, os tratados legais de assistência mútua (MLAT) e outros acordos celebrados pelos Estados devem garantir que, onde as leis de mais de um estado poderiam se aplicar à Vigilância das Comunicações, o padrão disponível com o nível de proteção mais alto para os indivíduos deve ser aplicado. Quando os Estados procurarem assistência para propósito de cumprimento da lei, o princípio da criminalidade dupla deve ser aplicado. Os Estados não podem usar processos de assistência mútua e pedidos estrangeiros de Informações Protegidas para driblar restrições legais domésticas na Vigilância das Comunicações. Os processos de assistência

legal mútua e outros acordos devem ser claramente documentados, publicamente disponíveis e sujeitos às garantias de equidade processual.

Salvaguardas Contra Acesso Ilegítimo E O Direito A Medidas Eficazes

Os Estados devem promulgar legislação criminalizando a Vigilância das Comunicações ilegal realizada por atores públicos e privados. A lei deve fornecer sanções civis e criminais suficientes e significativas, proteções para os denunciantes e caminhos de reparação para aqueles afetados. As leis devem estipular que quaisquer informações obtidas de maneira inconsistente com estes princípios são inadmissíveis como prova, ou não consideradas em nenhum procedimento, bem como evidências derivadas dessa informação obtida ilegalmente. Os Estados também devem elaborar leis que determinando que, após o material obtido pela Vigilância das Comunicações ter sido utilizado para o propósito para o qual a informação foi dada, esse material não seja retido, mas destruído ou devolvido àqueles afetados.

*O processo de elaboração destes Princípios começou em outubro de 2012, em uma reunião de mais de 40 especialistas de segurança e privacidade em Bruxelas. Após uma vasta consulta inicial, que incluiu uma segunda reunião no Rio de Janeiro em dezembro de 2012, a Access, a EFF e a Privacy International lideraram um processo de elaboração colaborativa que contou com a experiência de especialistas em direitos humanos e direitos digitais em todo o mundo. A primeira versão dos Princípios foi concluída em 10 de julho de 2013 e lançada oficialmente no Conselho de Direitos Humanos da ONU em Genebra, em setembro de 2013. O sucesso retumbante e a adoção global dos Princípios por mais de 400 organizações em todo o mundo exigiram uma série de alterações específicas, principalmente alterações textuais superficiais na linguagem dos Princípios, a fim de garantir a sua interpretação consistente e aplicação em várias jurisdições. De março a maio de 2013, realizou-se mais uma consulta para verificar e retificar esses problemas textuais e atualizar os Princípios de acordo

com esse trabalho. O efeito e a intenção dos Princípios não foram alterados por essas mudanças. Esta versão é o produto final desses processos e é a versão oficial dos Princípios.

NOTAS FINAIS

1 Declaração Universal dos Direitos Humanos, art. 12; Convenção das Nações Unidas sobre os Trabalhadores Imigrantes, art. 14; Convenção Internacional sobre os Direitos da Criança e do Adolescente, art. 16; Convenção Internacional dos Direitos Civis e Políticos, art. 17; Convenções Regionais do Sistema de Proteção aos Direitos Humanos, incluindo o art. 10 da Carta Africana da Proteção dos Direitos da Criança e do Adolescente, art. 11 da Convenção Interamericana dos Direitos Humanos, art. 4º dos princípios da União Africana dos Direitos da Liberdade de Expressão, art. 5º da Declaração Americana dos Direitos e Deveres do Homem, art. 21 da Carta Árabe sobre Direitos Humanos e art. 8º da Convenção Europeia dos Direitos Humanos; Princípios de Joanesburgo sobre Segurança Nacional, Liberdade de Expressão e Acesso à Informação; e os "Camden Principles on Freedom of Expression and Equality".

2 Declaração Universal dos Direitos Humanos art. 29; Comentário Geral nº 27, adotada pelo Comitê de Direitos Humanos sob o art. 40, §4º, da Convenção Internacional dos Direitos Civis e Políticos, CCPR/C/21/Ver.1/Add.9, 2 de novembro de 1999; ver também Martin Scheinin, "Relatório do Relator Especial sobre a promoção de direitos humanos e liberdades fundamentais no combate de terrorismo". 2009 A/HRC/17/34. Ver também Frank La Rue, "Relatório do Relator Especial para o Conselho de Direitos Humanos sobre as implicações da vigilância dos Estados nas comunicações sobre o exercício dos direitos à privacidade e à liberdade de opinião e de expressão", 2013, A.HRC.23.40 EN.

3 Os metadados das comunicações podem incluir informações sobre nossa identidade (informações do assinante, informações sobre o dispositivo), interações (origens e destinos das comunicações, especialmente aqueles que mostram os sites visitados, livros e outros materiais lidos, pessoas com quem se interagiu, amigos, família, conhecidos, buscas realizadas, recursos utilizados) e localização (lugares e horários, proximidade de outros. Em suma, os metadados oferecem registros de quase todas as ações que ocorrem na vida moderna, nosso estado de espírito, interesses, intenções e pensamentos mais íntimos.

4 Por exemplo, somente no Reino Unido há agora aproximadamente 500 mil solicitações de metadados de comunicações por ano, atualmente sob um regime auto-autorizável por parte dos departamentos de polícia, que têm o poder de autorizar suas próprias solicitações de acesso a informações mantidas por provedores de serviço. Neste meio tempo, os dados fornecidos pelos relatórios de transparência do Google mostram que as requisições de dados de usuários apenas nos Estados Unidos aumentaram de 8.888 em 2010 para

12.271 em 2011. Na Coreia, houve cerca de 6 milhões de pedidos de informação sobre assinante/quem postou a informação anualmente, e aproximadamente 30 milhões de pedidos de metadados de outras formas de comunicação anualmente em 2011-2012, quase todos os quais foram concedidos e executados. Dados de 2012 disponíveis em **http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586**

5 Veja, como exemplos, uma análise do trabalho de Sandy Petland, "Garimpando a Realidade", na publicação MIT's Technology Review de 2008, disponível em **http://www2.technologyreview.com/article/409598/tr10-reality-mining/** bem como o trabalho de Alberto Escudero-Pascual e Gus Hosein, "Questionando o acesso legal a dados de tráfego", em Communications of the ACM, Volume 47, número 3, março de 2004, páginas 77-82.

6 Relatório do relator especial da ONU, Frank La Rue, sobre a promoção e a proteção do direito à liberdade de opinião e expressão, 16 de maio de 2011, disponível em **http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf**

7 "As pessoas revelam os números de telefone que discam ou para os quais mandam mensagem às operadoras telefônicas, os URLs que visitam e os endereços de email com os quais se correspondem para os seus provedores de internet, e os livros, compras domésticas e medicamentos que compram para os sites de vendas... Eu não diria que todas as informações divulgadas voluntariamente para alguns membros do público com uma finalidade limitada sejam, apenas por essa razão, desvinculadas da proteção dada pela 4ª Emenda [da constituição dos EUA]." Estados Unidos v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

8 "O monitoramento a curto prazo dos movimentos de uma pessoa está de acordo com as expectativas de privacidade", no entanto "o uso a longo prazo de monitoramento por GPS em investigações da maioria dos crimes esbarra nas expectativas de privacidade". Estados Unidos v. Jones, 565 U.S., 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

9 "A vigilância prolongada revela tipos de informação que não seriam reveladas pela vigilância a curto prazo, como o que uma pessoa faz ou não faz repetidamente, o que ela não faz e qual o conjunto de atividades feitas. Esses tipos de informação podem revelar mais sobre uma pessoa do que qualquer informação do indivíduo vista isoladamente. Idas repetidas a uma igreja, bar, academia de ginástica ou livraria contam uma história não contada por nenhum tipo de ida isolada, assim como o ato de não ir a algum desses lugares durante o período de um mês. A sequência de movimentos de uma pessoa pode revelar ainda mais: uma única ida ao ginecologista diz pouco sobre uma mulher, mas uma ida seguida de compras numa loja de produtos para bebês depois de algumas semanas nos conta outra coisa.* Alguém que sabe de todas as saídas de uma outra pessoa pode deduzir se esta vai à igreja uma vez

por semana, se é alcoólatra, se faz musculação regularmente, se é um marido infiel, um paciente recebendo tratamento médico, se é associada a algum grupo particular ou político – e diz não só um fato sobre a pessoa, mas todos esses fatos." EUA v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.) p. 562; EUA v. Jones, 565 U.S. __, (2012), Alito, J., concurring. "Além disso, a informação pública pode cair no escopo da vida privada, onde é sistematicamente coletada e guardada em arquivos mantidos pelas autoridades. Isso é ainda mais verdadeiro quando tal informação diz respeito a um passado distante da pessoa... Na opinião desta Corte, tal informação, quando coletada sistematicamente e guardada num arquivo pelos agentes do estado, cai no escopo de 'vida privada' para efeitos do Art. 8(1) da Convenção." (Rotaru v. Romênia, [2000] ECHR 28341/95, §§ 43-44.

10 O termo "devido processo legal" neste contexto pode ser substituído por "justiça procedimental" ou "justiça natural", sendo bem articulado na Convenção Europeia de Direitos Humanos, artigo 6(1) e no artigo 8º da Convenção Americana de Direitos Humanos.

11 O Comissário de Intercepções de Comunicações do Reino Unido é um exemplo de tal órgão de controle independente. O Comissário de Interceptações de Comunicações (ICO) no Reino Unido publica um relatório que inclui alguns dados adicionais, mas não fornece dados suficientes para inspecionar os tipos de solicitação, o alcance de cada requisição de acesso, seu propósito e a inspeção aplicada a eles. Ver **http://www.iocco-uk.info/sections.asp?sectionID=2&type=top**.

12 Relatório do Relator Especial para a promoção e proteção da liberdade de expressão e opinião, Frank La Rue, 16 de maio de 2011 A/HRC/17/27, § 84.

NECESSÁRIO E PROPORCIONAL

PRINCÍPIOS INTERNACIONAIS SOBRE A APLICAÇÃO DOS DIREITOS HUMANOS NA VIGILÂNCIA DAS COMUNICAÇÕES

ANÁLISE LEGAL INTERNACIONAL DE REFERÊNCIA E APOIO

MAIO 2014

ELECTRONIC FRONTIER FOUNDATION

Electronic Frontier Foundation e ARTIGO19 são muito gratos a todos que nos ajudaram na pesquisa e elaboração deste documento. Agradecemos particularmente a Douwe Korff, professor de Direito na área de Direitos Humanos Internacionais, por preparar uma versão anterior do documento e a Cindy Cohn, Gabrielle Guillemin, Tamir Israel, Dr. Eric Metcalfe e Katitza Rodriguez, por sua contribuição posterior. Nosso especial agradecimento às organizações Access, Privacy International, Asociación por los Derechos Civiles, Comisión Colombiana de Juristas, Fundación Karisma, Human Rights Information and Documentation System – HURIDOCS, The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic e Open Net Korea por analisar e compartilhar seus materiais. Enquanto tentávamos realizar uma ampla consulta, teríamos recebido de bom grado material extra de especialistas em legislação relevante da África e do Leste Europeu, de órgãos nacionais e regionais, que não foram tão bem representados nesta primeira versão do documento.

necessaryandproportionate.org/LegalAnalysis

Índice

Introdução

Vivemos numa era em que o rápido desenvolvimento da economia e da capacidade de vigilância digital provoca uma série de desafios para muitos dos nossos direitos humanos mais caros.

- Como preservar a privacidade quando governos do mundo inteiro podem e realizam regularmente, sem custos e sem serem notados, a coleta e a análise de toda a comunicação feita pelos cidadãos—até mesmo em suas listas de contatos, documentos e conversas—com família, amigos e colegas?
- O que resta da liberdade de associação quando a comunicação e a localização de populações inteiras são ininterruptamente colhidas e armazenadas a partir de dados emitidos por telefones celulares?
- Como a verdadeira liberdade de expressão e opinião podem resistir se cada vez que assistimos a uma notícia desafiadora, lemos um documento polêmico, ou damos uma olhada no trabalho de um autor renomado, uma gravação digital é feita para ser assistida, lida e navegada por máquinas, algoritmos e agentes do estado?

Sobretudo, como nossos direitos humanos serão preservados na era digital em que muitas de nossas ações diárias, atividades políticas e comunicações emitem um fluxo contínuo de informação reveladora, com poucas limitações legais ou tecnológicas em seu monitoramento, coleta, análise e uso contra nós pelo governo?

Tais questões e as constantes preocupações que surgem com as técnicas de vigilância foram o ponto de partida para a elaboração dos Princípios Internacionais de Aplicação da Lei

dos Direitos Humanos à Vigilância das Comunicações, que explica como a legislação internacional de direitos humanos se aplica no contexto da vigilância da comunicação.[1] Os princípios estão, portanto, profundamente arraigados na legislação internacional de direitos humanos e na jurisprudência. As mais recentes revelações de Snowden demonstraram precisamente o quanto os direitos humanos podem ser violados se as questões de natureza tecnológica não forem dirimidas.

O principal fundamento dos *13 Princípios Necessários e Proporcional* (doravante denominados "os Princípios")[2] foi fornecer aos grupos da sociedade civil, aos estados, aos tribunais, órgãos legislativos e regulatórios, indústria e outros um arcabouço regulatório para avaliar se as leis de vigilância, vigentes ou propostas, e as práticas internacionais são compatíveis com os direitos humanos. Na era pós-Snowden, ficou clara a necessidade urgente de revisar e adotar leis nacionais de vigilância e práticas que observem os Princípios, além de assegurar as salvaguardas à privacidade transfronteiriça.

Paralelamente, uma das maiores preocupações concernentes aos Princípios foi manter a aplicação da lei atualizada com os últimos avanços tecnológicos e assegurar que as proteções essenciais, desenvolvidas na era pré-digital, permaneçam fortes. É inevitável que a legislação de direitos humanos não trate precisamente das mudanças na tecnologia ao longo do tempo. Nosso objetivo foi identificar princípios essenciais que sustentassem uma proteção robusta dos direitos humanos na era digital. Por essa razão, nem todas as proposições que sugerimos foram formal ou explicitamente endossadas pelos órgãos internacionais de defesa dos direitos humanos.

Os Princípios foram assinados por 400 organizações e 300 mil indivíduos do mundo inteiro, endossados pela Conferência Liberal Democrática do Reino Unido, bem como pelos parlamentos europeu, canadense e alemão.[3] Os Princípios fo-

ram citados pelo relatório do Grupo de Análise de Inteligência e Tecnologia de Comunicação do Presidente dos Estados Unidos,[4] pelo relatório da Comissão Interamericana de Direitos Humanos[5] e outros.[6]

Neste documento, a *Electronic Frontier Foundation* e a *ARTIGO 19* explicam a base legal ou conceitual para os Princípios específicos.[7] Nosso documento é dividido em três partes. A primeira parte é voltada para questões relativas ao âmbito de aplicação dos Princípios. A segunda parte introduz as definições fundamentais e conceitos, sobretudo o conceito de "informação protegida" em comparação com a abordagem tradicional e categórica da proteção e privacidade de dados e uma definição de "vigilância da comunicação". A terceira parte explica a base legal e conceitual de cada Princípio. Inicia-se estabelecendo o arcabouço dos direitos humanos básicos, sustentando os direitos à privacidade, liberdade de expressão e de associação. Depois, elabora-se a base legal para cada um dos Princípios com referência à jurisprudência e opiniões de vários especialistas e órgãos de direitos humanos internacionais, tais como relatores especiais da ONU. Tentamos explicitar quando nossas conclusões se baseiam em legislação firmemente estabelecida e quando estamos sugerindo novas práticas específicas, baseadas nos princípios fundamentais de direitos humanos.

Escopo:

APLICAÇÃO EXTRATERRITORIAL DOS TRATADOS DE DIREITOS HUMANOS

Um dos aspectos mais perturbadores das revelações de Snowden foi a extensão da cooperação e do compartilhamento de informações entre NSA, GCHQ e outros membros do grupo dos Cinco Olhos, no qual o material recolhido pela vigilância do regime de um dos países era prontamente compartilhado com os demais. Juntos, cada um dos Cinco Olhos

(Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia) está estrategicamente localizado para espionar grande parte da comunicação mundial quando esta é transmitida ou armazenada em seus respectivos territórios. As agências de inteligência internacional dessas nações construíram uma rede de interoperabilidade nos níveis técnico e operacional que abrange a rede de comunicação mundial. Ademais, há acordos entre países que não integram os Cinco Olhos para compartilhamento de informação, bem como cooperação uma mais ampla—principalmente entre órgãos responsáveis pela aplicação da lei—através de acordos mais formais, incluindo os Tratados de Assistência Legal Mútua (TALMs).

A cooperação internacional entre governos também gera questões, tais como quando e como os estados podem ser confiáveis no cumprimento às leis nacionais e internacionais em suas atividades de vigilância, que podem ter seu impacto estendido muito além de suas fronteiras. Uma questão é a extensão de se os estados podem ser responsabilizados "extraterritorialmente" pelas violações aos direitos humanos cometidas no exterior, por exemplo, a vigilância de comunicações privadas em outros países. É importante não esquecer, entretanto, que a tecnologia atual possibilita aos estados monitorar grande parte do tráfego internacional sem sair de suas fronteiras. Consequentemente, é importante referir-se à questão da jurisdição sob a legislação de direitos humanos e às diferentes formas de se responsabilizar um estado por seus atos, mesmo que os efeitos sejam sentidos fora de suas fronteiras.[8] Nossa discussão do Princípio 12, abaixo, traz uma análise mais profunda dessa questão no contexto específico dos TALMs.

Um problema crucial surge quando se depende de defesas dos direitos humanos de âmbito territorial extremamente restrito, que se tornam rapidamente ineficazes quando aplicadas a redes mundiais altamente integradas. Historicamente, limitações práticas restringem fortemente a extensão da atuação de um governo para acessar clandestinamente as comunicações

de indivíduos em outro país. Nos lugares onde há tais limitações, os indivíduos afetados poderiam teoricamente se valer das proteções de seu estado natal, uma vez que tais atividades de vigilância implicariam necessariamente em intrusão na soberania de outro estado e violação das leis locais. Porém, a natureza das redes digitais, que se baseia no envio e armazenamento sem fronteiras para sua eficiência e robustez, permite que os estados interceptem grandes volumes de informação externa no conforto de seus territórios. Acompanhando essa nova capacidade tecnológica, veio a mudança de foco pós-11/09, que coloca todos os indivíduos—em oposição aos poderes estrangeiros e aos estados—no foco de formidáveis poderes de vigilância e recursos de agências de inteligência estrangeira. A combinação desses fatores levou à situação em que os direitos à privacidade de estrangeiros são frequentemente invadidos em grau significativo e substancial por agências de inteligência externa.[9] Finalmente, enquanto as agências de inteligência externa frequentemente possuem amplitude significativa para espionar comunicações de estrangeiros,[10] a natureza altamente integrada das redes de comunicação levou muitas destas agências a fazer uma varredura de todos os dados indiscriminadamente, citando como justificativa dificuldades para distinguir entre comunicações domésticas e externas.[11]

Em suma, os governos podem realizar vigilância dentro e fora de suas fronteiras. Contudo, o arcabouço legal local da maioria dos países normalmente dá proteção muito maior aos direitos de privacidade de seus cidadãos do que dos não cidadãos ou não residentes. Consequentemente, muitos governos se dedicam à intensa vigilância de comunicações internacionais com muito pouca cautela com a privacidade de tais comunicações, provavelmente por crerem erroneamente que suas obrigações legais se aplicam apenas a seus próprios cidadãos ou residentes. E o que é ainda mais problemático: ao que parece, os países buscam acordos de compartilhamento de informações com outros países a fim de obter o tipo de material de vigilância referente a seus próprios cidadãos que

não poderia ser obtido sob a égide do ordenamento jurídico local. Porém, como explicitado abaixo, o gozo dos direitos fundamentais não é limitado aos cidadãos de determinados estados, mas sim de todos os indivíduos, a despeito de sua nacionalidade ou condição de apátrida, tais como requerentes de asilo, refugiados, trabalhadores migrantes e outras pessoas que se encontrem no território ou estejam sujeitas à jurisdição de um Estado.[12] Além disso, todas as pessoas são iguais perante a lei e, consequentemente, têm direito à igual proteção desta, sem discriminação.[13]

Diante disso, o Preâmbulo dos Princípios, na Seção Escopo da Aplicação, determina expressamente que os Princípios "se aplicam à vigilância conduzida dentro de um Estado ou extraterritorialmente". Isso reflete o requisito da legislação internacional de direitos humanos de que os estados respeitem os direitos de todas as pessoas sem distinção ou discriminação, quer seja para "todos que estejam em seu território ou jurisdição" ou simplesmente "sob sua jurisdição" ou "sujeito à sua jurisdição."[14]

É importante esclarecer, contudo, que a obrigação dos estados de respeitar os direitos das pessoas em sua "jurisdição" não se limita aos direitos das pessoas fisicamente em seu território. No caso Bósforo *versus* Irlanda,[15] por exemplo, a Corte Europeia de Direitos Humanos sustentou que a decisão do governo irlandês de apreender em Dublin um avião que pertencia a uma companhia turca foi o suficiente para submeter a empresa turca à jurisdição da República da Irlanda, para efeitos do processo.

O mesmo princípio também foi aplicado em casos envolvendo vigilância. No caso *Liberty e outros versus Reino Unido*, de 2008,[16] duas ONGs irlandesas se queixaram do monitoramento de suas comunicações pelo governo britânico por meio de sua Unidade de Teste Eletrônico, em Cheshire, Inglaterra—um equipamento capaz de monitorar 10 mil conversas simultâneas entre a Irlanda e a Europa. Naquele caso, a Câmara da

CEDH vislumbrou a violação do direito à privacidade das ONGs irlandesas, nos termos do Artigo 8º da CEDH, sustentando que nenhuma das ONGs estava fisicamente presente no território do Reino Unido. Em uma decisão anterior de admissibilidade no caso *Weber e Savaria versus Alemanha*,[17] a CEDH estava igualmente preparada para examinar as queixas de dois residentes do Uruguai contra o monitoramento de suas comunicações pelo governo alemão.[18]

O ponto em comum em cada um desses casos é que a vigilância estava sendo realizada *dentro* do território do estado em questão, mesmo que os sujeitos vigiados não estivessem lá. O dever do estado sob a égide da legislação internacional de direitos humanos é respeitar os direitos de todas as pessoas em seu território ou jurisdição, o que inclui, portanto, pessoas que estejam fisicamente fora do estado mas cujos direitos sejam afetados pelas ações do estado dentro de suas fronteiras.

Vale ressaltar, também, que a jurisdição territorial pode surgir não apenas pela localização física onde a vigilância da comunicação privada ocorreu, mas também onde os dados foram *processados*. Em outras palavras, mesmo que o governo britânico tenha capturado ligações telefônicas privadas das ONGs irlandesas a partir de uma unidade localizada *fora* do Reino Unido, por exemplo, estas ainda estariam sob sua jurisdição territorial se os dados das ligações telefônicas fossem processadas por agências do governo *dentro* do Reino Unido.

Mesmo que a vigilância tenha sido realizada pelo estado fora de seu território, este ainda seria responsável pelas violações de direitos humanos nos lugares onde exerceu autoridade ou efetivo controle. Segundo o Comitê de Direitos Humanos, no qual se examinaram os casos *Lopez Burgos v. Uruguai* e *Celiberti de Casariego v. Uruguai*:[19]

> O Artigo 2, parágrafo 1º, exige que os Estados Parte respeitem e assegurem os direitos do Pacto a todas as

> pessoas que possam estar em seus territórios e a todas as pessoas sujeitas a sua jurisdição. Isso significa que um Estado Parte deve respeitar e assegurar os direitos estabelecidos no Pacto a todos que estejam sujeitos ao poder ou efetivo controle daquele Estado Parte, mesmo que não esteja situado no território do Estado Parte.

A Corte Europeia de Direitos Humanos sustentou de maneira semelhante que:[20]

> ...Em circunstâncias excepcionais, os atos dos Estados Contratantes praticados fora de seus territórios ou que tenham produzido efeitos fora deles ("ato extraterritorial") podem integrar sua jurisdição nos termos do Artigo 1º da Convenção.

Alguns governos, notadamente os de Estados Unidos e Israel, negaram que as obrigações previstas no PIDCP se estendam a atos praticados fora de seus territórios.[21] Durante as discussões no Projeto da Resolução da Assembleia Geral da ONU sobre Privacidade na Era Digital—proposta em resposta às revelações de Snowden—um comunicado confirmou que os Estados Unidos continuam adotando a posição de que não está sujeito a nenhum dever legal de observar o Artigo 17 do PIDCP (privacidade) fora de seu território. Com efeito, essa questão é considerada uma "linha vermelha" que não deve ser ultrapassada. Suas primeiras instruções foram no sentido de que os negociadores dos Estados Unidos devem:[22]

> Esclarecer que as referências aos direitos de privacidade se referem explicitamente às obrigações dos Estados sob a égide do PIDCP e *remover sugestões de que tais obrigações são aplicáveis extraterritorialmente.* [Grifo nosso]

A posição dos Estados Unidos referente à inaplicabilidade do Pacto a suas atividades extraterritoriais foi duramente criticada pelo Comitê da ONU de Direitos Humanos na 110ª sessão.[23]

NECESSÁRIO E PROPORCIONAL

Conforme destacado pelo Comitê:

> "A delegação reconhece que a posição dos Estados Unidos sobre atividades extraterritoriais permitiu que os Estados Unidos cometessem violações em qualquer lugar exceto em seu próprio território? A não aplicabilidade do Pacto a atividades extraterritoriais levou à impunidade e à violação de direitos. Se todos os Estados adotassem essa interpretação não haveria qualquer proteção aos direitos."

Como se vê na discussão acima, essa visão retrógrada dos Estados Unidos de suas obrigações sob a égide do PIDCP é claramente contrária à legislação internacional de direitos humanos.[24] A Assembleia Geral das Nações Unidas vislumbrou tal contrariedade, tendo rejeitado as emendas sugeridas pelos Estados Unidos e expressamente reconheceu que a vigilância extraterritorial suscita preocupações quanto aos direitos humanos:

> Profundamente preocupado com o impacto negativo que a vigilância e/ou interceptação de comunicações, incluídas a vigilância e/ou interceptação de comunicações extraterritoriais, bem como a coleta de dados pessoais, em particular quando realizada em massa, podem ter sobre o gozo e o exercício dos direitos humanos;[25]

Seja pela jurisdição extraterritorial ou pela aplicação restritiva dos princípios da jurisdição territorial, é evidente que os estados não podem se eximir da obrigação de respeitar a privacidade das comunicações fundamentando-se seja na nacionalidade dos participantes ou em sua localização física. Por essa razão, os Princípios explicitam que os estados devem agir de maneira não discriminatória, a despeito de fatores como raça, cor, sexo, língua, religião, opinião política ou de outra natureza, nacionalidade ou origem social, propriedade, nascimento ou outro *status*.

Definições:

"INFORMAÇÃO PROTEGIDA" E "VIGILÂNCIA DA COMUNICAÇÃO"

Os Princípios se voltam para duas questões cruciais de definição que geraram desafios na aplicação da defesa dos direitos humanos na vigilância das comunicações tecnologicamente avançadas. A primeira se refere a que tipos de informação são protegidos. Tem havido uma tendência nas práticas de vigilância estatal de tratar certos tipos de dados como menos merecedores de proteção, com base em analogias artificiais que precedem o advento das redes digitais, apesar da natureza altamente reveladora e sensível dos dados. Os Princípios tratam desse tema definindo "informações protegidas" para incluir essas categorias de informação e reconhecer apropriadamente as implicações concernentes aos direitos humanos que surgem quando são atingidos. Quanto à segunda questão, o desenvolvimento tecnológico permite que entidades estatais monitorem, analisem, coletem e armazenem enormes quantidades de informação indefinidamente. Uma vez que essas atividades podem ser conduzidas sem um olhar individual direto sobre uma informação específica, alguns argumentam que o comprometimento da privacidade é inexistente ou muito limitado. No entanto, essas atividades de vigilância têm um profundo impacto sobre a privacidade dos indivíduos e, na prática, disponibiliza informações que normalmente não seriam disponibilizadas. Além disso, a premissa legal para essas distinções é duvidosa. Sendo assim, os Princípios definem "vigilância da comunicação" amplamente para abranger uma vasta gama de atividades que envolvam a privacidade e o valor expressivo inerente às redes de comunicação.

INFORMAÇÃO PROTEGIDA

Em apenas alguns anos, a tecnologia da comunicação passou

por mudanças sem precedentes, assim como o uso dessas tecnologias pelas pessoas no mundo inteiro. Ao mesmo tempo, grande parte da legislação existente e da jurisprudência sobre salvaguardas contra a vigilância invasiva foi desenvolvida algumas décadas atrás—nos tempos em que chamadas telefônicas ainda eram operadas por discagem e pulso e computadores pessoais eram uma raridade.

Em vez de manter conceitos ultrapassados e categorias de uma era pré-digital, os Princípios foram elaborados para refletir a maneira como os dados são rotineiramente armazenados e compartilhados hoje em dia por órgãos públicos e privados e para fornecer um nível de proteção compatível com a realidade dos danos que podem surgir quando o Estado acessa dados indevidamente.

Os Princípios usam a expressão "informação protegida" especialmente para se referir à informação (dados inclusive) que *deve* ser total e fortemente protegida, mesmo que não esteja protegida por lei atualmente, seja apenas parcialmente protegida por lei ou seja objeto de proteção mais branda. A intenção, porém, não é criar uma nova categoria, que por sua vez se tornará obsoleta com o tempo, mas sim assegurar que o foco seja e continue sendo a capacidade da informação, isolada ou quando combinada com outras, de revelar fatos privados sobre uma pessoa ou sobre aqueles com quem ela se corresponde. Assim sendo, os Princípios adotam uma definição singular que abrange tudo o que inclui qualquer informação relativa à comunicação de uma pessoa e que não esteja prontamente à disposição do público em geral.

Embora os tribunais recentemente tenham começado a resistir a essa abordagem, há distinções consagradas nas legislações da América do Norte, da Europa e de algumas localidades da Ásia e da América Latina entre o "conteúdo" de uma mensagem (a mensagem em si), os "dados da comunicação"

ou "metadados" (tais como informações sobre quem enviou a mensagem para quem e quando ou onde a mensagem foi enviada)[26] e "dados do assinante" (dados referentes ao proprietário da conta envolvida em uma comunicação).[27] Seguindo essa distinção, leis da América do Norte, Europa e algumas leis da Ásia e da América tradicionalmente conferem ao *conteúdo* da comunicação de uma pessoa uma proteção bem maior contra a interferência do que para qualquer dado relativo àquela comunicação. Previsivelmente, essa distinção foi baseada no modelo tradicional do serviço postal, que faz distinção entre a informação escrita no envelope e o conteúdo do envelope (de fato, a expressão "dados do envelope" é frequentemente usada como sinônimo de "dados da comunicação" ou "metadados"). Essa distinção ultrapassada, porém, perdeu o sentido diante dos métodos modernos de interceptação, diferentemente do correio postal convencional; por exemplo, a interceptação de *e-mail* implica em tornar tanto o conteúdo quanto os metadados instantaneamente acessíveis para a agência que realiza a interceptação. Além do mais, os metadados agora são armazenados em formatos digitais pelos provedores de serviço e podem ser adquiridos em massa, por encomenda, de maneira sem correspondente no serviço postal.[28] Ademais, não há equivalente "postal" para o significativo volume de atividade anônima *online* que pode ser relacionada a um indivíduo quando as informações do assinante são reveladas ao estado.[29]

Essas distinções foram adotadas como uma espécie de parâmetro simplista para privacidade: a ideia de que saber meramente para quem foi enviado um único envelope num dado momento não é tão reveladora quanto o conteúdo da carta. Ainda assim, o crescente valor dos metadados e as técnicas para agregá-los e analisá-los, significa que mesmo "simples metadados" podem revelar muito mais sobre atividades ou pensamentos de um indivíduo do que há 30 ou 40 anos atrás. Isso se deve, em parte, ao crescente volume e âmbito dos dados coletados: no início dos anos 1980, por exemplo, quando a Corte Europeia

de Direitos Humanos recebeu a primeira queixa sobre uso de medição de telefone[30] para coletar detalhes das ligações telefônicas de um suspeito, a única informação que estava gravada era o número dos telefones chamados e a duração das chamadas. Nos dias atuais, agências estatais buscam coletar não somente a identidade de quem faz a chamada, mas também os dados da conta, endereços, detalhes dos cartões de crédito, o modelo de aparelho usado e os dados sobre a localização de sua movimentação física. No caso de navegação na internet, uma simples URL digitada em um navegador (que constituiria mais um "metadado" do que conteúdo em certas jurisdições),[31] pode facilmente ser tão reveladora—e às vezes até mais—do que o conteúdo da página acessada em si.[32] Da mesma forma, identificar o proprietário de um endereço IP, identificador de dispositivo móvel ou de um endereço IP de *e-mail,* identificador móvel de assinante (IMSE), ou endereço de *email* podem ser altamente reveladores em um ecossistema onde os indivíduos deixam pegadas eletrônicas em todas as suas interações digitais. Nesse sentido, os metadados podem ser um "parâmetro adequado para conteúdo".[33] Além disso, as pessoas simplesmente usam tecnologias de comunicação com muito mais frequência hoje do que usavam a comunicação por cartas de papel. Por fim e igualmente importante, a capacidade do governo de coletar um volume muito maior desses dados por um período de tempo mais longo e organizá-los usando técnicas modernas de vigilância permite que um retrato íntimo da vida de uma pessoa seja rápida e facilmente criado por simples metadados.

A relativa falta de proteção concedida aos metadados de uma pessoa historicamente é sobremaneira evidente no ordenamento constitucional dos Estados Unidos, embora mais recentemente os tribunais, naquele país e em outros lugares, venham reconhecendo cada vez mais a inaplicabilidade dessa distinção para as comunicações modernas. Embora a Quarta Emenda proteja o *conteúdo* da comunicação de uma pessoa com outras[34]—e nenhuma decisão definitiva tenha sido obtida pelos tribunais no que se refere à vigilância em massa como a

evidenciada nas práticas pós 11/09 da NSA—os tribunais dos Estados Unidos sustentam que a Quarta Emenda não se aplica à informação que a pessoa compartilha "voluntariamente" com outros (a chamada "doutrina da terceira parte"), incluindo os detalhes dos registros de chamadas mantidos pelas empresas de telefonia:[35]

> Os usuários de telefone [...] sabem que a informação numérica é necessariamente transmitida para a empresa telefônica; que a empresa tem equipamentos para gravar essa informação; e que esta de fato grava essa informação para uma gama de fins legítimos do negócio. Embora as expectativas subjetivas não possam ser cientificamente medidas, é por demais forçoso acreditar que os assinantes de linhas telefônica, nessas circunstâncias, tenham qualquer expectativa de que os números que digitam permanecerão secretos.

Com o subsequente avanço na tecnologia das comunicações, a conclusão dos tribunais dos Estados Unidos de que não há expectativa de privacidade em registros telefônicos se estendeu a outras formas de comunicação. Em 2008, no caso *United States v. Forrester*, 512 F.3d 500, por exemplo, o Tribunal de Recursos da Nona Circunscrição sustentou que:

> Os usuários de *e-mail* e internet não têm expectativa de privacidade nos dados de remetente/destinatário de suas mensagens ou dos endereços IP dos sites que visitam porque deveriam saber que essa informação é fornecida para os provedores de serviços de internet e utilizada por estes para o propósito específico de direcionar o encaminhamento da informação.

No recente caso da Suprema Corte *United States v. Jones*, 132 S. Ct. 949 (2012), todavia, a juíza Sotomayor pareceu considerar a possibilidade de mudar esse entendimento, tendo em mente referências a outros casos:

> Eu não suporia que todas as informações voluntariamente reveladas para algum membro do público para um fim específico esteja, apenas por essa razão, fora da esfera de proteção da Quarta Emenda. Ver *Smith*, 442 U. S., 749 ("A privacidade não é uma mercadoria, totalmente possuída ou totalmente negada. Aqueles que revelam certos fatos para um banco ou uma companhia telefônica com um propósito comercial específico não precisa supor que essas informações sejam liberadas para outras pessoas para outros fins."); ver também *Katz*, 389 U. S., 351–352 ("O que a pessoa procura preservar como privado, mesmo em uma área acessível ao público, deve ser constitucionalmente protegido.").

Tal entendimento ainda não foi adotado pela Suprema Corte, posto que no caso *Jones* a decisão acolheu outros fundamentos. Porém, isso foi recentemente questionado no Grupo de Análise de Inteligência e Tecnologia de Comunicação do Presidente dos Estados Unidos.[36]

Como os tribunais dos Estados Unidos ainda precisam reconhecer as proteções constitucionais, os metadados são protegidos atualmente sobretudo por normas como o Estatuto Pen Register,[37] que atribui menos proteção a esse tipo de dados do que ao "conteúdo". Este, por sua vez, inspirou estatutos similares em outros países, como a Coréia, onde a aquisição de metadados é condicionada a decisão judicial.[38]

Por outro lado, a Corte Europeia de Direitos Humanos reconheceu os dados de comunicações como um "elemento integrante" de uma comunicação privada, que, portanto, goza da proteção ao direito de privacidade previsto no Artigo 8 da Convenção Europeia de Direitos Humanos (CEDH), embora menor do que a conferida ao conteúdo da comunicação.[39] Outros tipos de dados pessoais (incluindo dados que não sejam de comunicação) também se encontram sob a proteção da legislação

Europeia de proteção de dados[40] e o Artigo 8 da Carta de Direitos Fundamentais da União Europeia estabelece especificamente que todos têm direito à proteção de seus dados pessoais, o que deveria, a princípio, se estender aos metadados e às informações do assinante. É animador o fato de a Grande Seção do Tribunal de Justiça da União Europeia ter rejeitado muito recentemente o argumento de que os "metadados" devem atrair menos proteção do que "conteúdo" das comunicações no contexto do Artigo 7 da Carta Europeia de Direitos Fundamentais.[41] Ao mesmo tempo, está claro que a legislação europeia nessa área também sofre de alguns sérios problemas: primeiro, como citado acima, a antiga distinção entre metadados ou dados de comunicação, de um lado, e o conteúdo das comunicações, de outro, está sendo desgastada pelas mudanças tecnológicas; segundo, não está clara a extensão das proteções concedidas aos dados de comunicações pelo Artigo 8 da CEDH e da proteção conferida a outros tipos de dados pessoais sob a proteção da legislação de dados, uma sobreposta a outra. Isso é particularmente problemático, dado que a legislação Europeia de direitos humanos e a legislação de proteção de dados da União Europeia são capazes de proteger a mesma informação de forma bem diferente e estão sujeitas a exceções muito distintas.[42]

Em face desses problemas, é evidente que as distinções existentes entre metadados e conteúdo não existem mais e que uma abordagem nova é necessária para proteger a privacidade individual na era digital. Por essa razão, os Princípios emanam do fundamento de que toda informação relacionada com a comunicação privada de uma pessoa deve ser considerada "informação protegida", à qual se deve conferir a mais forte proteção legal. Na medida em que é necessário atribuir níveis adicionais de proteção em casos particulares, deve-se, para tanto, basear-se na natureza da invasão no contexto em particular, mais do que em referências a categorias abstratas e definições arcaicas.

VIGILÂNCIA DAS COMUNICAÇÕES

Na esteira das revelações de Snowden, vários governos buscaram defender mais agressivamente suas atividades distinguindo a coleta automática e a varredura de comunicações privadas do efetivo escrutínio dessas comunicações por humanos. Alguns oficiais sugeriram que se a informação é meramente coletada e mantida, mas não é vista por humanos, não houve invasão de privacidade. Outros argumentaram que a análise de palavras chave e outros macanismos de seleção em tempo real feita por computadores não é "vigilância" para o fim de atrair a incidência de proteções legais.

A legislação internacional de direitos humanos, todavia, deixa claro que a coleta e retenção dos dados de comunicações caracteriza intromissão no direito à privacidade, sejam estes posteriormente acessados ou utilizados por oficiais do governo ou não. No caso *S and Marper v. United Kingdom,* por exemplo, a Grande Seção do Tribunal de Justiça Europeu de Direitos Humanos sustentou que "a mera retenção e armazenamento de dados pessoais por autoridades públicas, não importa como tenham sido obtidos, devem ser considerados causadores de impacto direto nos interesses da vida privada de um indivíduo, independentemente de haver ou não uso subsequente dos dados."[43] Em *Digital Rights Ireland Ltd v. Minister for Communications,* a Grande Seção do Tribunal de Justiça da União Europeia sustentou de forma semelhante que a retenção de dados da comunicação "para o propósito de um possível acesso aos mesmos pelas autoridades nacionais competentes" constituiu uma "invasão particularmente séria da vida privada e familiar, do lar e das comunicações, nos termos do Artigo 7 da Carta de Direitos Fundamentais da União Europeia.[44]

Por essas razões, os Princípios deixam claro que a "Vigilância das Comunicações" incluem não somente a leitura propriamente dita de dados privados de comunicações por outro ser humano, mas também toda a extensão de monitoramento,

interceptação, coleta, análise, uso, preservação, retenção de dados, interferência e acesso à informação que inclui e reflete as comunicações de uma pessoa no passado, presente e futuro, ou que possa ter origem nessas comunicações. Qualquer sugestão, por parte dos governos, de que a coleta ou o monitoramento automáticos não constituem vigilância, portanto, está simplesmente em desacordo com as exigências das leis internacionais de direitos humanos, e os Estados não devem ter a permissão de ignorar as proteções à privacidade recorrendo a tais definições arbitrárias.

EXPLICAÇÃO PRINCÍPIO A PRINCÍPIO

Os Princípios são firmemente fundados na consagrada legislação de direitos humanos. Em particular, estão ligados aos direitos à privacidade, liberdade de opinião e expressão e liberdade de associação, como garantidos pela Declaração Universal de Direitos Humanos (DUDH), pelo Pacto Internacional de Direitos Civis e Políticos (PIDCP), pela Convenção Europeia de Direitos Humanos (CEDH), pela Carta Europeia de Direitos Fundamentais (EU Charter) e pela Convenção Interamericana de Direitos Humanos (IACHR).[45]

Ainda que cada um desses direitos seja formulado de formas ligeiramente diferentes,[46] a estrutura de cada artigo está, em geral, dividida em duas partes. O primeiro parágrafo define a núcleo do direito, enquanto o segundo estabelece as circunstâncias em que aquele direito deve ser restringido ou limitado. Normalmente, o segundo parágrafo determina que qualquer restrição ao direito essencial deve observar os seguintes requisitos:

- Deve ser estabelecido “por lei”;
- Não deve ser “arbitrário”;
- Deve buscar um dos objetivos legítimos enumerados taxativa ou exaustivamente naquele parágrafo; e

- Deve "necessariamente" atingir o objetivo em questão—o que foi mantido para incluir os requisitos de adequação e proporcionalidade.

Esse teste das "limitações admissíveis" foi aplicado igualmente aos direitos à privacidade, liberdade de expressão e liberdade de associação.[47] Exploramos a base legal de cada um desses requisitos mais detalhadamente no cabeçalho de cada Princípio correspondente abaixo (Princípios 1 a 5). Quando apropriado, fazemos referência ao contexto específico de vigilância. Então, explicamos nossa opinião e a base legal por trás da adoção dos demais Princípios (Princípios 6 a 13). Ainda que os tenhamos tratado separadamente, os Princípios destacam expressamente que pertencem à mesma unidade e são auto-referentes, o que significa que cada princípio e preâmbulo deve ser lido e interpretado como parte de um quadro maior.

PRINCÍPIO 1: LEGALIDADE

Princípios gerais

O princípio da legalidade é um aspecto fundamental de todos os instrumentos internacionais de direitos humanos e, na verdade, do Estado de Direito em geral. É uma garantia básica contra o exercício arbitrário de poderes pelo Estado. Por essa razão, qualquer restrição sobre os direitos humanos deve ser "prevista" ou "prescrita" por lei.[48]

De acordo com o PIDCP, o princípio da legalidade está intimamente associado ao conceito de "ingerência arbitrária". Por exemplo, o Artigo 17 estabelece que "ninguém poderá ser objeto de ingerência arbitrária ou ilegal em sua vida privada, em sua família ou correspondência". A Comissão de Direitos Humanos interpretou "ingerência arbitrária" da seguinte forma:[49]

> A expressão "ingerência arbitrária" é também relevante para a proteção do direito previsto no Artigo 17. Na opinião do Comitê, a expressão "ingerência

> arbitrária" também pode estender-se à ingerência estabelecida em lei. A introdução do conceito de arbitrariedade pretende garantir que mesmo a ingerência prevista por lei esteja em conformidade com as disposições, propósitos e objetivos do Pacto e seja, em qualquer caso, razoável nas circunstâncias específicas.

Além disso, o significado de "lei" implica certas exigências mínimas de qualidade referentes à clareza, acessibilidade e previsibilidade. Especificamente, a Comissão de Direitos Humanos detalhou o significado de "lei", para os efeitos do Artigo 19 do PIDCP (liberdade de opinião e de expressão), como segue:[50]

> 25. Para os efeitos do Parágrafo 3º, uma norma, para ser caracterizada como "lei", deve ser formulada com precisão suficiente para permitir que um indivíduo regule sua conduta de acordo com ela e deve ser acessível ao público. A lei não pode conferir critério irrestrito aos responsáveis pela execução da restrição da liberdade de expressão. As leis devem fornecer orientações suficientes aos responsáveis pela sua execução, permitindo-lhes determinar que tipo de expressão pode ser devidamente restringida ou não.

O Tribunal Europeu de Direitos Humanos tem seguido uma abordagem semelhante na sua jurisprudência. Mais especificamente, considerou que a expressão "previsto em lei" implica os seguintes requisitos:[51]

> Em primeiro lugar, a lei deve ser devidamente acessível: o cidadão deve conseguir ter uma indicação do que é adequado às circunstâncias das normas legais aplicáveis a um determinado caso. Em segundo lugar, uma norma não pode ser considerada "lei" a menos que seja formulada com precisão suficiente para permitir que o cidadão regule sua conduta; ele conseguir prever (se necessário for, com o aconselhamento apropriado), em

> um nível adequado às circunstâncias, as consequências que uma determinada ação pode acarretar.

As mesmas exigências se aplicam no que diz respeito ao direito à privacidade, nos termos do Artigo 17 do PIDCP, e do Artigo 8 da CEDH.[52] Mais especificamente, o Tribunal Europeu dos Direitos Humanos esclareceu, no contexto de vigilância:[53]

> A lei deve ser clara o suficiente em seus termos, para dar aos cidadãos uma indicação devida sobre em quais circunstâncias e condições as autoridades públicas poderão recorrer a essa ingerência, secreta e potencialmente perigosa, no respeito pelo direito à vida privada e à correspondência.

O Tribunal Europeu continuou a explicação:[54]

> Seria contrário ao Estado de Direito se o poder discricionário concedido ao Executivo fosse expresso nos termos de um poder ilimitado. Consequentemente, a lei deve indicar o alcance de qualquer poder discricionário conferido às autoridades competentes, e a forma de seu exercício, com clareza suficiente, tendo em conta o propósito legítimo da medida em questão, para dar ao indivíduo a proteção adequada contra a ingerência arbitrária.

Em outras palavras, normas secretas, orientações ou interpretações secretas das normas não possuem qualidade de "lei".[55] Uma lei que não é pública não é lei, pois é um componente essencial do Estado de Direito que as leis devam ser conhecidas e acessíveis a todos. Da mesma forma, as leis ou normas redigidas no sentido de conceder um poder ilimitado às autoridades caem em conflito com os requisitos da "lei". O alcance e a forma de exercer qualquer poder discricionário devem ser indicados na própria lei ou em diretrizes publicadas com "clareza razoável", de modo que as pessoas possam prever razoavelmente como a lei será aplicada na prática. Isto

é ainda mais importante dados os riscos de arbitrariedade inerentes ao exercício do poder em segredo.[56]

No contexto da vigilância, isso significa que apenas aprovar uma lei que autorize a vigilância em massa em nível nacional não torna a vigilância "legal" se essa lei não cumprir certos requisitos básicos de clareza e acessibilidade em primeiro lugar.

Garantias mínimas no contexto da vigilância da comunicação

Os requisitos acima citados de clareza, acessibilidade e precisão assumem um significado especial no contexto da vigilância da comunicação. Isso por causa da ameaça específica à própria essência da democracia representada pela vigilância secreta, conforme o Tribunal Europeu de Direitos Humanos reconheceu já em 1978.[57] O Tribunal considerou que a "mera existência" de uma legislação permitindo que um sistema monitorasse secretamente as comunicações deu origem a uma "ameaça de vigilância", o que equivalia a uma interferência na privacidade de todos aqueles a quem a legislação pode ter sido aplicada.[58] Em vista desses riscos, o Tribunal concluiu que devem existir garantias adequadas e eficazes contra o abuso previsto na lei, mais especificamente no estatuto.[59]

Particularmente, o Tribunal Europeu de Direitos Humanos identificou as seguintes garantias mínimas que uma lei de vigilância deve cumprir, a fim de ser compatível com o Artigo 8 da CEDH:[60]

- as infrações e atividades para as quais se pode ordenar a vigilância devem ser enunciadas de forma clara e precisa;
- a lei deve indicar claramente que categorias de pessoas podem ser submetidas à vigilância;
- deve haver limites de prazo rigorosos para as operações de vigilância;

- devem-se estabelecer procedimentos rigorosos para ordenar o exame, uso e armazenamento dos dados obtidos através da vigilância;
- a lei deve estabelecer as precauções a ser tomadas quanto à comunicação de dados a terceiros;
- deve haver regras rigorosas sobre a destruição ou eliminação dos dados de vigilância para impedir que esta permaneça escondida após o fato;
- os órgãos responsáveis pela supervisão da utilização dos poderes de vigilância devem ser independentes e responsáveis, e nomeados pelo Parlamento em vez do Executivo.

Seguiu-se a mesma abordagem nos âmbitos da ONU e Sistema Interamericano. Mais especificamente, os Relatores Especiais da ONU e da OEA para a Liberdade de Expressão emitiram recentemente uma declaração conjunta sobre os programas de vigilância, na qual disseram:[61]

> Os Estados devem garantir que a interceptação, coleta e o uso de informações pessoais, incluindo todas as limitações ao direito das pessoas afetadas de acessarem tais informações, sejam claramente autorizados por lei, a fim de protegê-las de interferências arbitrárias ou abusivas em seus interesses privados. A lei deve estabelecer limites no que diz respeito à natureza, âmbito e duração desse tipo de medidas; sobre as razões para requisitá-las; sobre quais as autoridades com competência para autorizá-las, executá-las e monitorá-las; e os mecanismos legais pelos quais podem ser impugnadas.
>
> Dada a importância do exercício desses direitos para um sistema democrático, a lei deve autorizar o acesso às comunicações e às informações pessoais somente nas circunstâncias mais excepcionais definidas pela

> legislação. Quando a segurança nacional é invocada como razão para a vigilância de correspondência e informações pessoais, a lei deve especificar claramente os critérios a serem utilizados para determinar os casos em que tal vigilância é legítima. Sua aplicação só poderá ser autorizada no caso de um risco evidente a interesses protegidos e quando o dano resultante pode vir a ser maior que o interesse geral da sociedade em manter o direito à privacidade e à livre circulação de ideias e informações. A coleta dessas informações deverá ser controlada por um órgão de supervisão independente e regido por garantias suficientes de que existem o devido processo legal e supervisão judicial, dentro dos limites admissíveis em uma sociedade democrática.

Seus pontos de vista também refletem as recomendações do Relator Especial da ONU sobre a Promoção e Proteção dos Direitos Humanos e Liberdades Fundamentais no Combate ao Terrorismo, Martin Scheinin, que disse em seu relatório de 2009:[62]

> 69. Devem-se estabelecer mandatos de supervisão independentes fortes para rever as políticas e práticas, no intuito de assegurar que haja forte fiscalização do uso de técnicas de vigilância intrusivas e de processamento de informações pessoais. Portanto, não pode existir nenhum sistema de vigilância secreto que não esteja sob a revisão de um órgão de supervisão independente, e todas as interferências deve ser autorizadas através de um órgão independente.

Voltaremos a tratar da necessidade de uma forte supervisão independente nos Princípios 6, 7, 9 e 10 mais adiante.

PRINCÍPIO 2: FIM LEGÍTIMO

De acordo com a Lei Internacional dos Direitos Humanos, qualquer restrição sobre os direitos à privacidade, liberdade de expressão e liberdade de associação devem buscar ao menos

um dos "fins legítimos", que estão exaustivamente enumerados no artigo correspondente em questão. Esses objetivos são redigidos de maneira extremamente ampla e incluem segurança pública, prevenção do crime, proteção da moral e dos direitos de outros e segurança nacional.[63] Nos termos do Artigo 8 da CEDH, também se inclui "o bem-estar econômico do país". Embora o Artigo 17 do PIDCP não estipule explicitamente que alguma restrição ao direito à privacidade deva ser necessária para uma finalidade específica, tanto o Relator Especial da ONU sobre Combate ao Terrorismo quanto o Relator Especial das Nações Unidas sobre a Liberdade de Expressão sustentaram que as "limitações admissíveis" dispostas no Artigo 19, entre outros artigos do PIDCP, são igualmente aplicáveis ao Artigo 17 do PIDCP.[64]

De acordo com a Lei Europeia dos Direitos Humanos, os Estados raramente encontram qualquer dificuldade em demonstrar que a restrição em questão busca um objetivo legítimo. Isso ocorre principalmente porque o Tribunal tende a concentrar sua análise na estrutura legislativa para o exercício dos poderes de vigilância, em vez de concentrá-la em uma medida de vigilância específica, usada em um caso particular. Também é geralmente aceito pelo Tribunal que os poderes de vigilância são necessários para fins de segurança nacional e de aplicação da lei.[65] A necessidade de que as medidas de vigilância sejam mais especificamente "direcionadas" é um aspecto que está mais estritamente ligado à questão da proporcionalidade da medida, mas, na prática, raramente é examinada pelo Tribunal.[66]

Por outro lado, o Relator Especial da ONU sobre a Liberdade de Expressão, Frank LaRue, expressou, em um relatório recente, sua preocupação de que noções "vagas e indeterminadas" de "segurança nacional"", particularmente, tinham sido utilizadas indevidamente para justificar a interceptação e o acesso a comunicações sem salvaguardas adequadas.[67] O Relator Especial concluiu:

> 60. O uso de um conceito amorfo de segurança nacional para justificar limitações invasivas no gozo dos direitos humanos é uma preocupação séria. O conceito é definido de forma muito ampla e, portanto, vulnerável à manipulação por parte do Estado, como forma de justificar ações que têm como alvo grupos vulneráveis como os defensores dos direitos humanos, jornalistas, ou ativistas. Ele também atua para garantir o sigilo muitas vezes desnecessário em torno de investigações ou atividades de aplicação da lei, o que prejudica os princípios da transparência e prestação de contas.[68]

Cientes do potencial de abuso inerente a tais conceitos excessivamente amplos, os Princípios buscaram adotar um padrão mais rigoroso sobre o que constitui um "fim legítimo" em relação à vigilância em massa. Por essa razão, os padrões "objetivo urgente e substancial", aplicado no Canadá, e "interesse imperioso do governo", usado nos Estados Unidos, também foram descartados por serem insuficientemente rigorosos.[69] Em vez disso, os Princípios refletem um padrão mais elevado imposto na Alemanha. Especificamente, o Tribunal Constitucional Alemão decidiu que medidas profundamente intrusivas, tais como a busca de um computador por agências de aplicação da lei, não podem ser justificadas simplesmente com a referência a algum interesse geral vagamente definido. O Tribunal Constitucional alemão considerou que tais medidas devem ser justificadas com base na evidência de que há "uma ameaça concreta a um interesse protegido por lei", tais como uma ameaça à "vida, à integridade física ou à liberdade de uma pessoa", ou a "bens públicos, perigos que ameacem as próprias bases ou a existência do Estado, ou os pré-requisitos fundamentais da existência humana".[70]

Além disso, os Princípios proíbem expressamente a discriminação nas leis, incluindo discriminações baseadas em nacionalidade, origem social, procedência ou qualquer outra situação. Essa é, naturalmente, uma disposição padrão na Lei Inter-

nacional dos Direitos Humanos.[71] Aqui, em conjunto com a aplicação extraterritorial da lei discutida acima, garante-se que as proteções da lei alcancem todas as pessoas sujeitas à vigilância, independentemente de sua localização ou cidadania.

PRINCÍPIOS 3, 4, 5: NECESSIDADE, ADEQUAÇÃO E PROPORCIONALIDADE

O princípio de que qualquer interferência a um direito específico, como o direito à privacidade ou a liberdade de expressão, deve ser "necessária em uma sociedade democrática" é uma das pedras angulares da Lei dos Direitos Humanos. De maneira geral, significa que um Estado deve não só demonstrar que a sua interferência no direito de uma pessoa atende a uma "necessidade social imperiosa", como também que é proporcional, ou, conforme a jurisprudência da Corte Interamericana, *adequada*[72] ao objetivo legítimo perseguido.[73]

Particularmente, o Tribunal Europeu de Direitos Humanos esclareceu que o termo "necessário" não é sinônimo de "indispensável", nem tão flexível quanto os termos "admissível", "comum", "útil", "razoável", ou "desejável".[74] Sujeito à doutrina da "margem de apreciação", o Tribunal Europeu procede à avaliação da necessidade e da proporcionalidade de uma medida "à luz de todas as circunstâncias". No entanto, certas medidas, tais como poderes de vigilância secreta, são analisadas mais cautelosamente.[75]

O Comitê de Direitos Humanos segue uma abordagem semelhante. Em especial, a Comissão explicou em seu Comentário Geral sobre o Artigo 12 do PIDCP (liberdade de circulação):[76]

> O Artigo 12, Parágrafo 3, indica claramente que não basta que as restrições apresentem os propósitos admissíveis; elas também devem ser necessárias para protegê-los. As medidas restritivas devem estar em conformidade com o princípio da proporcionalidade;

> devem ser adequadas para alcançar a sua função protetiva; *devem ser os instrumentos menos intrusivos entre aqueles que podem alcançar o resultado desejado*; e devem ser proporcionais ao interesse a ser protegido. [Grifo nosso]

Os mesmos princípios se aplicam à interpretação do Artigo 19 do PIDCP[77] e do Artigo 17 do PIDCP.[78]

O Comitê de Direitos Humanos às vezes usa também a palavra "adequado" em sua análise. Por exemplo, em relação ao Artigo 19 do PIDCP (liberdade de expressão), o Comitê observou que as medidas restritivas "devem ser adequadas para atingir a sua função de proteção".[79]

Da mesma forma, como mencionado acima, a Corte Interamericana de Direitos Humanos, por vezes, refere-se ao conceito de "adequação". Particularmente, o Tribunal considerou se a medida em questão poderia contribuir para a realização do objetivo invocado para limitar o direito em questão.[80]

Tribunais em vários Estados esclareceram que, substancialmente, "adequação" ou "proporcionalidade" não significam que as medidas em questão tenham de ser inteiramente bem-sucedidas. Em vez disso, elas impõem um requisito análogo ao conceito canadense de "racionalmente conectadas", apesar de "proporcionalidade" ser aplicada com mais rigor. A medida não deve apenas ter alguma ligação lógica com o objetivo pretendido, mas também deve ser "eficaz" para alcançá-lo. Uma medida inerentemente incapaz de alcançar o objetivo declarado, ou que seja comprovada e grosseiramente ineficaz para alcançá-lo, não poderá nunca ser considerada "adequada", "necessária" ou "proporcional".

Esta exigência de proporcionalidade é especialmente importante no contexto de vigilância em massa, que se baseia na coleta indiscriminada e retenção de comunicações e

metadados sem nenhuma forma de direcionamento ou suspeita razoável. Em *S and Marper*, por exemplo, a Grande Câmara do Tribunal Europeu dos Direitos Humanos considerou que a retenção "frequente e indiscriminada" de dados de DNA equivalia a uma "intervenção desproporcionada" na vida privada das pessoas cujos dados haviam sido tomados. A Grande Câmara conferiu especial atenção ao fato de que o material foi "mantido indefinidamente, independentemente da natureza ou gravidade da infração da qual a pessoa era suspeita".[81] Em outro caso envolvendo o uso de poderes de busca, a Grande Câmara notou que a ausência de qualquer exigência na polícia para ter uma "suspeita razoável" de que a pessoa investigada estava envolvida na criminalidade, significa que o poder de busca carecia de "garantias jurídicas adequadas contra o abuso" (parágrafos 86-87).[82] Mais recentemente, a Grande Câmara do Tribunal de Justiça da União Europeia, em sua decisão no grupo *Digital Rights Ireland Ltd*,[83] considerou que, embora a conservação de dados de comunicações ao abrigo da Diretiva fosse para o objetivo legítimo de combater um "crime grave", a natureza geral da obrigação implicava "uma interferência nos direitos fundamentais de praticamente toda a população europeia",[84] incluindo "pessoas para as quais não há evidência capaz de sugerir que o seu comportamento pode ter uma ligação, mesmo indireta ou remota, com crime grave".[85]

Por sua própria natureza, a vigilância em massa não envolve nenhuma forma de direcionamento ou seleção, e muito menos qualquer exigência às autoridades para mostrar suspeita razoável ou causa provável. Assim, a vigilância em massa é inevitavelmente desproporcional como uma questão de simples definição.[86] Os Princípios refletem os padrões internacionais acima citados sob os títulos de "necessidade", "adequação" e "proporcionalidade".

Quanto à vigilância orientada, os Princípios discutem fatores que devem ser estabelecidos por uma autoridade judicial competente, antes da vigilância. Os fatores exigem limitações

cuidadosas das informações acessadas, assim como limitações de uso e retenção. Importante ressaltar, como discutiremos mais adiante, que esta disposição exige a participação de uma autoridade judiciária competente.

PRINCÍPIOS 6, 7: AUTORIDADE JUDICIAL COMPETENTE E DEVIDO PROCESSO LEGAL

Vigilância e autorização judicial prévia

Conforme mencionado acima, os Princípios exigem que todas as decisões relativas à Vigilância das Comunicações sejam tomadas por uma autoridade judicial competente, agindo de forma independente do governo e de acordo com o devido processo legal. Isso reflete o requisito fundamental da Lei Internacional dos Direitos Humanos, que dispõe que o uso dos poderes de vigilância lícitos por funcionários públicos não só devem ser necessários e proporcionais, mas também contar com a presença de garantias rigorosas contra o abuso,[87] monitoradas de forma independente. Conforme o Tribunal Europeu dos Direitos Humanos sustentou em sua decisão realizada em 1979 no caso Klass contra Alemanha:[88]

> O Estado de Direito implica*, inter alia*, que uma interferência das autoridades do Poder Executivo nos direitos individuais deve estar sujeita a um controle eficaz, normalmente assegurado pelo Poder Judiciário, pelo menos em última instância, controle judicial que ofereça as melhores garantias de independência, imparcialidade e um procedimento adequado.

Embora o Tribunal no caso Klass tenha concordado que "é, em princípio, desejável confiar o controle de supervisão a um juiz", não foi tão longe a ponto de afirmar que uma autorização judicial prévia fosse necessária em todos os casos, contanto que o órgão autorizador relevante fosse "suficientemente independente" das "autoridades encarregadas da vigilância" para "dar uma decisão objetiva", e que também tenha sido investido

"com poderes e competências suficientes para exercer um controle eficaz e contínuo".[89] No entanto, em casos posteriores o Tribunal deixou claro que é desejável uma autorização judicial para o uso de vigilância lícita. Em um caso de 1999, por exemplo, o Tribunal declarou que:

> É, para dizer o mínimo, surpreendente que [a] tarefa [de autorizar interceptações] seja atribuída a um funcionário do departamento jurídico dos Correios, que é membro do executivo, sem a supervisão de um juiz independente, especialmente nesta área sensível das relações confidenciais entre um advogado e seus clientes, que diretamente dizem respeito aos direitos de defesa.[90]

Os princípios, no entanto, refletem a visão de que a autorização judicial prévia dos poderes de vigilância não é apenas desejável, mas essencial. Isso porque nenhum dos outros dois ramos do governo consegue conferir o grau necessário de independência e objetividade para evitar o abuso dos poderes de vigilância. O ponto de vista do Tribunal de Justiça no caso *Klass*, de que a supervisão de um órgão parlamentar deve ser suficientemente independente, já não parece defensável, particularmente na sequência dos ataques de 11/9, em que os legisladores se mostraram muito dispostos a sacrificar os direitos individuais em nome da promoção da segurança. No caso do Poder Executivo, os perigos são ainda mais agudos. No Reino Unido, por exemplo, os mesmos ministros do governo que são responsáveis pelas atividades dos serviços de inteligência, são também responsáveis pela autorização de mandados de interceptação, e fazem isso com base no parecer daquelas agências, sendo dificilmente uma salvaguarda confiável contra o abuso.

Além disso, em agosto de 2012 o Tribunal Constitucional da Coreia do Sul rejeitou a coleta de dados de assinantes de indivíduos na ausência de autorização judicial prévia, com base

em que isso equivaleria a "tratá-los como criminosos em potencial".[91] Esse entendimento foi seguido pela Comissão Nacional de Direitos Humanos da Coreia, que decidiu em abril de 2014 que a falta de qualquer requisito de autorização judicial prévia para o acesso aos dados coletados pela polícia viola os direitos humanos internacionais.[92] Também é de se destacar que o Comitê de Direitos Humanos da ONU, entre suas recomendações recentes relativas à vigilância da NSA, recomendou que o governo dos Estados Unidos estabelecesse "a participação do judiciário na autorização ou no monitoramento das medidas de vigilância".[93] Por essas razões, os Princípios endossam a visão de que apenas um juiz pode oferecer as garantias suficientes de independência e imparcialidade para assegurar que os poderes de vigilância são exercidos de forma tanto necessária quanto proporcional.

Contudo, na prática, apenas ter um juiz tomando decisões de vigilância não é suficiente para proteger os direitos fundamentais. Os Princípios também deixam clara a importância de ter juízes familiarizados tanto com as tecnologias envolvidas quanto com os princípios de direitos humanos, estando aptos para avaliar seu provável impacto sobre a privacidade individual. Da mesma forma, os juízes envolvidos devem ter recursos suficientes para desempenhar as funções que lhes são atribuídas, incluindo a supervisão *contínua* de todas as atividades de vigilância que tenham autorizado.

Um dos principais defeitos dos modelos existentes de autorização judicial prévia é o fato de que os pedidos de vigilância são feitos inevitavelmente *ex parte,* sem aviso prévio.[94] Em termos práticos, pouquíssimas aplicações são recusadas e um fator importante é, sem dúvida, a falta de qualquer tipo de desafio contraditório, pois os interesses da pessoa que é o objeto proposto da vigilância não são efetivamente representados. Em algumas jurisdições, no entanto, foram adotados vários mecanismos para tentar introduzir um elemento contraditório no processo. Um exemplo é o Monitor de Interesse Público de Queensland,

no qual sempre que um pedido de vigilância é feito, um advogado é automaticamente nomeado para representar os interesses da pessoa escolhida como sujeita à vigilância.[95] Outros casos podem envolver a nomeação de um defensor especial (como o usado em processos de imunidade de interesse público no Reino Unido e em outros locais), a fim de representar os interesses da pessoa que não tem conhecimento do pedido.[96] Esses modelos estão longe de serem perfeitos, mas representam tentativas de boa fé de se fazer o possível para impugnar eficazmente as decisões de vigilância secreta.

Outro princípio relevante nesse contexto é o Devido Processo Legal, ou seja, as decisões de vigilância não devem apenas ser feitas de acordo com a lei, mas também de uma maneira compatível com os direitos fundamentais do indivíduo afetado.[97] A autorização judicial prévia é uma garantia importante nesse sentido, mas muitos países preveem que os poderes de vigilância podem ser usados sem autorização judicial algumas vezes, em casos de emergência. Portanto, os Princípios exigem que a autorização retroativa deva ser solicitada dentro de um período de tempo razoavelmente possível, a fim de evitar o abuso de poderes de emergência. Eles também exigem pós-notificação das decisões de vigilância (ver Notificação de Usuário abaixo), de modo que as pessoas tenham a oportunidade de impugnar a legalidade, necessidade e proporcionalidade de qualquer decisão de vigilância que lhes diga respeito. Na ausência de um procedimento contraditório eficaz na autorização de vigilância, os Estados também devem considerar a introdução de mecanismos internos adequados para permitir que os pedidos de vigilância *ex parte* sejam adequadamente impugnados antes de a autorização ser concedida.[98]

Compartilhamento de dados, supervisão judicial e autorização prévia

Entre os muitos problemas causados pela coleta e retenção de dados de comunicações privadas em massa, um deles é

a falta de controles adequados sobre a partilha subsequente desses dados por diferentes agências governamentais, bem como entre os diferentes governos, como discutido acima. Um exemplo recente é a maneira na qual dados da NSA, supostamente coletados com a finalidade de combater as ameaças à segurança nacional, em vez disso tenham sido utilizados para repressão às drogas, para aplicação da lei habitual e fins de fiscalização tributária.[99] Na verdade, esses problemas podem surgir mesmo dentro de diferentes departamentos da mesma agência, como por exemplo a partilha de dados entre o setor de conformidades gerais das receitas fiscais do Canadá e suas divisões de investigações criminais, que operam sob restrições legais bem diferentes, refletindo os diferentes padrões que são aplicáveis em processos cíveis e criminais.

Esse problema de compartilhamento de dados irrestrito deve ser tratado não só através de medidas adequadas de proteção de dados, mas também por meio de supervisão judicial com mandados de busca, se for o caso, para permitir ao tribunal avaliar se é necessário e proporcional que as informações solicitadas sejam compartilhadas com outros órgãos públicos. Isso é diretamente abordado no princípio da proporcionalidade também.

PRINCÍPIO 8: NOTIFICAÇÃO DO USUÁRIO E O DIREITO A UM RECURSO EFICAZ

De acordo com a Lei Internacional dos Direitos Humanos, os princípios da Notificação do Usuário e da Transparência são mais bem compreendidos não só à luz do direito à privacidade, mas também como parte do direito a um recurso eficaz e a um julgamento justo.[100] Por isso é fundamental em qualquer sistema de justiça eficaz que onde existe um direito, haja um recurso (*ubi jus ibiremedium*).[101] Contudo, é impossível uma pessoa efetivamente impugnar uma interferência do governo em sua privacidade, se em primeiro

> lugar não sabe que é vítima dela. De maneira geral, a ausência de transparência relativa à aplicação da legislação que rege a vigilância secreta pode impedir o escrutínio democrático significativo dessas leis, deixando as agências de inteligência efetivamente como legisladoras de si mesmas.

Infelizmente, apesar de a Legislação Europeia exigir a Notificação do Usuário no contexto da proteção de dados em geral,[102] o Tribunal Europeu dos Direitos Humanos até agora não decidiu que a Notificação do Usuário é um requisito necessário em casos que envolvam a vigilância secreta.[103] Na verdade, no caso de 1979 de *Klass contra a Alemanha*, o Tribunal reconheceu que a falta de qualquer solicitação de pós-notificação significa que as decisões de vigilância são efetivamente não-judiciais, no que diz respeito à pessoa afetada:

> A própria natureza e lógica da vigilância secreta ditam que não só a fiscalização, mas também a revisão de acompanhamento, devem ser feitas sem o conhecimento do indivíduo. Consequentemente, uma vez que o indivíduo vai necessariamente ser impedido de buscar um recurso eficaz por sua própria vontade, ou de tomar parte direta em qualquer processo de revisão, é essencial que os procedimentos estabelecidos forneçam garantias adequadas e equivalentes para salvaguardar os direitos do indivíduo.

Em um caso posterior, em 2007, o Tribunal sugeriu que "assim que a notificação puder ser feita sem comprometer o objetivo da vigilância após o seu término, devem-se fornecer informações às pessoas em causa",[104] mas não chegou a constatação de que a notificação fosse uma exigência necessária das leis de vigilância em geral. Contudo nos 35 anos desde a decisão do Tribunal no caso *Klass*, tornou-se claro que não há "salvaguardas adequadas e equivalentes" para uma Notificação do Usuário eficaz. No Reino Unido, por exemplo, a esmagadora

maioria das decisões de vigilância baseadas no Regulamento da Lei de Poderes Investigatórios foram feitas sem prévia autorização judicial ou supervisão judicial eficaz com base *ex post facto*.[105] Como consequência do raciocínio do Tribunal no caso *Klass*, muitas decisões de vigilância escaparam tanto do escrutínio público quanto da supervisão judicial eficaz.

A abordagem falha tomada pelo Tribunal Europeu dos Direitos Humanos no caso *Klass* está, aliás, claramente em desacordo com a experiência das jurisdições nas quais os requisitos de Notificação do Usuário pós-vigilância têm vigorado por muitos anos. No Canadá, por exemplo, a lei limita o tempo de vigilância e escutas telefônicas e impõe a obrigação de notificar a pessoa sob vigilância no prazo de 90 dias após o fim da fiscalização, prorrogável até um máximo de três anos de cada vez.[106] Por esta razão, os Princípios salientam a necessidade de notificação na primeira oportunidade possível, estabelecendo uma lista exaustiva de circunstâncias que podem justificar atraso, somente quando a notificação puser seriamente em risco a finalidade da vigilância ou seja um risco iminente de perigo para a vida humana. Eles também exigem que qualquer atraso seja determinado pela autoridade judicial competente, o que implica, às vezes, que a notificação precise ocorrer mesmo antes que um risco ao propósito pelo qual foi autorizada a vigilância seja considerado "elevado".[107] Isso é feito porque as investigações sempre podem se estender indefinidamente, sem qualquer legitimidade. De fato, algumas Leis de escutas telefônicas reconhecem expressamente isso.

Na prática, qualquer sistema de Notificação do Usuário será inevitavelmente vulnerável a requerimentos *ex parte* das agências governamentais para atrasar ou impedir a notificação em casos específicos. A natureza desses requerimentos significa que será solicitado aos tribunais que determinem a necessidade de sigilo com base em informação unilateral, apresentada pelas autoridades. Portanto, para que o princípio da Notificação do Usuário funcione efetivamente, compete aos le-

gisladores criarem mecanismos para tornar acessíveis as decisões de vigilância para o exercício do contraditório, tanto quanto possível, conforme discutido na seção anterior sobre autorização judicial prévia.

Finalmente, é importante ter em mente que a Notificação do Usuário e a Transparência servem para interesses diferentes: o primeiro diz respeito ao fornecimento de informações suficientes sobre a decisão de vigilância, para permitir ao indivíduo afetado impugná-la ou buscar soluções; o último destina-se a assegurar que o público em geral tenha informações suficientes para avaliar se as leis que regem a vigilância estão funcionando eficazmente, incluindo se há garantias suficientes para o direito do indivíduo à privacidade. Isso será discutido na próxima seção.

Portanto, o princípio da Notificação do Usuário requer a notificação com tempo suficiente para possibilitar uma impugnação e só autoriza demora em circunstâncias específicas, autorizada por uma autoridade judiciária competente, para garantir que o atraso seja justificado e não superior ao estritamente necessário, para proteger uma investigação ou para proteger contra um risco à vida humana.

PRINCÍPIOS 9, 10: TRANSPARÊNCIA E ESCRUTÍNIO PÚBLICO

O princípio do escrutínio público está intimamente ligado à questão dos recursos nos casos individuais, mas é distinto desta: refere-se à importância da transparência para a democracia em geral. Em uma democracia, os cidadãos participam da elaboração das leis por meio de seus representantes eleitos. Portanto, é essencial que eles tenham informações suficientes sobre a forma como essas leis estão funcionando, a fim de tomar decisões informadas, seja nas urnas ou quando deliberarem com os outros sobre questões de política pública.[108] Também é essencial em uma democracia que os funcionários

públicos a quem tenha sido atribuído o poder de realizar uma vigilância sejam sujeitos a uma supervisão eficaz, a fim de garantir que esses poderes sejam usados legalmente em vez de arbitrariamente, e que eles permaneçam responsáveis perante o público em geral.[109]

A necessidade de garantir a transparência democrática é ainda mais importante nos casos em que, por razões operacionais, alguns aspectos do sistema permanecem em segredo e não estão sujeitas à supervisão judicial normal. Assim como o Tribunal Europeu dos Direitos Humanos considerou no caso *Klass*, os "poderes de vigilância secreta de cidadãos, caracterizados como exercidos pela polícia do Estado, são toleráveis nos termos da Convenção apenas na medida do estritamente necessário para salvaguardar as instituições democráticas".[110] Isso dá origem a dois requisitos fundamentais: primeiro, qualquer sistema de leis que rege a vigilância deve não apenas colocar restrições firmes em qualquer poder de apreciação atribuído aos funcionários públicos, como também a lei em questão deve ser "clara o suficiente em seus termos para dar aos cidadãos uma indicação adequada de sob quais circunstâncias e em que condições as autoridades públicas têm o poder de recorrer a esse tipo de interferência secreta e potencialmente perigosa ao direito de respeito à vida privada e à correspondência."[111] Em segundo lugar, as leis também devem fornecer garantias suficientes para evitar o risco de abuso de poder ou arbitrariedade.[112]

Como o Comitê de Direitos Humanos da ONU também notou, é importante que o Estado não apenas forneça garantias no papel, mas realmente realize verificações contínuas para analisar se essas salvaguardas funcionam na prática. O fracasso manifesto desse tipo de supervisão nos Estados Unidos, no Reino Unido e em outros lugares é uma das características mais marcantes das consequências das revelações de Snowden.[113] A lembrança da importância do bom funcionamento de órgãos de supervisão e monitoramento pela Comissão de Direitos

Humanos é de suma importância, e devidamente refletida nos Princípios.[114]

O escrutínio público também exige que os governos divulguem informações suficientes, claras e precisas ao público, para permitir uma avaliação séria da necessidade e proporcionalidade do uso de poderes de vigilância na prática.[115] Estatísticas opacas e sem sentido não podem servir a esse fim. Embora algumas questões operacionais precisem permanecer em segredo, em uma sociedade democrática isso nunca deverá levar ao uso inexplicável dos poderes de vigilância sem o escrutínio público e democrático.

Assim, os Princípios contêm requisitos relativamente detalhados e exigem uma supervisão independente. Eles também proíbem expressamente a interferência com os prestadores de serviços que buscam publicar informações como parte de seus esforços de transparência.

PRINCÍPIO 11: INTEGRIDADE DAS COMUNICAÇÕES E SISTEMAS

O direito à privacidade implica o direito das pessoas de construir meios de se comunicar uns com os outros de uma forma segura contra intrusões exteriores. O dever dos governos de respeitar a privacidade das comunicações também impõe uma obrigação correspondente a esses governos de respeitar a integridade de todos e quaisquer sistemas usados para transmitir comunicações privadas. No entanto, uma das revelações mais significativas este ano foi a extensão em que a NSA, o GCHQ e outros aparentemente trabalharam para minar a infraestrutura de comunicações globais, seja por obtenção de chaves de criptografia privadas para serviços comerciais, instalação de *backdoors* em ferramentas de segurança, seja minando os padrões chaves de criptografia invocados por milhões de pessoas em todo o mundo.[116] Em abril de 2013, o Relator Especial da ONU sobre Liberdade de Expressão observou

que "a segurança e o anonimato das comunicações também são prejudicados por leis que limitam o uso de ferramentas de proteção de privacidade que podem ser usadas para proteger as comunicações, como a criptografia".[117] Assim, ele recomendou que:

> Os indivíduos devem ser livres para usar qualquer tecnologia que escolherem para proteger suas comunicações. Os Estados não devem interferir no uso de tecnologias de criptografia, nem obrigar o fornecimento de chaves de criptografia.

Desta forma, o Princípio 11 reflete o requisito básico de que qualquer interferência na privacidade das comunicações deve não apenas ser lícita, mas também proporcional. Assim como seria irracional que os governos insistissem que todos os residentes de casas devessem deixar suas portas destrancadas, apenas no caso de a polícia precisar realizar uma busca numa propriedade em particular, ou exigissem que todas as pessoas instalassem câmeras de vigilância em suas casas, com base em que isso poderia ser útil em futuras acusações, é igualmente desproporcional aos governos interferir na integridade das comunicações de todos, a fim de facilitar suas investigações, ou para exigir a identificação dos usuários como condição prévia para a prestação de serviços ou a retenção de todos os dados do cliente.[118] Notadamente, nas suas observações sobre o Quarto Relatório Periódico sobre os Estados Unidos, conduzida como parte de sua Revisão Periódica Universal, os problemas inerentes a regimes de retenção de dados foram recentemente reconhecidos pela Comissão de Direitos Humanos, que afirmou que os Estados Unidos deveriam, entre outras coisas, "abster-se de impor a retenção obrigatória de dados por terceiros".[119] Desta forma, o pressuposto inerente por trás de tal interferência, de que todas as comunicações são potencialmente criminosas, contraria a presunção de inocência, um requisito fundamental da Lei Internacional dos Direitos Humanos.[120]

PRINCÍPIO 12: SALVAGUARDAS PARA A COOPERAÇÃO INTERNACIONAL

Com frequência cada vez maior, as atividades de vigilância dos Estados nas comunicações alcançam as fronteiras territoriais. Além das redes colaborativas de vigilância de comunicações de alcance global, conduzidas por muitas agências de inteligência estrangeiras e discutida em mais detalhes acima, a cooperação mais ampla entre os governos também inclui a cooperação mais formal entre as agências de aplicação da lei, inclusive através de Tratados de Assistência Legal Mútua (TALM).

A cooperação internacional entre governos levanta questões a respeito de como e quando os Estados poderão ser responsabilizados, nos termos das legislações nacional e internacional, pelas suas atividades de vigilância, que podem ter um impacto muito além de suas próprias fronteiras. Uma questão é a extensão na qual os Estados podem ser "extraterritorialmente" responsáveis por suas violações dos direitos humanos no exterior (por exemplo, a vigilância das comunicações privadas em outros países). É importante ter em mente, porém, que a tecnologia atual permite aos Estados monitorar um grande volume de tráfego internacional de dentro dos limites de suas próprias fronteiras. Portanto, é importante fazer uma breve referência à questão da jurisdição nos termos da Lei Internacional dos Direitos Humanos e as diferentes maneiras em que um Estado pode ser responsabilizado por suas ações, mesmo quando os efeitos são sentidos além de suas fronteiras.[121]

Uma área específica de preocupação é a prática não sancionada dos Estados de "puxar" os dados de servidores de outros países, sem o consentimento ou conhecimento desses governos. Depreende-se das revelações de Snowden, por exemplo, que as autoridades americanas podem exigir que as empresas sediadas nos Estados Unidos produzam tais dados de servidores que possuem ou que operam em outros países, e também podem direcionar essas empresas a não informarem às autoridades

dos países de onde eles retiram os dados, às entidades cujos dados estão entregando, nem mesmo às pessoas afetadas sobre tais divulgações obrigatórias de dados.

Não só essas práticas violam claramente os requisitos da legislação nacional de proteção de dados dos países dos quais os dados são retirados, mas também violam o princípio fundamental do Direito Internacional de que o Estado "não pode tomar medidas no território de outro Estado por meio de aplicação das legislações nacionais sem o consentimento deste último".[122] Como a Comissão de Direito Internacional disse:[123]

> No que diz respeito à jurisdição para a aplicação da lei, um Estado não pode impor a aplicação de sua lei criminal, isto é, *investigar* crimes ou prender suspeitos, no território de outro Estado, sem o consentimento do outro Estado. [Grifo nosso]

O canal adequado para a cooperação internacional nesses assuntos é por meio dos Tratados de Assistência Legal Mútua (TALM). Neste contexto, uma provisão do Conselho da Convenção Europeia sobre o Cibercrime, que sugere que a coleta de dados transnacional por agências de aplicação da lei pode ser possível com o consentimento, não do Estado de destino, mas com "o consentimento legal e voluntário da pessoa que tem a legítima autoridade para divulgar os dados para [o solicitante LEA]" (Art. 32 (b)), é altamente controversa. Na recente Conferência Octopus de Cooperação contra o Cibercrime (Estrasburgo, 4 a 6 de dezembro de 2013), decidiu-se analisar a elaboração de um novo protocolo, para tanto a Convenção sobre o Cibercrime ou o Conselho da Convenção de Proteção de Dados Europeu (ou um tratado inteiramente novo, em separado) resolverem esse problema.[124] Isso confirma que o acesso transnacional aos dados, e "puxar" os dados de outros países sem o consentimento destes ainda é visto como claramente contrário ao Direito Internacional Público e que o controverso artigo *Convenção sobre o Cibercrime*, por si só, não expressa tal consentimento.

PRINCÍPIO 13: SALVAGUARDAS CONTRA O ACESSO ILEGÍTIMO

O último princípio se baseia em uma série de normas internacionais relativas à proteção dos direitos de privacidade. Em primeiro lugar, o dever dos governos de deter a vigilância ilegal por meio de sanções penais e civis reflete as exigências da Lei Internacional dos Direitos Humanos para proteger os indivíduos de violações de sua privacidade, não só pelo Estado, mas também por particulares.[125] Em segundo lugar, a necessidade de vias de recurso reflete também as normas internacionais relativas ao direito a um recurso efetivo contra as violações dos direitos humanos.[126]

Em terceiro lugar, a necessidade de proteger eficazmente os denunciantes flui de diversos instrumentos internacionais, incluindo o artigo 19 do PIDCP e da Convenção das Nações Unidas contra a Corrupção (2005).[127] Vários especialistas da ONU enfatizaram a importância dos denunciantes em revelar o delito de autoridades públicas, bem como as violações aos direitos humanos. Em especial, o Relator Especial da ONU sobre a Liberdade de Opinião e Expressão ressaltou várias vezes que a denúncia é um aspecto importante do direito à liberdade de expressão.[128] Mais especificamente, o Relator Especial da ONU sobre a Promoção e Proteção dos Direitos Humanos e das Liberdades Fundamentais no Combate ao Terrorismo afirmou que os denunciantes são cruciais para "quebrar elos ilegítimos de sigilo" dentro dessas agências de inteligência e de segurança que estão cometendo violações aos direitos humanos, e que nestes casos, o interesse público na divulgação prevalece sobre o interesse público na não divulgação.[129] Ele afirmou ainda que os denunciantes devem ser protegidos de represálias legais e de ações disciplinares na divulgação de informações não autorizadas, e que são necessários mecanismos para a sua proteção.[130] Vários princípios, incluindo os *Princípios de Joanesburgo sobre Segurança Nacional, Liberdade de Expressão e Acesso à Informação*,[131] e os *Princípios Tshwane relativos a Segurança*

Nacional e o Direito à Informação[132] se aprofundam mais sobre os tipos de recursos e proteções que devem ser oferecidas aos denunciantes.[133]

Em quarto lugar, a obrigação de produzir provas inadmissíveis, obtidas de maneira inconsistente com os Princípios, sublinha a necessidade de garantir que todos os órgãos governamentais ajam em conformidade com os direitos fundamentais, o que é, por sua vez um requisito fundamental do Estado de Direito. Em alguns países, a regra de exclusão contra o uso de provas obtidas ilegalmente é absoluta, refletindo um princípio constitucional fundamental (ver, por exemplo, o "fruto da árvore venenosa", doutrina nos termos da legislação dos Estados Unidos.[134]) Em outras jurisdições, a regra não é necessariamente absoluta em sua natureza,[135] mas os meios ilícitos pelos quais as provas foram obtidas é sempre um fator importante para os tribunais levarem em consideração para determinar se a pessoa recebeu um julgamento justo.[136]

Quinto e último, a necessidade de destruir ou devolver o material obtido durante uma vigilância reflete as leis bem estabelecidas de proteção de dados em uma ampla gama de jurisdições.

NOTAS FINAIS

1 Para mais detalhes sobre o processo de consulta, ver Privacy International, "Towards International Principles on Communications Surveillance", referente à reunião de especialistas em Bruxelas em outubro de 2012, 21 de novembro de 2012, disponível em: **https://www.privacyinternational.org/blog/towards-international-principles-on-communications-surveillance**. Em seguida, foi organizada uma reunião pela Electronic Frontier Foundation no Rio de Janeiro, Brasil, em dezembro de 2012, com a participação do Relator Especial da ONU para a Promoção e Defesa do Direito à Liberdade de Opinião e Expressão, Frank La Rue: ver ONU – Documento A/HRC/23/40, § 10. A Electronic Frontier Foundation, a Privacy International e a Access fizeram uma consulta global, que terminou em janeiro de 2013, e nós, juntamente com diversas ONGs, advogados das áreas criminal, de direitos humanos e da privacidade, trabalhamos na revisão do texto até julho de 2013.

2 O texto completo dos Princípios Internacionais de Aplicação da Lei de Direitos Humanos à Vigilância das Comunicações está disponível em: **https://en.necessaryandproportionate.org/text**.

3 A lista completa de signatários está disponível em: **https://en.necessaryandproportionate.org/signatories**.

4 "Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies", *Liberty and Security in a Changing World,* 12 de dezembro de 2013, rodapé 120, disponível em: **http://whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf**.

5 Relatório Annual da Comissão Interamericana de Direitos Humanos, 31 de dezembro de 2014, disponível em: **http://www.oas.org/en/iachr/docs/annual/2013/informes/LE2013-eng.pdf**.

6 *Necessary and Proportionate*, "News", disponível em: **https://en.necessaryandproportionate.org/news**.

7 Somos muito gratos a todos que nos ajudaram na pesquisa e elaboração deste documento. Agradecemos particularmente a Douwe Korff, professor de Direito na área de Direitos Humanos Internacionais, por preparar uma versão anterior do documento e a Cindy Cohn, Gabrielle Guillemin, Tamir Israel, Dr. Eric Metcalfe e Katitza Rodriguez, por sua contribuição posterior. Nosso especial agradecimento às organizações Access, Privacy International, Asociación por los Derechos Civiles, Comisión Colombiana de Juristas, Fundación Karisma, Human Rights Information and Documentation System – HURIDOCS, The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic e Open Net Korea por analisar e compartilhar seus materiais. Enquanto tentávamos realizar uma ampla consulta, teríamos recebido de bom grado material extra de especialistas em legislação relevante da África e do Leste Europeu, de órgãos nacionais e regionais, que não foram tão bem representados nesta primeira versão do documento.

8 Para uma análise acadêmica mais aprofundada e jurisprudência mais extensa do Comitê de Direitos Humanos e outras fontes, ver Martin Scheinin & Mathias Vermeulen, "Unilateral Exceptions to International Law: Systematic legal Analysis and Critique of Doctrines that seek to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism," section 3.7 in *Denial of Extraterritorial Effect of Human Rights (Treaties)*, disponível em: **http://projects.essex.ac.uk/ehrr/V8N1/Scheinin_Vermeulen.pdf**.

9 Para se ter um exemplo, ver: G. Greenwald & E. MacAskill, "Boundless Informant: the NSA's Secret Tool to Track Global Surveillance Data", *The Guardian*, 11 de junho de 2013, disponível em: **http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining**. A NSA talvez seja o exemplo mais esclarecedor do escopo e da amplitude que possui uma agência de inteligência externa para potencializar a espionagem de indivíduos em todo o mundo através de redes interconectadas. Porém, muitos de seus parceiros no grupo dos Cinco Olhos estão estrategicamente localizados para suplementar o alcance da NSA com informações que trafegam (ou estão armazenadas) em sua próprio extensão. Para se ter exemplo, conferir: N. Hopkins, "Theresa May Warns Yahoo That Its Move to Dublin is a Security Worry", 20 de março de 2014, *The Guardian*, disponível em: **http://www.theguardian.com/technology/2014/mar/20/theresa-may-yahoo-dublin-security-worry**.

10 Privacy International, "Eyes Wide Open", Versão 1.0, 2013, disponível em: **https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/eyes_wide_open_v1.pdf**.

11 Ver, por exemplo, S. Ackerman & J. Ball, "Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ", *The Guardian*, 28 de fevereiro de 2014, disponível em: **http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo**: "Programas como o Nervo Óptico, que coleta informação em massa predominantemente de IDs de usuários anônimos, não conseguem filtrar informações de cidadãos do Reino Unido ou dos Estados Unidos."; John Foster, Chefe, Serviço de Segurança de Comunicações Canadense (CSEC), Depoimento ao Comitê do Senado de Segurança Nacional e Defesa, 41° Parlamento, 2° Sessão, 2013-14, 3 de fevereiro de 2014, disponível em: **http://www.parl.gc.ca/content/sen/committee/412/SECD/pdf/02issue.pdf**, p. 2-71: "Manteremos os metadados porque as comunicações passam por redes, as comunicações canadenses e estrangeiras se misturam. Quando se coleta metadados é impossível. Está tudo misturado, os bons cidadãos e os terroristas usam as mesmas redes. Então, quando se coleta, não temos como separar sem olhar; logo, nós usamos tais dados."

12 Comitê de Direitos Humanos da ONU (Human Rights Committee - HRC), Comentário Geral nº 31 [80], "A natureza das obrigações jurídicas gerais impostas aos Estados Partes no Pacto", 26 de Maio de 2004, CCPR/C/21/Rev.1/Add.13, disponível em: **http://www.refworld.org/docid/478b26ae2.html** [acessado em 30 de abril de 2014]

13 Por exemplo, de acordo com a Convenção Interamericana de Direitos Humanos, os estados devem: "230. [A]bster-se de tomar parte em ações ou favorecer práticas que possam ser dirigidas de alguma forma, direta ou indiretamente, a criar situações nas quais determinados grupos ou pessoas sejam discriminados ou arbitrariamente excluídos, de fato ou de direito, de gozar ou exercitar o direito à livre expressão. Do mesmo modo, os estados devem adotar medidas positivas (legislativa, administrativa ou de qualquer outra natureza), em condições de equidade e não discriminação, para reverter ou mudar situações discriminatórias já existentes que possam comprometer o efetivo gozo e exercício do direito à liberdade de expressão por certos grupos. Esse princípio também se aplica àqueles no poder ou efetivo controle de forças de um Estado Parte atuando fora do seu território, não importando em que circunstâncias tal poder ou controle efetivo tenha sido obtido." Ver IACHR. Relatório Anual 2008. Relatório Anual do Relator Especial para Liberdade de Expressão. Capítulo III (Quadro geral do ordenamento jurídico Interamericano do Direito à Liberdade de Expressão). OEA/Ser.L/V/II.134 Doc. 5 rev. 1. 25 de fevereiro de 2009. § 230, disponível em: **http://cidh.oas.org/annualrep/2008eng/Annual%20Report%202008-%20RELE%20-%20version%20final.pdf**. Ver também: Comissão Interamericana de Direitos Humanos. Gabinete do Relator Especial para Liberdade de Expressão. Liberdade de Expressão e a Internet. Registros oficiais OAS; OEA/Ser.L. OEA/Ser.L/V/II CIDH/RELE/INF.11/13, 31 de dezembro de 2013, pg. 8, disponível em: **http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf**.

14 Pacto Internacional de Direitos Civis e Políticos (International Covenant on Civil and Political Rights - "ICCPR"), Art. 2(1), Resolução da Assembleia Geral da Organização das Nações Unidas 2200A (XXI), Convenção para Proteção dos Direitos Humanos e Liberdades Fundamentais, com as alterações feitas pelos Protocolos No. 11 e No. 14, Roma, 4.XI.1950, ("Convenção Europeia de Direitos Humanos" ou "CEDH"), Art. 1; Convenção Americana de Direitos Humanos, Tratado OEA Séries No. 36, 22 de novembro de 1969, ("IACHR"), Art. 1.1. A Carta Africana de Direitos Humanos, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982) ("ACH&PR") por sua vez estipula que "os Estados Membros da Organização da Unidade Africana, partes da presente Carta devem reconhecer os direitos, deveres e liberdades consagrados neste Capítulo e devem se comprometer a adotar medidas legislativas ou de outra natureza para torná-los efetivos" (Art. 1).

15 (2005) 42 EHRR 1.

16 (2009) 48 EHRR 1.

17 No. 54934/00, 29 de junho de 2006.

18 O governo alemão alegou que a aplicação *ratione personae* era incompatível na medida em que o "monitoramento das telecomunicações feitas fora do país" era um "ato extraterritorial" e, portanto, fora da jurisdição da Alemanha, nos termos do Artigo 1º da CEDH. A CEDH, contudo, declinou de

enfrentar a aplicação nessa hipótese (ver parágrafo 72 da decisão), embora tenha finalmente enfrentado a aplicação em outras hipóteses.

19 Casos nos. 52/1979 e 56/1979, ambos de 29 de julho de 1981, §§ 12.3 e 10.3, respectivamente. Ver também as Observações Finais do Comitê nos relatórios de Israel em 1998 e 2003, mencionados em Scheinin e Vermeulen, o.c. (nota de rodapé 8, acima), pg. 37, nota de rodapé 81. Ver também o Comentário Geral 31, parágrafo 10.

20 CEDH, *Issa and Others v. Turkey*, julgamento de 16 de novembro de 2004, concluído em 30 de março de 2005, § 68.

21 Ver Observações Finais de 2006 do CDHNU no relatório dos Estados Unidos sob a égide do PIDCP; CCPR/C/USA/CO/3, § 10; e o relatório de 2011 dos Estados Unidos para o CDHNU no CCPR/C/USA/4, § 505.

22 Direito à Privacidade na Era Digital (Right to Privacy in the Digital Age – U.S. Redlines), disponível em: **http://columlynch.tumblr.com/post/67588682409/right-to-privacy-in-the-digital-age-u-s**.

23 Relatório do Comitê de Direitos Humanos sobre os Estados Unidos, 14 de março de 2014, disponível em: **http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=14383&LangID=E**.

24 Para mais informações, ver Electronic Frontier Foundation e Human Rights Watch, "Joint Submission to the Human Rights Committee," 14 de fevereiro de 2014, disponível em: **https://www.eff.org/files/2014/03/10/hrweffsubmission_on_privacy_us_ccpr_final.pdf**.

25 Assembleia Geral das Nações Unidas, "O Direito à Privacidade na Era Digital", novembro de 2013, A/C.3/68/L.45, **http://www.hrw.org/sites/default/files/related_material/UNGA_upload_0.pdf**.

26 Os "dados de comunicação" (ou "registros de comunicação") podem ser subdivididos em categorias diferentes, como "dados do assinante" e "dados de tráfego". Observe que o termo "metadados" é mais frequentemente utilizado na jurisprudência dos Estados Unidos, enquanto a jurisprudência da América Latina, do Reino Unido e da Europa referem-se mais aos "dados de comunicação" (que possui uma definição legal no Reino Unido na secção 21(4) do *Regulation of Investigatory Powers Act* (RIPA)). No entanto, o termo "metadados" tem sido cada vez mais utilizado no Reino Unido e na Europa: ver, por exemplo, *Practice Direction 31B of the Civil Procedure Rules in England and Wales*, que define metadados como "dados acerca de dados", ou a *INSPIRE Metadata Regulation* (EC) No 1205/2008 de 3 de dezembro de 2008. Sir David Omand, ex chefe do GCHQ, criticou publicamente a sugestão de que o termo "metadados", como utilizado na legislação dos Estados Unidos, seja equivalente à definição de "dados de comunicação" do RIPA. Contudo, em procedimentos atuais do Tribunal de Poderes Investigatórios relativos ao PRISM e ao TEMPORA, o governo britânico não sugeriu que haja alguma

informação definida pelo termo "metadados" e que não seja também definida pela definição legal de "dados de comunicação".

27 Na Coreia, por exemplo, os "dados de comunicação" ou "metadados" assim definidos incluem "registros de comunicação" acessíveis pela polícia apenas através de autorização judicial de acordo com o Decreto de Proteção do Segredo das Comunicações e os "dados de comunicação" disponibilizados para a polícia a critério dos provedores de serviços, que são regidos pela Lei de Empresas de Comunicações, tratam-se, na verdade, das informações que o assinante provê quando da assinatura dos serviços de comunicações. O *Código Criminal* canadense proíbe a interceptação de comunicações privadas, o que é geralmente interpretado como sendo aplicável ao conteúdo, não aos metadados (ou "dados de transmissão"). As informações de transmissão são protegidas pela constituição e normalmente precisam de autorização judicial para serem divulgadas. O governo canadense tentou introduzir a nova categoria de "informação do assinante" na legislação, o que obrigaria as empresas de telecomunicações a revelar tais informações quando diversas agências estatais as requisitassem. A lei, porém, não foi aprovada (M. Geist, "Lawful Access is Dead (For Now): Government Kills Bill C-30," 12 de fevereiro de 2013, disponível em: **http://www.michaelgeist.ca/content/view/6782/125/**. A legislação dos Estados Unidos também reconheceram a categoria "informação do assinante" em seu regime de Segurança Nacional de Correspondências, por exmeplo, que autoriza o FBI a constranger os provedores de comunicações a identificar clientes (revelar nome, endereço, tempo de serviço e informação de cobrança): D. Doyle, "National Security Letters in Foreign Intelligence Investigations: A Glimpse at the Legal Background", Congressional Research Service, 3 de janeiro 2014, disponível em: **https://www.fas.org/sgp/crs/intel/RS22406.pdf**.

28 Por exemplo, a Agência de Segurança Nacional dos Estados Unidos coletou *todos* os metadados de *todas* as chamadas telefônicas de empresas de telefonia norte-americanas através de pedidos renovados periodicamente e feitos pelo Tribunal de Vigilância de Inteligência Estrangeira (FISC). Para uma descrição do programa, ver: Privacy and Civil Liberties Oversight Board, "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court", 23 de janeiro 2014, pp. 8-10. Em resposta às preocupações com a privacidade, o presidente Obama anunciou recentemente a extinção próxima do programa de aquisição de metadados da NSA: C. Savage, "Obama to Call for End to N.S.A.'s Bulk Data Collection," 24 de março 2014, *New York Times*, disponível em: **http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html**. Um programa parecido envolvia a produção periódica de todos os metadados da *internet* a partir de uma certa data anterior, mas foi descontinuado em 2011: G. Greenwald & S. Ackerman, "NSA Collected US Email Records in Bulk for More than Two Years under Obama", 27 de junho de 2013, *The Guardian*, disponível em: **http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama**.

29 D. Gilbert, I.R. Kerr & J. McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunication Providers", [2006] 51 *Crim. L. Quart.* 469, disponível em: **http://iankerr.ca/wp-content/uploads/2011/08/the_medium_and_the_message.pdf**.

30 O equivalente a "registro de números telefônicos" na legislação norte-americana ou "números registrados" em outras jurisdições.

31 Ver Peter Sommer, *Can we separate "comms data" and "content"—and what will it cost?*, apresentação no evento "Scrambling for Safety" de 2012, disponível em: **http://www.scramblingforsafety.org/2012/sf2012_sommer_commsdata_content.pdf**.

32 Igualmente, o Grupo de Trabalho do Artigo 29 afirmou que "Também é particularmente importante notar que os metadados muitas vezes produzem informação mais facilmente que o conteúdo das comunicações em si": *ver* Grupo de Trabalho do Artigo 29, Opinião 04/2014 sobre a vigilância de comunicações eletrônicas para o propósito de inteligência e segurança nacional, 10 de abril de 2014, WP215 disponível em: **http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.**

33 Ver a declaração do Professor Edward Felten, ex chefe da área tecnológica da Comissão Federal de Comércio dos Estados Unidos, sobre o litígio entre a União Americana pelas Liberdades Civis em relação às revelações de Snowden, disponível em: **https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26 ACLU PI Brief - Declaration - Felten.pdf**. Ver também Amici Curiae Brief of Experts in Computer and Data Science in Support of Appellants and Reversal in ACLU v. Clapper, 2nd Circuit appeal, disponível em: **https://www.eff.org/document/computer-scientists-amicus-aclu-v-clapper**.

34 Ver, por exemplo, *Katz v. United States,* 389 U.S. 347 (1967), em que a Suprema Corte Americana argumenta que o monitoramento pelo FBI de chamadas telefônicas feitas de um telefone público corresponde a uma 'busca' autorizada pela Quarta Emenda.

35 *Smith v. Maryland*, 442 U.S. 735, 744 (1979). Como descrito mais abaixo, ao mesmo tempo em que falta proteção constitucional nos Estados Unidos, existem algumas proteções legais pela lei norte-americana para informações em posse de terceiros, até mesmo metadados, como por exemplo os estatutos que regem os dispositivos para detectar e seguir a pista (*pen register/trap and trace*). Estes são, porém, insuficientes pelos "Princípios Necessário e Proporcional", uma vez que a corte emite um mandado com base apenas quando se demonstra sua "relevância" para uma investigação. *Ver* 8 U.S. Code 3123 (para prováveis dados transacionais) e 18 U.S. Code 2703 (c), (d) (para informações armazenadas de comunicações já ocorridas).

36 Grupo de Análise do Presidente, "Liberty and Security in a Changing World", dezembro de 2013, página 121, citando os Princípiosa, disponível em: **http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf**.

37 18 U.S. Code 3123 (para prováveis dados transacionais) e 18 U.S. Code 2703 (c), (d) (para informações armazenadas de comunicações já ocorridas).

38 Decreto de Proteção ao Segredo das Comunicações da Coreia, Artigo 13, disponível em: **http://elaw.kiri.re.kr/en_service/lawPrint.do?hseq=21696**.

39 Ver, por exemplo, *Malone v. United Kingdom* (1985) 7 EHRR 14, § 84.

40 Ver, particularmente, Grupo de Trabalho do Artigo 29, *Opinião 4/2007 sobre o conceito de "dados pessoais",* 20 de junho de 2007, WP136, disponível em: **http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf**. Ver também Grupo de Trabalho do Artigo 29, *Opinião 4/2007 sobre a vigilância de comunicações eletrônicas para fins de inteligência e segurança nacional,* 10 de abril de 2014, WP215, disponível em: **http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf**.

41 Ver: *Digital Rights Ireland v. Ireland*, Joint Cases C-293/12 and C-594/12, 8 de abril de 2014, §§ 25-31: "Em tais circunstâncias, embora, como é evidente..., a diretiva não permita a retenção do conteúdo da comunicação ou informação consultada usando-se uma rede de comunicações eletrônicas, não é inconcebível que a retenção dos dados em questão possam ter um efeito no uso, por assinantes ou usuários registrados, dos meios de comunicação abrangidos por essa diretiva e, consequentemente, no exercício de sua liberdade de expressão garantida pelo Artigo 11 da Carta. A retenção de dados para fins de possível acesso a eles pelas autoridades nacionais competentes...afeta direta e especificamente a vida privada e, consequentemente, os direitos garantidos pelo Artigo 7 da Carta. Mormente, tal retenção de dados também se encontra sob a regência do Artigo 8 da Carta por constituir processamento de dados pessoais dentro do escopo do artigo; portanto, necessariamente deve satisfazer os requisitos de proteção de dados oriundos desse artigo. Ver também o § 37: "Fica declarado que a interferência causada pela Diretiva 2006/24 nos direitos fundamentais dispostos nos Artigos 7 e 8 da Carta é, como também foi colocado pelo Advogado-Geral, particularmente nos parágrafos 77 e 80 de seu Parecer, abrangente, e deve ser considerada particularmente séria.", referente ao Parecer do Advogado-Geral sobre o assunto (emitido em 12 de dezembro de 2013). O Artigo 7 da *Carta Europeia de Direitos Fundamentais* declara que "Todos têm o direito ao respeito por sua vida privada e familiar, lar e comunicação."

42 Dentre outras coisas, a legislação de proteção da UE está sujeita a um amplo princípio de "equilíbrio" que permite o processamento de dados

pessoais (não-sensíveis) sem consentimento e sem uma base legal clara contanto que os interesses sobre esses dados não "superem" os "interesses legítimos" do controlador, salvo quando o que constitui interesses "sensíveis" e "legítimos" não esteja claramente definido. Além disso, há exceções amplas que permitem o processamento de dados pessoais sensíveis quando é "necessário" proteger certos interesses mais amplos, inclusive a exclusão direta para fins de "segurança nacional".

43 *S and Marper v. United Kingdom* (2009) 48 EHRR 50, § 121. O caso referiu-se à retenção "ilimitada e indiscriminada" de amostras de DNA de pessoas from persons presas, mas não acusadas ou condenadas.

44 Apensos C 293/12 e C 594/12, 8 de abril de 2014, §§ 29 e 39. A Grande Seção do TJUE também concluiu que a retenção era uma interferência no direito à proteção de dados sob o Artigo 8 da Carta (ver *§* 36 de seu julgamento). No Caso C-70/10, *Scarlet Extended SA v. SABAM* (2010), o TJUE concluiu igualmente que um sistema de filtros proposto pelos detentores de direitos para combater a infração aos direitos autorais era ilegal, com base no fato de exigir que os provedores realizassem um "monitoramento preventivo" em tempo real das comunicações entre seus clientes, infringindo o Artigo 15(1) da Diretiva 2000/31 e propenso a infringir os direitos à proteção dos dados e à liberdade de expressão sob os artigos 8 e 11 da Carta Europeia de Direitos Fundamentais.

45 Ver Artigos 8-11 da CEDH, Artigos12, 17, 18, 19, 21 e 22 do PIDCP e Artigos 11, 12, 13, 15 e 16 da IACHR.

46 Isto pode ser notado especialmente em relação ao direito à privacidade. Por exemplo o Artigo 8 da CEDH se refere ao direito ao respeito à vida familiar e privada, ao lar e à correspondência, enquanto o Artigo e 7 da Carta da UE se refere ao direito ao respeito à vida privada e familiar, lar e *comunicações*. Para uma análise mais detalhada do direito à privacidade sob o PIDCP e outros instrumentos domésticos e regionais, ver Relator Especial da ONU na Promoção e Proteção dos Direitos Humanos e Liberdades Fundamentais na Luta Contra o Terrorismo, A/HRC/13/37, 28 de dezembro de 2009, § 11, disponível em: **http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf**.

47 Ver Relator Especial da ONU na Promoção e Proteção dos Direitos Humanos e Liberdades Fundamentais na Luta Contra o Terrorismo, *Ibid.*, § 16-18; ver também Relator Especial da ONU na Promoção e Proteção do Direito à Liberdade de Opinião e Expressão, A/HRC/23/40, 17 de abril de 2013, § 28-29.

48 Ver nota 45 acima. Outros artigos nos tratados de direitos humanos referem-se a "lei", "legalidade", ou "legal" como no Artigo 5 da CEDH (livre de prisão e detenção arbitrárias) e no Artigo 7 da CEDH (nenhuma punição sem lei).

49 Comitê de Direitos Humanos da ONU, Comentário Geral nº 16 (1988) em Instrumentos de Direitos Humanos, Volume I, Compilação dos Comentários Gerais e Recomendações Gerais adotadas pelos Órgãos dos Tratados de Direitos Humanos, HRI/GEN/1/Rev.9 (Vol. I) 2008 , pp 191-193, § 4. Veja também o Comitê dos Direitos Humanos da ONU, Toonen v. Australia, Comunicação nº 488/1992, § 8.3, CCPR/C/50/D/488/1992 UNODC (1994) e Van Hulst v the Netherlands, Comunicação nº 903/1999, § 7.6, U.N. Doc. CCPR/C/82/D/903/1999 (2004). Em ambas as comunicações, o Comitê observou que a razoabilidade exige proporcionalidade. De modo mais geral, consulte "ACLU Privacy Rights In the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights", março de 2014, disponível em: **https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf**.

50 Ver Comitê de Direitos Humanos da ONU, Comentário Geral nº 34 sobre as liberdades de opinião e de expressão (Artigo 19 do PIDCP), disponível em: **http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf**.

51 Julgamento no caso *Sunday Times vs. United Kingdom*, no. 6538/74; 26 de abril de 1979, § 49.

52 Em relação ao Artigo 17 do PIDCP, ver referências na nota 46 acima. O Tribunal Europeu de Direitos Humanos aplicou os princípios desenvolvidos ao abrigo do artigo 10 da CEDH (direito à liberdade de expressão) no caso *Sunday Times*, no caso *Silver and others v. the United Kingdom*, n. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25 de março de 1983, §§ 85-86, que diz respeito ao direito à privacidade dos prisioneiros nos termos do Artigo 8 da CEDH.

53 *Malone v the United Kingdom.* no. 8691/79, 2 de agosto de 1984, § 67.

54 *Ibid*., § 68.

55 *Silver and others v. the United Kingdom* citado acima*, §§* 85-86 e *Malone v. the United Kingdom* citado acima, § 67.

56 *Malone v. the United Kingdom*, § 67.

57 *Klass and Others v. Germany*, n. 5029/71, 6 de setembro de 1978, §§. 42 e 49. Particularmente, o Tribunal de Justiça sustentou que "o Tribunal, estando ciente do perigo que tal lei coloca de minar ou mesmo destruir a democracia com o argumento de defendê-la, afirma que os Estados contratantes não podem, em nome da luta contra a espionagem e o terrorismo, adotar quaisquer medidas que considerem adequadas". Ver também o Gabinete do Relator Especial para a Liberdade de Expressão da Comissão Interamericana de Direitos Humanos, Liberdade de Expressão e a Internet (OEA / Ser.L / V / . II , CIDH / RELE / INF 11/13, 31 de dezembro de 2013), § 150: "No que diz respeito à liberdade de expressão, a violação da privacidade das comunicações podem dar origem a uma restrição direta quando, por

exemplo, o direito não pode ser exercido de forma anônima, como consequência da atividade de vigilância. Além disso, a mera existência desses tipos de programas leva a uma limitação indireta que tem um efeito inibidor sobre o exercício da liberdade de expressão".

58 *Klass and Others v. Germany,* citado acima, § 37

59 Ver *Weber & Savaria v. Germany*, n. 54934, 29 de junho de 2006, §. 95.

60 Ver, especialmente, *Klass and Others v. Germany* citado acima, *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 de julho de 2008 e *Rotaru v. Romania*, no. 28341/95, [GC] de 4 de Maio de 2000, sobre a vigilância realizada pelas agências de inteligência. Para mais detalhes sobre a jurisprudência do TEDH sobre a vigilância, ver Ficha sobre a Proteção de Dados Pessoais, disponível em: **http://www.echr.coe.int/Documents/FS_Data_ENG.pdf**.

61 *Declaração Conjunta sobre os programas de vigilância e seu impacto sobre a Liberdade de Expressão*, emitido pelo Relator Especial das Nações Unidas sobre a Proteção e Promoção do Direito à Liberdade de Opinião e Expressão e pelo Relator Especial para a Liberdade de Expressão da Comissão Interamericana de Direitos Humanos Direitos, junho de 2013, §8 e 9, disponível em: **http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1**.

62 A/HRC/13/37, 28 de dezembro de 2009, disponível em: **http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf.**

63 Ver, por exemplo, o Artigo 19 do PIDCP (liberdade de opinião e expressão), referente ao respeito dos direitos e da reputação dos outros, [ou] à proteção da segurança nacional ou da ordem pública, ou da saúde ou da moral públicas; O Artigo 8 da CEDH (direito à privacidade) refere-se à "segurança nacional, segurança pública ou o bem-estar econômico do país, para a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e liberdades dos outros"; o Artigo 13 da CIDH (liberdade de expressão) se refere ao respeito dos direitos ou reputação de outros, à proteção da segurança nacional, da ordem pública, ou da saúde ou da moral públicas.

64 Ver nota de rodapé 46 acima.

65 Ver, por exemplo, *Klass and others,* citado acima, § 46

66 Uma rara exceção é o caso *Uzun v. Germany,* no. 35623/05, 2 de setembro de 2010; ver também *Peck v. the United Kingdom,* n. 44647/98, 28 de janeiro de 2003.

67 AHRC2340, relatório de 17 de abril de 2013, § 58, disponível em: **http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.**

68 *Ibid.*

69 Ver, por exemplo, no Canadá*: R. v. Oakes*, [1986] 1 S.C.R. 103; *R. v. Big M Drug Mart Ltd.*, [1985] 1 S.C.R. 295; Estados Unidos: *Austin v. Michigan Chamber of Commerce*, 494 U.S. 652, 655 (1990). *Boos v. Barry*, 485 U.S. 312, 334 (1988) (pluralidade); ver também *Burson v. Freeman*, 504 U.S. 191, 198 (1992) (pluralidade); *Board of Airport Comm'rs v. Jews for Jesus, Inc.*, 482 U.S. 569, 573 (1987); *Cornelius v. NAACP Legal Defense and Educ. Fund, Inc.*, 473 U.S. 788, 800 (1985); *United States v. Grace*, 461 U.S. 171, 177 (1983); *Perry Educ. Ass'n v. Perry Local Educators' Ass'n*, 460 U.S. 37, 45 (1983).

70 *Dictum* no Tribunal Constitucional de 27 de fevereiro de 2008 (1 BvR 370/07 e 1 BvR 595/07).

71 Ver, por exemplo, o Artigo 2 (1) PIDCP, Artigo 1.1 e 24 CIDH, o Artigo 14 da CEDH, o Artigo 2 da Convenção Internacional para a Eliminação de Todas as Formas de Discriminação Racial e o Artigo 2 da Convenção para Eliminação de Todas as Formas de Discriminação Contra as Mulheres. Ver também, por exemplo, *Carson and others v. United Kingdom* (2010) 51 EHRR 13, em que a Grande Câmara do Tribunal Europeu dos Direitos Humanos considerou que "outra situação" nos termos do Artigo 14 da CEDH inclui "país de residência" (§§ 70 -71).

72 Corte Interamericana de Direitos Humanos, Caso *Tristán Donoso contra Panamá*, Exceção Preliminar, Mérito, Reparações e Custas. Sentença de 27 de janeiro de 2009. Série C No. 193, § 56.

73 *Handyside v. the United Kingdom*, no. 5493/72, 7 de dezembro de 1976, §§ 48 e 49.

74 *Ibid.*, § 48.

75 *Klass v. Germany*, § 42.

76 Comentário Geral nº 27 de 1999, CCPR/C/21/Rev.1/Add.9, reproduzido em Instrumentos de Direitos Humanos, Volume I, Compilação dos Comentários Gerais e Recomendações Gerais adotadas pelos Órgãos dos Tratados de Direitos Humanos, HRI/GEN/1 / Rev.9 (Vol. I) 2008, pp 223-227, §§ 11-16.

77 Ver Comentário Geral nº 34 já referido, nota 20, § 34.

78 Ver referências na nota 46 acima.

79 Ver Comentário Geral nº 34, *ibid*.

80 Corte Interamericana de Direitos Humanos, Caso *Fontevecchia y D'Amico contra Argentina*, Mérito, Reparações e Custas. Sentença de 29 de novembro de 2011. Série C No. 238, § 53.

81 *S and Marper v. United Kingdom* (2009) 48 EHRR 50, § 118. O próprio governo britânico admitiu que a retenção de dados de DNA "não foi justificada por nenhum grau de suspeita de envolvimento dos candidatos em um crime ou propensão para o crime, nem direcionada à retenção de registros em relação a supostos crimes investigados no passado" (§ 94).

82 *Gillan and Quinton v. United Kingdom* (2010) 50 EHRR 45, §§ 86-87

83 Apensos C293/12 e C594/12, 8 de abril de 2014.

84 *Ibid*., § 56.

85 *Ibid*., § 58.

86 Privacy International, Electronic Frontier Foundation, Access, APC, ATIGO 19, Human Rights Watch et al, consulta OHCHR *em conexão com a Resolução da Assembleia Geral* 68/167 "O direito à privacidade na era digital", 1 de abril de 2014, disponível em: **https://www.eff.org/files/2014/04/17/ngo_submission_final_31.03.14.pdf**.

87 Ver, por exemplo, *Weber and Savaria v. Germany*, já referido no parágrafo 95, em que o Tribunal identificou várias "garantias mínimas que devem ser estabelecidas na lei estatutária, a fim de evitar 'abusos de poder'"(§ 95).

88 (1979-1980) 2 EHRR 214, § 55.

89 *Klass v. Germany*, já referido, n. 56.

90 *Kopp v. Switzerland* [1999] 27 EHRR 91, § 74.

91 Ver **http://news.mt.co.kr/mtview.php?no=2014041611218282360** (em coreano).

92 Ver a decisão do Tribunal Constitucional 2010 Hunma 47, 252 (consolidado), anunciada em 28 de agosto de 2012, e a subsequente decisão do Tribunal Superior Coreano em outubro de 2012 (Suprema Corte de Seul, 2011Na19012, Juiz Chefe Kim Sang-jun), que responsabilizou um grande portal responsável para a divulgação da identidade de um blogueiro para a polícia quando nenhum mandado foi produzido.

93 UNHRC, Concluding Observations on the 4th U.S. report, 27 de março de 2014, disponível em: **http://justsecurity.org/wp-content/uploads/2014/03/UN-ICCPR-Concluding-Observations-USA.pdf,** para. 22.

94 Para uma análise do potencial impacto de tais práticas, ver: KS Bankston, "Only the DOJ Knows: The Secret Law of Electronic Surveillance", (2007) 41 Univ. . S.F. L. Rev. 589, disponível em: **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2009442**.

95 Ver Eric Metcalfe, *Secret Evidence*, JUSTICE, junho de 2009, disponível em: **http://www.justice.org.uk/data/files/resources/33/Secret-Evidence-10-June-2009.pdf** at 177.

96 Ver *ibid* na p.173 para a discussão do modelo canadense e SIRC, p 231, para a apresentação de propostas de introduzir os defensores de interesse público. Agora é cada vez mais comum nos tribunais britânicos nomear defensores imunes de interesse público: ver, por exemplo. *CM (Zimbabwe) v Secretary of State for the Home Department* [de 2013] EWCA Civ 1303. Ver, mais recentemente, o relatório do Serviço de Pesquisa do Congresso, *Reform of the Foreign Intelligence Surveillance Courts: Introducing a Public Advocate,* 21 de março de 2014, disponível em: **http://www.fas.org/sgp/crs/intel/R43451.pdf**.

97 Ver, por exemplo, a discussão sobre a necessidade de autorização judicial prévia, no contexto de pesquisas de computador no julgamento do Supremo Tribunal do Canadá em R. v Vu, 2013 SCC 60, disponível em: **http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/13327/index.do**

98 Consulte a seção sobre Notificação de Usuário abaixo para mais detalhes.

99 Ver Jennifer Stisa Granick & Christopher Jon Sprigman, *NSA, DEA, IRS Lie About Fact That Americans Are Routinely Spied On By Our Government: Time For A Special Prosecutor*, 14 de agosto de, 2013, disponível em: **http://www.forbes.com/sites/jennifergranick/2013/08/14/nsa-dea-irs-lie-about-fact-that-americans-are-routinely-spied-on-by-our-government-time-for-a-special-prosecutor-2/**.

100 O direito a um julgamento justo é garantido pelo Artigo 10 da DUDH, Artigo 6 da CEDH, Artigo 8 da CIDH e Artigo 14 do PIDCP. O direito a um recurso efetivo é garantido nos termos do Artigo 8 DUDH, Artigo 15 da CIDH, Artigo 13 da CEDH e artigo 2.3 do PIDCP. De acordo com a Carta da União Europeia, ambos os direitos são protegidos nos termos do artigo 47.

101 Ver, por exemplo, *Ashby v White* (1703) 92 ER 126 por Lord Holt CJ: "É vão imaginar um direito sem um recurso, pois desejar um direito e desejar uma solução é recíproco."

102 Ver, em especial, o Artigo 8 do Conselho da Europa de 1981, *Convenção para a Proteção das Pessoas no que diz respeito ao Processamento Automático de Dados Pessoais* (Convenção n º 108) e artigos 10, 11 e 12, bem como 18 e 19 do CE 1995, a Diretiva que trata da proteção das pessoas relativamente ao processamento de dados pessoais e à livre circulação desses dados (Diretiva 95/46/CE). Para uma discussão mais ampla, ligada à evolução tecnológica, ver Douwe Korff, *Working Paper No. 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, preparado por Douwe Korff & Ian Brown, et al, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, estudo commissionado pela Comissão Europeia,

2010, disponível em: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf.

103 Ver *Klass v Germany* (1979-1980) 2 EHRR 214 , § 58: "Na opinião do Tribunal, tem de ser verificado se é mesmo viável, na prática, exigir a notificação posterior em todos os casos. A atividade ou perigo contra o qual uma determinada série de medidas de vigilância é dirigida pode continuar por anos, até mesmo décadas, após a suspensão dessas medidas. A notificação subsequente a cada indivíduo afetado por uma medida de suspensão poderia comprometer o objetivo de longo prazo que originalmente levou à vigilância. Além disso [...] tal notificação pode servir para revelar os métodos de trabalho e áreas de atuação dos serviços de inteligência e até, possivelmente, identificar seus agentes. Na opinião do Tribunal, na medida em que a 'interferência' que resulta da legislação é impugnada, em princípio é justificada nos termos do artigo 8 (2) [...] o fato de não informar o indivíduo após cessada a vigilância, não pode ser incompatível com esta disposição, uma vez que é este fato que assegura a eficácia da 'interferência'.

104 *Association for European Integration and Human Rights and Ekimdzhievv. Bulgaria*, 62540/00, 28 de junho de 2007, § 90. Ver também *Weber and Savaria v Germany, em que* o Tribunal reiterou que a notificação pode constituir uma salvaguarda importante, porém mais uma vez não uma condição necessária.

105 Ver *Freedom from Suspicion: Surveillance Reform for a Digital Age* (JUSTICE, outubro de 2011).

106 Ver Código Penal , R.S.C. de 1985, c. C -46 , Parte VI. A Parte VI funcionou eficazmente durante várias décadas, mostrando que os requisitos de notificação individuais são praticamente viáveis. Além disso, a Suprema Corte do Canadá tomou recentemente medidas no sentido de reconhecer que a obrigação de notificação individual é um imperativo constitucional sob a seção 8 da *Carta Canadense de Direitos e Liberdades*, que garante o direito de estar livre de busca e apreensão injustificadas: *R. v Tse* , 2012 SCC 16 , §. 11 (notificação individual, uma exigência constitucional para escutas telefônicas em que não há autorização judicial prévia por causa de circunstâncias exigentes); R. v TELUS Communications Co., 2013 SCC 16 , § 30 ("uma notificação foi necessária para atender as normas constitucionais mínimas da s 8". Proteções contra buscas e apreensões injustificadas, mas em *obiter*); *R. v Chehil* de 2013 SCC 49, § 58 ("o aviso após o fato, de investigações não sujeitas a autorização judicial prévia, é uma salvaguarda importante contra o abuso de tais poderes", referindo-se a cães farejadores de droga 'cheirando' a mala de alguém). A seção USC dos Estados Unidos 50 2518 (8) (d) exige aviso sobre escutas "dentro de tempo razoável, mas não após 90 dias a apresentação de um pedido de uma ordem de aprovação". No entanto, nenhum desses requisitos foi aplicado à vigilância conduzida sob as autoridades de inteligência estrangeiras.

107 Por exemplo, a Lei da Coreia, que permite atraso no Notificação do Usuário com a aprovação do Procurador-Chefe Regional, violará este princípio. Lei de Proteção ao Sigilo das Comunicações artigo 9-2 (5).

108 Ver Artigo 19, *The Public's Right to Know: Principles on Freedom of Information Legislation,* junho de 1999.

109 Ver também *Tshwane Principles on National Security and the Right to Information* para uma discussão da autoridade do Estado em reter informação do público em área de segurança nacional, disponível em: **http://www.right-2info.org/national-security/Tshwane_Principles**.

110 *Klass*, § 42. Ver também § 49: "O Tribunal, estando ciente do perigo constituído por uma lei de minar ou mesmo destruir a democracia com o argumento de defendê-la, afirma que os Estados Contratantes não podem, em nome da luta contra a espionagem e o terrorismo, adotar quaisquer medidas que considerem adequadas".

111 *Malone v United Kingdom*, §. 67

112 *Huvig v France* (1990) 12 EHRR 528, § 29-35.

113 Cindy Cohn, Mark Jaycox, *NSA Spying: The Three Pillars of Government Trust Have Fallen*, 15 de agosto de 2013, disponível em: **https://www.eff.org/deeplinks/2013/08/nsa-spying-three-pillars-government-trust-have-fallen**.

114 Ver também, por exemplo, Grupo de Trabalho do Artigo 29, Parecer 04/2014 sobre a vigilância das comunicações eletrônicas para fins de inteligência e segurança nacional, 10 de abril de 2014, WP215, disponível em: **http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.**

115 Veja-se, em particular, os Princípios 2 e 3 do Princípio Direito de Saber (nota 109 acima).

116 Ver Kurt Opsahl, Crucial Unanswered Questions about the NSA's BULLRUN Program, disponível em: **https://www.eff.org/deeplinks/2013/09/crucial-unanswered-questions-about-nsa-bullrun-program**.

117 Relatório do Relator Especial sobre a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão (A.HRC/23/40, 17 de abril de 2013), § 79.

118 Relatório do Relator Especial sobre a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão, Frank La Rue, 16 de maio de 2011, A/HRC/17/27, para. 84.

119 23 de abril de 2014, CCPR/C/USA/CO/4, § 22.

120 Vide, por exemplo, o Artigo 14 (2) PIDCP e o Artigo 6 (2). Em *S e Marper*, acima, a Grande Câmara observou que, embora "seja verdade que a retenção de dados privados dos requerentes não pode ser equiparada com a expressão das suspeitas", a presunção foi, todavia, relevante para a apreciação da proporcionalidade, na medida em que a percepção das pessoas cujos dados foram retidos "de que eles não estão sendo tratados como inocentes é agravada pelo fato de que os seus dados são mantidos por tempo indeterminado, da mesma forma como os dados de pessoas condenadas, enquanto que os dados de quem nunca foi suspeito de um crime são obrigatoriamente destruídos", (§ 122).

121 Para uma análise acadêmica mais aprofundada e referências mais amplas para a jurisprudência do Comitê de Direitos Humanos e de outras fontes, consulte Martin Scheinin & Mathias Vermeulen, "Exceções unilaterais de Direito Internacional: Análise jurídica sistemática e crítica das doutrinas que procuram negar ou reduzir a aplicabilidade das normas de direitos humanos na luta contra o terrorismo", seção 3.7 em Negação do Efeito Extraterritorial dos Direitos Humanos (Tratados), disponível em: **http://projects.essex.ac.uk/ehrr/V8N1/Scheinin_Vermeulen.pdf**.

122 Ian Brownlie, Princípios do Direito Internacional Público, 6 ª ed., 2006, p. . 306 A expressão clássica do princípio pode ser encontrada na adjudicação do único árbitro no caso *Palmas Island*, Max Huber: *"A soberania nas relações entre Estados significa independência. Independência em relação a uma parte do globo é o direito de exercer nela, com a exclusão de qualquer outro Estado, as funções de um Estado. O desenvolvimento da organização nacional de estados durante os últimos séculos e, como corolário, o desenvolvimento do direito internacional, estabeleceu este princípio da competência exclusiva do Estado no que diz respeito ao seu próprio território, de forma a torná-lo o ponto de partida na resolução ad maioria das perguntas que dizem respeito a relações internacionais."* Ilha de Palmas Case (Holanda / Estados Unidos da América), Prémio de 4 de Abril de 1928, UNRIAA, vol. II (1928), pp 829-871, na p. 838, disponível em: **http://legal.un.org/riaa/cases/vol_II/829-871.pdf**.

123 Relatório 2006 da Comissão de Direito Internacional, Anexo E (nota 83, acima), § 22, p. 526 [grifo nosso].

124 Na conferência, ver Conselho da Europa, Conferência Octopus - Cooperação contra o Cibercrime, 4 a 6 de dezembro de 2013, disponível em: **http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2013/Octopus2013_en.asp.** No momento da elaboração deste documento (dezembro de 2013), as atas e conclusões da conferência ainda não haviam sido lançadas, mas a necessidade de um novo protocolo foi amplamente acordada na sessão de encerramento, embora a natureza deste protocolo ainda não fosse muito clara—exceto que as opções de "consentimento" em um trabalho anterior, do ano de 2013, eram insuficientes (que se refere ao consentimento da pessoa em causa/suspeito,

que, concordamos não se pode presumir como sendo fornecidas voluntariamente; e sobre o consentimento de pessoas que possuem "autoridade legal" em divulgar dados [leia-se: provedores de internet e fornecedores de comunicações eletrônicas], que, concordamos, não estão em posição de fazer um julgamento relevante sobre a divulgação). A questão, portanto, será abordada em mais estudos.

125 Ver, por exemplo, o julgamento da Convenção Europeia dos Direitos Humanos, em *CAS* e *CS v Romania*, no. 26692/05, 20 de março de 2012, § 71: "obrigações positivas sobre o Estado são inerentes ao direito de efetivo respeito pela vida privada nos termos do Artigo 8; essas obrigações podem envolver a adoção de medidas, mesmo na esfera das relações dos indivíduos entre si".

126 Ver, por exemplo, o Artigo 2 (3) (a) do PIDCP e o Artigo 13 da CEDH.

127 Ver também o artigo 10 da CEDH. No caso seminal de *Guja v Moldova* (nº 14277/04, 12 de fevereiro de 2008), a Grande Câmara do TEDH considerou que a sinalização por um funcionário público ou um empregado no setor público de conduta ilegal ou má conduta no local de trabalho deve, em determinadas circunstâncias, ser beneficiada com proteção. O Tribunal passou a sustentar que, na análise de qualquer interferência sobre o direito de um denunciante à liberdade de expressão, deve ser dada atenção especial ao interesse público envolvido nas informações divulgadas (parágrafo 74) e no motivo por trás das ações do empregado reportado (parágrafo 77).

128 Ver, por exemplo, o Comitê das Nações Unidas sobre Direitos Humanos, Relatório do Relator Especial sobre a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão, Sr. Abid Hussain, apresentadas de acordo com resolução da Comissão 1999-1936 E/CN.4 / 2000/63. 18 de janeiro de 2000; ver também a Declaração Conjunta do Relator Especial das Nações Unidas sobre a Proteção e Promoção do Direito à Liberdade de Opinião e Expressão e Relator Especial para a Liberdade de Expressão da Comissão Interamericana de Direitos Humanos, 21 de junho de 2013.

129 Relatório do Relator Especial sobre a Promoção e Proteção dos Direitos Humanos e das Liberdades Fundamentais no Combate ao Terrorismo, Martin Scheinin, A/HRC/10/3, 4 de fevereiro de 2009, § 61.

130 *ibid*. Para mais informações e normas sobre denunciantes, consulte o Artigo 19, *USA must respect international standards on protection of whistleblowers*, disponível em: **http://www.article19.org/resources.php/resource/37133/en/usa-must-respect-international-standards-on-protection-of-whistleblowers**.

131 Em particular, os Princípios de Joanesburgo dispõem que ninguém pode ser punido por motivos de segurança nacional por divulgação de informações, se (i) a divulgação na verdade não prejudicar e não for passível de prejudicar um interesse de segurança nacional legítimo, ou (ii) o interesse

público em conhecer a informação se sobrepuser ao prejuízo da divulgação.

132 Os Princípios Tschwane preveem que a lei deve proteger contra retaliação aqueles denunciantes se, *inter alia*, o denunciante "acredita, com motivo razoável para tal, que havia um risco significativo de se fazer a divulgação interna e/ou a um órgão de supervisão independente resultar na destruição ou ocultação de provas, a interferência com uma testemunha, ou retaliação contra a pessoa ou um terceiro" e "acredita razoavelmente que o interesse público em ter a informação revelada supera qualquer prejuízo para o interesse público que resultaria da divulgação".

133 A lei dos EUA é particularmente fraca a este respeito: ver Trevor Timm, *If Snowden Returned to US for Trial, All Whistleblower Evidence Would Likely Be Inadmissible*, 23 de dezembro de 2013, disponível em: **https://huffingtonpost.com/trevor-timm/if-snowden-returned-to-us_b_4495027.html**. Além disso, enquanto a Lei de Proteção da Comunidade de Inteligência do Denunciante, em 1998, estabelece um procedimento para a comunicação interna dentro das agências e através do Inspetor Geral para os comitês de inteligência do Congresso, não prevê nenhuma solução para represálias que venham a ocorrer".

134 Ver *Silverthorne Lumber Co v United States*, 251 U.S. 385 (1920).

135 Ver, por exemplo, os julgamentos do Tribunal Europeu dos Direitos Humanos em *Schenk v Switzerland* (1988) 13 EHRR 242 e *Chinoy v United Kingdom*, no. 15199/89, 4 de setembro de 1991.

136 Ver, por exemplo, o julgamento do Tribunal Europeu dos Direitos Humanos, em *Khan contra Reino Unido* (2000) 31 EHRR 45, parág. 34: "A pergunta que deve ser respondida é se o processo como um todo, incluindo a maneira em que as provas foram obtidas, foram justas. Trata-se de um exame da 'ilegalidade' em questão e, onde a violação de uma outra Convenção de direito relaciona-se, e a natureza da violação encontrada".

necessaryandproportionate.org/LegalAnalysis