L. DIREITO À PRIVACIDADE

O DIREITO À PRIVACIDADE NAS SOCIEDADES DEMOCRÁTICAS
O DIREITO À PRIVACIDADE NA *INTERNET*
O DIREITO À PRIVACIDADE NO COMBATE AO TERRORISMO

"Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."
Artº 12º, Declaração Universal dos Direitos Humanos, 1948.

HISTÓRIA ILUSTRATIVA

Revelação de Dados Pessoais devido a Medidas de Segurança Desapropriadas

Em agosto de 2008, o Comissário para a Proteção de Dados da Irlanda recebeu uma queixa respeitante à alegada revelação de informações pessoais, por parte de uma companhia aérea. A queixosa afirmou que, em junho de 2008, na sequência de uma chamada telefónica, a companhia aérea revelou, através de correio eletrónico, um itinerário de viagem para si própria e para o seu marido, ao empregador do seu marido e que, como consequência, o seu marido foi despedido. A queixosa afirmou que o empregador do seu marido redigiu uma declaração a afirmar que a mensagem eletrónica referida foi enviada pela companhia aérea, após a mera indicação do apelido. Foi disponibilizada uma cópia desta declaração ao Comissário para a Proteção de Dados.
No decurso desta investigação, a companhia aérea informou o Comissário para a Proteção de Dados que foram realizadas as perguntas de segurança, antes do envio da mensagem eletrónica em questão à terceira parte. A companhia aérea não contestou o envio da mensagem eletrónica, porém, atendendo a que não gravou a chamada telefónica com o pedido de informações, nem se demonstrou que o sistema das perguntas de segurançativesse sido efetivado, não foi possível apresentar provas de que foram feitas, neste caso, as perguntas de segurança. O Comissário para a Proteção de Dados também considerou o facto de a reserva ter sido feita através do computador pessoal da queixosa, utilizando um endereço eletrónico pessoal e não um endereço eletrónico do local de trabalho do marido.
O Comissário para a Proteção de Dados, com base nas informações apresentadas, juntamente com o facto de que a companhia aérea não apresentou quaisquer provas de que as suas medidas de segurança foram, de facto, utilizadas nesta situação, decidiu, após a investigação desta queixa, que a companhia aérea infringiu a lei, ao processar as informações pessoais da queixosa e do seu marido e revelar ao empregador do marido o itinerário da viagem deles, através do uso de uma mera mensagem eletrónica. (Fonte: Irish Data Protection Commissioner. 2009. *Case Study 1: Disclosure of personal data due to inappropriate security measures.)*

Questões para debate

1. Quais são os direitos em questão?
2. Realizar um debate sobre os problemas relacionados com a revelação de informações delicadas.
3. Qual o sistema de proteção internacional a ser usado neste tipo de casos?

A SABER

1. INTRODUÇÃO

Desenvolvimento Histórico do Direito à Privacidade

O conceito de privacidade (em latim *privates* que significa separado do resto) indica que uma pessoa pode separar-se do resto e, desta forma, revelar-se. Apesar das fronteiras da privacidade divergirem culturalmente, partilham um entendimento básico comum.
O primeiro artigo sobre a privacidade, nos

EUA, foi publicado por Warren e Brandeis, em 1890. O âmago do **conceito liberal da liberdade** explica o direito à privacidade, tal como desenvolvido no final do século XVIII e durante todo o século XIX. A privacidade desenvolveu-se historicamente como uma zona isolada, manifestada em estruturas como a proteção do domicílio, da família e do segredo da correspondência. Devido ao surgimento da 'nova comunicação social', acrescentou-se o segredo da telecomunicação.

Desde então, a forma de se assegurar e proteger a privacidade mudou substancialmente, devido ao desenvolvimento tecnológico e especialmente desde o uso mais amplo da *internet*. Em particular, na última década, o significado e a compreensão de privacidade mudou devido ao *Web 2.0* e ao uso vasto das redes sociais.

Privacidade e Segurança Humana

Uma pessoa cuja privacidade seja significativamente afetada não pode viver uma vida sem medo e sem privação. Pressupõe-se a garantia da proteção básica dos direitos de privacidade para que se possa viver uma vida com segurança humana.

2. DEFINIÇÃO E DESENVOLVIMENTO DA QUESTÃO

A privacidade é protegida a nível internacional através de dois instrumentos essenciais, a **Declaração Universal dos Direitos Humanos (DUDH)** e o **Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP)**.

Refere o artº 12º da DUDH:

"Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."

O artº 17º do PIDCP é a disposição internacional mais importante no que respeita à privacidade. Refere o seguinte:

"1. Ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação.

2. Toda e qualquer pessoa tem direito à proteção da lei contra tais intervenções ou tais atentados."

O **Comité dos Direitos Humanos** tem a tarefa de monitorizar a implementação do PIDCP. Também apresenta Comentários Gerais sobre assuntos específicos respeitantes ao Pacto. O **Comentário Geral nº 16**, sobre o direito ao respeito da privacidade, família, domicílio e correspondência e proteção da honra e reputação (art.º 17º), de 1988, e o **Comentário Geral nº 19**, sobre a proteção da família, direito ao casamento e igualdade dos cônjuges (artº 23º), de 1990, são especialmente relevantes para a área da proteção da privacidade.

Tal como mencionado no Comentário Geral nº 16, o artº 17º protege o direito de todos contra as interferências na sua privacidade, arbitrárias ou ilegais. De acordo com o Comité dos Direitos Humanos, estes direitos têm de ser protegidos contra **interferências do Estado**, mas também contra **violações por outras pessoas, singulares**

ou jurídicas. O Comité estabelece um entendimento amplo do termo **'família'** de forma a abranger não apenas a família 'típica', de um casal casado e com filhos, mas também outros tipos de família. O artº 17º do PIDCP não contém uma cláusula de limitações específica.

Conteúdo do Direito à Privacidade

O direito à privacidade pode dividir-se em vários **subgrupos**, nos termos do artº 17º do PIDCP, ou seja, o direito à privacidade, identidade, integridade, intimidade, autonomia, comunicação e sexualidade.

- **Privacidade:**

O direito à privacidade, em sentido estrito, tal como adotado no artº 12º da DUDH, protege o campo específico da existência individual que não toca a esfera de privacidade dos outros. Também pode ser compreendido como o elemento que não cai em nenhuma das categorias que a seguir se mencionam.

- **Identidade:**

A identidade inclui 'características' pessoais, tais como o nome, aparência, indumentária, cabelo, género, código genético, assim como a confissão religiosa ou crença de cada um.

- **Integridade:**

A integridade pessoal também se encontra protegida pelo artº 17º do PIDCP. Tal significa que, por exemplo, um tratamento médico sem o consentimento ou mesmo contra a vontade do paciente deve considerar-se como uma infração ao direito à privacidade.

- **Intimidade:**

A intimidade encontra-se, em primeiro lugar, assegurada pela proteção ao domicílio e à correspondência, assim como através da proteção de dados. Uma pessoa encontra-se protegida contra a publicação, sem consentimento prévio, das suas especificidades pessoais.

- **Autonomia:**

Esta abrange a área de realização pessoal dos seres humanos. É o direito ao seu próprio corpo, que também confere o direito a agir contra o próprio corpo, incluindo o direito a cometer suicídio.

- **Comunicação:**

Esta área abrange a interação com as outras pessoas e confere, além da proteção especial da família, um direito a desenvolver relações com outras pessoas.

- **Sexualidade:**

A autonomia sexual é uma parte especial e particularmente importante do direito à privacidade. Qualquer regulação dos comportamentos sexuais constitui uma interferência no direito à privacidade. Apenas é permitida a interferência se for absolutamente necessária à proteção das pessoas afetadas (por exemplo, das crianças).

(Fonte: Manfred Nowak. 2005. *CCPR Commentary, artº 17º CCPR*.)

Grupos Especialmente Vulneráveis

- **Pessoas com deficiência**

As pessoas com deficiência que necessitem de cuidados especiais e de ajuda são, muitas vezes, suscetíveis de sofrerem interferências nos seus direitos à privacidade, por exemplo, se estiverem em instalações fechadas.

- **Pessoas afetadas por doenças e os idosos**

As pessoas afetadas por doenças ou os idosos a viverem em hospitais, clínicas

ou lares enfrentam um risco particular de afetação do seu direito à privacidade.

- **Crianças**

No que respeita aos novos meios de informação, as crianças são suscetíveis de sofrer infrações aos seus direitos à privacidade se revelarem informações pessoais em redes sociais ou na *internet* em geral.

Direitos Humanos das Crianças

3. PERSPETIVAS INTERCULTURAIS E QUESTÕES CONTROVERSAS

A Erosão do Direito à Privacidade devido a Políticas de Combate ao Terrorismo

Os Estados, ao lidarem com as políticas atuais de combate ao terrorismo, dão, frequentemente, ênfase à existência de **duas novas dinâmicas** que têm de ser consideradas em conjunto com a proteção do direito à privacidade. Em primeiro lugar, os Estados defendem que a sua capacidade para prevenir e investigar atos de terrorismo está fortemente relacionada, quase unicamente com o **aumento dos poderes de vigilância**. Por este motivo, a maior parte da legislação de combate ao terrorismo, após os ataques terroristas de 11 de setembro de 2001, tem-se centrado no aumento dos poderes de vigilância dos governos. Em segundo lugar, os Estados consideram que, pelo facto de o terrorismo ser uma questão global, a busca de terroristas não pode ser limitada pelas **fronteiras nacionais**. O auxílio de terceiros, potencialmente na posse de quantidades extensivas de informação sobre os indivíduos, constitui um recurso rico para se identificar e monitorizar os suspeitos de terrorismo. Como resultado destas perspetivas, os Estados que não possuem salvaguardas constitucionais ou legais têm podido transformar radicalmente e expandir as suas leis relativas à vigilância, com apenas algumas restrições. Nos países que possuem essas salvaguardas constitucionais e legais, os governos questionaram a proteção do direito à privacidade ao não aplicarem e transformarem as salvaguardas existentes, por força da cooperação com países terceiros ou com privados, ou ao substituírem os sistemas de vigilância doméstica por outros extraterritoriais.

Os Estados podem fazer uso de medidas específicas de vigilância legais, mas apenas se for uma situação de **interferência específica resultante de um processo** com fundamento em causa provável ou se existirem **motivos razoáveis** e em **respeito absoluto pelos direitos humanos**. O primado do Direito exige que exista uma base factual, relacionada com o comportamento de um indivíduo, que justifique a suspeita de que esteja envolvido em atividades criminosas. Os desenvolvimentos nos últimos anos demonstraram que tem havido um aumento desproporcionado da vigilância das comunicações, pelos serviços de informação e pelas entidades responsáveis pelo cumprimento da lei, em todo o mundo. Existe uma atribuição de importância inegável às novas tecnologias (por exemplo, as "escutas" e as tecnologias de vigilância que podem aceder à posição geográfica de telefones móveis, a tecnologia que informa os governos sobre o conteúdo de conversações de texto privadas, de usuários da Voz sobre o Protocolo de Internet (VoIP), ou que instala programas espiões nos computadores dos suspeitos, de forma a permitir o acesso remoto aos computadores). Em alguns países, foram até banidas as tecnologias de encriptação, que tornam as

comunicações mais seguras, porém, mais difíceis de serem intercetadas.
(Fonte: United Nations. 2009. *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*.)

Primado do Direito e Julgamento Justo

Tipos de vigilância usada, detenções e condenações através de interceções instaladas, de 1 de janeiro até 31 de dezembro de 2011, nos EUA.

Jurisdições	Despachos para a instalação de interceções	Linhas (incluindo quaisquer tipos de telefone: fixo, celular, móvel)	Oral (incluindo microfone)	Eletrónico (incluindo *pager* digital, fax, computador)	Combinação	Pessoas detidas	Pessoas condenadas
Total	2189	2092	6	4	87	3547	465
Federal	367	358	0	1	8	1006	47

(Fonte: US Courts Statistics 2011, www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/Table6.pdf.)

Poderes Ampliados para Parar, Interrogar e Inspecionar
Os Estados aumentaram as suas atividades de identificação, examinação e rotulação do **público em geral**, sob a desculpa de "medidas de combate ao terrorismo". Assim, utilizam várias técnicas que podem violar o direito à privacidade do indivíduo: quando a vigilância se realiza em locais públicos e se refere a grupos mais alargados de pessoas, as medidas de vigilância ficam, tipicamente, sujeitas a regimes mais fracos de autorização e supervisão judicial. Os padrões de direitos humanos existentes foram flexibilizados, retorcidos e rompidos, através do uso de interceções e de buscas, através da ampliação da **vigilância** das finanças, comunicações e **dados** de viagens, através do uso de **perfis** para a identificação de potenciais suspeitos, através da compilação de diversas listas e **bases de dados** para calcular a probabilidade de atividades suspeitas e identificar os indivíduos considerados passíveis de serem objeto de uma maior vigilância. Durante os últimos anos, aplicaram-se técnicas ainda mais inovadoras, como por exemplo, a recolha de **dados biométricos** ou o uso de **examinadores do corpo** que podem ver através das roupas.

A tendência geral alarmante é a de os Estados aumentarem os seus poderes para intercetar, questionar, inspecionar e identificar indivíduos e reduzirem, em simultâneo, os controlos jurídicos internos para a prevenção do **uso incorreto destes poderes**. Estes poderes deram origem a preocupações quanto aos **perfis étnicos e à discriminação** em diversos países e preocupações de que estes novos poderes causem tensões sérias entre os cidadãos e o Estado.

(Fonte: United Nations. 2009. *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.*)

 *Antirracismo e Não Discriminação*

O Uso da Biometria e os Perigos dos Sistemas de Identificação Centralizados

O uso de **técnicas de biométrica**, tais como o reconhecimento facial, as impressões digitais e a examinação da íris, constitui uma componente chave das novas políticas de identificação. Devido ao aumento da recolha de informações biométricas, a percentagem dos erros e falhas pode aumentar significativamente. Tal pode resultar na **criminalização errada** de indivíduos, assim como na exclusão social. Para além disso, contrariamente a outros identificadores, os biométricos não podem ser revogados. Uma vez copiados e utilizados de forma errónea por uma parte, não é possível dar a um indivíduo uma nova assinatura biométrica. Também relacionado com esta questão é de mencionar que, contrariamente à sua objetividade científica, a prova do DNA também pode ser falsificada. A recolha centralizada de biométricos apresenta o risco de multiplicar os erros judiciários que podem ser ilustrados pelo exemplo que se segue:

"Após os ataques bombistas de Madrid, em 11 de março de 2004, a polícia de Espanha conseguiu uma impressão digital numa bomba que não explodiu. Os peritos em impressões digitais do Departamento Federal de Investigação dos Estados Unidos da América - United States Federal Bureau of Investigation (FBI) – declararam que a impressão digital de um advogado correspondia à amostra encontrada no local do crime. A impressão digital da pessoa encontrava-se no sistema nacional de impressões digitais pelo facto de ter sido soldado dos Estados Unidos. O indivíduo foi detido em reclusão solitária, durante duas semanas, mesmo não sendo sua a impressão digital. Os examinadores não analisaram suficientemente a correspondência, tendo a situação piorado quando se descobriu que o advogado tinha defendido um terrorista condenado, era casado com uma imigrante egípcia e se tinha convertido ao islamismo."

(Fonte: *United Nations. 2009. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.)*

Circulação de Listas de Vigilância

Outra técnica disponível é a **monitorização das listas de vigilância**. De mencionar, desde já, a **Resolução 1267 do Conselho de Segurança** da Organização das Nações Unidas, adotada por unanimidade, em 1999, fazendo referência a diversas outras Resoluções [1189 (1998), 1193 (1998) e 1214 (1998)], sobre a situação no Afeganistão. O Conselho estabeleceu um regime de sanções a abranger indivíduos e entidades associadas à Al-Qaida, Osama bin Laden e/ou aos Talibãs, independentemente da sua localização, conhecido por "**Comité de Sanções contra a Al-Qaida e os Talibã".** O regime foi, desde então, reafirmado e modificado por uma dúzia de outras Resoluções do Conselho de Segurança das Nações Unidas [incluindo as Resoluções 1333 (2000), 1390 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008) e 1904 (2009)], de forma a que as sanções podem agora ser aplicadas a indivíduos designados e a entidades associadas à Al-Qaida, Osama bin Laden e/ou aos Talibãs, independentemente da sua localização. Desde a invasão do Afeganistão pelos EUA, em 2001, que as sanções

têm sido aplicadas a indivíduos e a organizações em todas as partes do mundo.
(Fonte: *United Nations Security Council Counter Terrorism Committee*, http://www.un.org/en/sc/ctc/rights.html.)

Em 19 de dezembro de 2006, o Conselho de Segurança adotou a **Resolução 1730 (2006),** para estabelecer um **procedimento de remoção da lista**. Quem constasse da lista poderia solicitar ao Comité que este reconsiderasse o seu caso. O procedimento de listagem permaneceu indefinido até 22 de dezembro de 2006, altura em que o Conselho de Segurança adotou a **Resolução 1735 (2006)**. Esta Resolução estabeleceu uma série de formulários para os países preencherem, de forma a colocarem na lista nomes de pessoas e entidades com ligações aos Talibãs.
O Conselho de Segurança também estabeleceu o **Gabinete do Provedor**, através da Resolução 1904 (2009), para assistir o Comité na consideração dos pedidos de remoção da lista.
(Fontes: Tessa Van Lieshout. 2006. *The United Nations and the fight against terrorism; United Nations Security Council Committee pursuant to Resolutions 1267 (1999) and 1989 (2011) concerning Al-Qaida and associated individuals and entities.*)

Primado do Direito e Julgamento Justo

Recolha de Dados em Bases de Dados Centralizadas
Apesar das novas técnicas biométricas poderem, em determinadas circunstâncias, ser instrumentos legítimos para a identificação de suspeitos, a questão do armazenamento de biométricos fora de um documento de identidade, como por exemplo, o passaporte, mas numa **base de dados centralizada,** constitui um motivo de preocupação. Tal prática aumenta os **riscos de insegurança na informação** ao deixar os indivíduos vulneráveis em relação ao Estado.
Por este motivo, em 2009, as Nações Unidas foram solicitadas, por diversos Comissários para a Proteção dos Dados e da Vida Privada, para *'preparar um **instrumento juridicamente vinculativo**, a estabelecer com clareza e em pormenor os direitos à proteção dos dados e à privacidade como direitos humanos a serem efetivados'*. Desde então, os governos estão convidados a adotarem instrumentos jurídicos nestes termos, assim como o Conselho da Europa, de acordo com o artº 23º da Convenção do Conselho da Europa para a Proteção dos Dados, que se encontra em processo de revisão. Porém, têm de fazer uma tentativa séria de avançarem, ao nível internacional, na melhoria dos padrões universais de proteção da privacidade, não apenas no interesse de protegerem os direitos individuais, mas também – embora não de forma equitativa – no interesse de baixarem as barreiras ao fluxo de dados através das fronteiras.
Por outro lado, têm havido alguns desenvolvimentos a nível nacional que conduziram ao aumento das preocupações, mesmo em algumas das sociedades mais liberais. Por exemplo, o Comité Especial sobre a Constituição da Câmara dos Lordes, no Reino Unido, afirmou: *"A vigilância é uma parte incontornável da vida no Reino Unido. Cada vez que fazemos uma chamada telefónica, enviamos uma mensagem eletrónica, navegamos na internet ou mesmo caminhamos na nossa avenida, os nossos atos podem ser monitorizados e gravados. Para dar uma resposta ao crime, combater a ameaça do terrorismo e melhorar a eficácia administrativa, os governos que se*

têm sucedido no Reino Unido construíram gradualmente um dos sistemas de vigilância mais abrangentes e avançados tecnologicamente do mundo. Em simultâneo, o setor privado tem sofrido desenvolvimentos semelhantes que contribuíram para uma mudança profunda no modo de vida neste país. O desenvolvimento da vigilância eletrónica e a recolha e processamento de informações pessoais tornaram-se invasivas, rotineiras e quase dadas como garantidas. Muitas destas práticas de vigilância são desconhecidas da maioria das pessoas e as suas consequências potenciais não são totalmente apreciadas."

(Fontes: Peter Malanczuk. 2009. *Data, Transboundary Flow, International Protection; 31st International Conference of Data Protection and Privacy Commissioners*. 2009. *Standards on Privacy and Personal Data*.)

Privacidade na *Internet* – as Redes Sociais

Atendendo ao rápido desenvolvimento da tecnologia de informação e à expansão das **redes de comunicação globais** (por exemplo, o *Facebook* tinha 901 milhões de utilizadores em abril de 2012), a regulamentação internacional adequada da circulação de dados transnacional e a harmonização das leis internas respetivas irão permanecer como prioridades nas agendas legislativas, nos anos vindouros. Existem múltiplas questões jurídicas ligadas à questão do crescimento célere dos sítios de redes sociais, sendo uma delas a **proteção de dados pessoais** e a questão da **privacidade** em geral.

Os sítios de redes sociais (por exemplo, o *Facebook*, o *Twitter*, o *Friendster*, etc.) oferecem aos seus utilizadores uma forma fácil de partilharem informações sobre si próprios e sobre outros. Porém, muitos utilizadores apercebem-se rapidamente que a informação que pretendem partilhar apenas com os seus amigos pode terminar nas **mãos das autoridades, de estranhos, dos meios de comunicação social e do público em geral**. Por exemplo, **os recrutadores de trabalho** verificam estes sítios com o propósito de acederem às origens de potenciais empregados. A pesquisa através destes sítios pode trazer uma quantidade substancial de informações pessoais sobre uma pessoa. A política de alguns sítios, imposta com vigor, sobre o uso do nome real em determinadas redes sociais piora o problema. Relacionado com esta questão está a possibilidade de qualquer pessoa, das centenas de "amigos" de um utilizador, poder descarregar as informações que queira e usá-las onde e como quiser (por exemplo, imagens). A realidade demonstra que o acesso abrange mais do que os amigos e membros. Os utilizadores têm de compreender que qualquer pessoa, como potenciais empregadores, autoridades responsáveis pelo cumprimento da lei, etc., pode aceder a fotografias, comentários e informações colocadas nas páginas de perfil. Porém, estas informações referem-se à imagem que uma pessoa pretende transmitir ao mundo fora da rede. É frequente que os utilizadores que esperam que as suas informações sejam vistas apenas por pessoas que conhecem, sejam surpreendidos com a forma como os seus dados pessoais são disseminados. O problema principal é que uma vez **publicados** na *internet*, ficam com **pouco ou nenhum controlo** sobre eles.

Os termos de privacidade estabelecidos por defeito, em contas individuais, permitem que se mostrem muitas informações a quem veja o perfil. Assim, 'o modelo de privacidade', isto é, as definições apropriadas da privacidade por defeito, já incluídas

nos sítios e programas, seriam a solução preferível para a proteção suficiente dos dados pessoais.

As características pessoais, como as partilhadas em *blogs* e comentários, podem ser acedidas por qualquer pessoa que veja a página do perfil. Se os operadores dos sítios de redes sociais colocassem as definições de privacidade por defeito, a um nível de proteção mais elevado, os utilizadores iriam ganhar imediatamente mais controlo sobre os seus dados pessoais. As políticas de privacidade, tais como os contratos, deveriam ser claras e de fácil acesso para que os utilizadores tivessem uma noção clara do conteúdo em questão. Infelizmente, as políticas de privacidade dos sítios e os termos de uso aparecem frequentemente com um excesso de referências cruzadas e são desnecessariamente complicados. Tal torna a tarefa de leitura da informação mais difícil do que teria de ser.

Em abril de 2012, o Comité de Ministros do Conselho da Europa adotou uma **Recomendação sobre a proteção dos direitos humanos em relação aos mecanismos de busca**, estabelecendo que os Estados Partes devem acautelar a transparência na forma como a informação é recolhida através dos mecanismos de busca, aumentar a transparência na recolha de dados pessoais, etc.

(Fontes: Council of Europe. 2012. *Recommendation on the protection of human rights with regard to search engines;* Peter Malanczuk. 2009. *Data, Transboundary Flow, International Protection*.)

Pornografia Infantil

A **Convenção sobre os Direitos da Criança**, que entrou em vigor em 1990, é o primeiro documento juridicamente vinculativo sobre os direitos humanos das crianças. O **artº 16º** adota a mesma linguagem que a DUDH, para garantir os direitos à privacidade das crianças.

A Convenção sobre os Direitos da Criança exige aos governos que protejam as crianças de todas as formas de exploração sexual ou abuso e tomem todas as medidas possíveis para assegurarem que estas não sejam raptadas, vendidas ou traficadas. Complementando esta Convenção, o **Protocolo Facultativo** à Convenção sobre os Direitos da Criança relativo à **Venda de Crianças, Prostituição Infantil e Pornografia Infantil** exige aos Estados Partes que proíbam a venda de crianças (também para propósitos não sexuais – tais como outras formas de trabalhos forçados, adoção ilegal e doação de órgãos), a prostituição infantil e a pornografia infantil e punam estas ofensas com penas adequadas. Este Protocolo Facultativo tem, presentemente, 143 Estados Partes (maio de 2011).

Direitos Humanos da Criança

4. IMPLEMENTAÇÃO E MONITORIZAÇÃO

Na maioria dos países, as normas básicas de direitos humanos estão estabelecidas na Constituição. A Constituição normalmente também estabelece vias para se invocar as normas de direitos humanos perante os **tribunais** internos, no caso de alegada violação destes direitos. A nível internacional, têm-se concluído **tratados de direitos humanos** para se proteger estes direitos. Sempre que um Estado se torne parte destes tratados é obrigado a implementar e garantir o cumprimento das suas normas a nível interno. O direito internacional não indica a forma como o Estado irá implementar essas normas, tal irá depender da sua ordem jurídica interna.

A Organização das Nações Unidas

Alguns tratados de direitos humanos, tais como o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), estabelecem um mecanismo de supervisão para a monitorização da implementação das normas de direitos humanos. Este mecanismo consiste num **sistema de relatórios** que os Estados têm, obrigatoriamente, de apresentar, com periodicidade regular, a um órgão de monitorização internacional sobre a forma como implementam as normas do tratado.

O Comité dos Direitos Humanos é um órgão de **peritos independentes** que monitoriza a implementação do PIDCP pelos Estados Partes do Pacto. Todos os Estados Partes estão obrigados pelo Pacto a submeter **relatórios** regulares ao Comité, sobre a forma como implementam os direitos. Os Estados têm de apresentar um relatório inicial, um ano após acederem ao Pacto, e depois sempre que o Comité solicite um relatório (normalmente, em cada quatro anos). O Comité examina cada relatório e apresenta as suas preocupações e recomendações ao Estado Parte, sob a forma de "**Observações Finais**".

Para além do procedimento dos relatórios, o artº 41º do Pacto estabelece que o Comité pode considerar um sistema de queixas entre Estados, as **comunicações inter-Estados**. Para além disso, o **Primeiro Protocolo Facultativo ao Pacto** atribui ao Comité a competência para também examinar as **comunicações** de indivíduos, respeitantes a alegadas violações da Convenção por parte dos Estados Partes do Protocolo.

O Comité dos Direitos Humanos publica ainda a sua interpretação do conteúdo das normas de direitos humanos, sob a forma de Comentários Gerais, em relação a assuntos temáticos específicos. Por exemplo, no seu **Comentário Geral nº 16: O direito ao respeito da privacidade, da família, do domicílio e da correspondência e à proteção da honra e da reputação (artº 17º)** refere o seguinte:

"Mesmo em relação a interferências que estejam em conformidade com o Pacto, a legislação relevante deve especificar em pormenor as circunstâncias precisas em que tais interferências são permitidas. A decisão da admissão de uma tal interferência é tomada exclusivamente pela autoridade designada nos termos da lei e analisada caso a caso. O cumprimento do artº 17º exige que se garantam, 'de jure' e 'de facto', a integridade e a confidencialidade da correspondência. Deve proibir-se a vigilância, seja eletrónica ou de outra forma, as interceções telefónicas, telegráficas ou através de outras formas de comunicação, as escutas telefónicas e a gravação de conversas. As buscas domiciliárias devem restringir-se a buscas de provas necessárias e não devem permitir-se se constituírem uma perseguição. A recolha e conservação de informações pessoais em computadores, bases de dados e outros dispositivos, seja por autoridades públicas ou por particulares ou organismos, devem ser reguladas por lei. Os Estados têm de adotar medidas eficazes para garantirem que as informações sobre a vida privada de uma pessoa não cheguem às mãos de pessoas que não estejam autorizadas por lei para as receberem, processarem e usarem e que nunca sejam usadas para fins incompatíveis com o Pacto. Cada indivíduo deve também poder saber quais as autoridades públicas, pessoas singulares ou

entidades privadas que controlam ou que podem vir a controlar os seus ficheiros. Se os ficheiros contiverem dados pessoais incorretos ou se tiverem sido recolhidos ou processados de forma contrária à lei, cada indivíduo deve ter o direito de pedir a sua retificação ou eliminação."

O Relator Especial das Nações Unidas para a Promoção e Proteção dos Direitos Humanos e Liberdades Fundamentais no Combate ao Terrorismo

Os diversos desenvolvimentos da situação dos direitos humanos em todo o mundo, desde 11 de setembro de 2001, têm sido bem documentados. Os ataques do 9/11 foram seguidos por uma onda de ataques racistas contra muçulmanos e árabes, apenas devido à sua aparência, em todo o mundo. Os governos também responderam com medidas legislativas abrangentes. Muitos Estados adotaram leis a criminalizarem condutas, a banirem determinadas organizações, a congelarem valores, a restringirem liberdades civis e a reduzirem as salvaguardas contra as violações de direitos humanos. Isto conduziu a uma tendência perigosa para a legitimação das violações de direitos humanos, com o pretexto do combate ao terrorismo. Os Estados que reagiram com exagero à ameaça colocada pelo terrorismo arriscaram a violação dos direitos humanos, não apenas dos alegados terroristas, mas também dos seus próprios cidadãos, cujos direitos e liberdades poderão, por isso, ter ficado diminuídos.

Com o estabelecimento da Direção Executiva do Comité Contra o Terrorismo (*Counter-Terrorism Committee Executive Directorate*, CTED), através da Resolução 1535 (2004) do Conselho de Segurança, o Comité começou a avançar para uma política mais proactiva no respeitante aos direitos humanos. O CTED foi mandatado para comunicar com o Alto Comissariado das Nações Unidas para os Direitos Humanos (ACNUDH) e com outras organizações de direitos humanos em questões relacionadas com o combate ao terrorismo e foi, também, nomeado um perito em direitos humanos para o Comité. Adicionalmente, em abril de 2005, com a Resolução 2005/80 da Comissão de Direitos Humanos, foi nomeado um **Relator Especial para a promoção e proteção dos direitos humanos e liberdades fundamentais no combate ao terrorismo.** No seu Relatório de 2009, refere-se, de forma exaustiva, ao direito à privacidade e à sua erosão nas medidas do combate ao terrorismo: uma vez que um indivíduo esteja a ser formalmente investigado ou examinado por uma agência de segurança, as informações pessoais são partilhadas entre agências de segurança por razões de combate ao terrorismo, ficando o direito à privacidade quase automaticamente afetado. Estas são situações em que os Estados têm o poder legítimo para limitar o direito à privacidade, nos termos do quadro jurídico internacional dos direitos humanos. Porém, o combate ao terrorismo não legitima automaticamente qualquer interferência com o direito à privacidade. Qualquer instância de interferência tem de ser sujeita a uma avaliação crítica. O artº 17º do PIDCP constitui a mais importante norma de tratados, juridicamente vinculativa, sobre o direito humano à privacidade, a nível global.

(Fontes: OHCHR. 2007. *Human Rights, Terrorism and Counter-terrorism*; Tessa van Lieshout. 2006. *The United Nations and the fight against terrorism.;* United Nations. 2009. *Report of the Special Rap-*

porteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.)

Convenções Regionais e Órgãos de Monitorização
Esforços da União Europeia

Em 1995, o Conselho da União Europeia ("Conselho da UE") e o Parlamento Europeu adotaram a Diretiva 95/46/EC, relativa à Proteção das Pessoas Singulares no que diz Respeito ao Tratamento de Dados Pessoais e à Livre Circulação desses Dados **("Diretiva de Proteção de Dados"**), para a harmonização das leis nos Estados-membros da UE. A Diretiva de Proteção de Dados foi adotada com dois propósitos, o de garantir a **proteção de dados** dos indivíduos e o de remover os obstáculos à **livre circulação** de dados pessoais entre Estados-membros da UE. A Diretiva de Proteção de Dados aplica-se ao processamento de informações pessoais em ficheiros eletrónicos e manuais.

Os direitos incluem:

- o direito à correção dos dados inexatos,
- o direito à prevenção dos processamentos ilegais, e
- o direito a optar, sem custos, a não receber diretamente anúncios de vendas.

Exige-se o consentimento expresso do indíviduo para o uso comercial e governamental de dados pessoais delicados relacionados com a saúde, vida sexual, convicções religiosas ou filosóficas. Esta Diretiva aumentou a pressão sobre os países fora da UE para adotarem leis restritivas semelhantes de proteção de dados pessoais, para assegurar que determinados tipos de circulação de informação continuam na Europa.

Em 1997, o Parlamento Europeu e o Conselho da UE adotaram a Diretiva suplementar 97/66/EC, relativa ao Tratamento de Dados Pessoais e à Proteção da Privacidade no setor das Telecomunicações **("Diretiva da Privacidade nas Telecomunicações")**, abrangendo os telefones, a televisão digital, as redes móveis e outros sistemas de telecomunicações. Com esta Diretiva, os portadores e fornecedores de serviços têm de assegurar a privacidade das comunicações dos utilizadores, incluindo as comunicações e atividades realizadas pela *internet*. A Diretiva da Privacidade nas Telecomunicações restringe o acesso aos dados das faturações e limita a atividade comercial, o que significa que uma vez que se complete uma chamada têm de ser eliminadas as informações recebidas pela realização da comunicação.

Em 2002, o Parlamento Europeu e o Conselho da UE adotaram a Diretiva 2002/58/EC, relativa ao Tratamento de Dados Pessoais e à Proteção da Privacidade no setor das Comunicações Eletrónicas **(Diretiva relativa à Privacidade e às Comunicações Eletrónicas)**. Os Estados Partes têm de adotar legislação que estabeleça a exigência da conservação dos dados de tráfego e dados de localização de todas as comunicações efetuadas através de telefones móveis, mensagens de SMS, linhas de telefones fixos, faxes, correio eletrónico, salas de conversação, *internet* ou de qualquer outro dispositivo de comunicações eletrónicas. Estas medidas podem ser implementadas com fundamentos diversos, incluindo a segurança nacional, a prevenção do crime e o cumprimento da lei. A Diretiva relativa à Privacidade e às Comunicações Eletrónicas inclui disposições novas para a proteção de chamadas, comunicações, dados de tráfego e de localização para possibilitar um aumento significativo da privacidade. Abrange to-

das as informações transmitidas através da *internet* ("tráfego"), embora o "*spam*", isto é, a publicidade comercial através do correio eletrónico não solicitada nem consentida, seja proibido e os utilizadores dos telefones móveis estejam protegidos do sistema de localização e de vigilância por agências estatais.

Em 2006, a UE prosseguiu com a aprovação da **Diretiva 2006/24/EC**, do Parlamento Europeu e do Conselho, relativa à Conservação de Dados Gerados ou Tratados no Contexto da Oferta de Serviços de Comunicações Eletrónicas Publicamente Disponíveis ou de Redes Públicas de Comunicações, que altera a Diretiva relativa à Privacidade e às Comunicações Eletrónicas. Esta Diretiva, muito controversa, exige que os fornecedores armazenem os dados por um período entre seis meses e dois anos.

Em 2007, a UE e os EUA chegaram a um acordo sobre a transferência de dados financeiros pessoais da **Sociedade para Telecomunicações Financeiras Interbancárias Globais** (*Society for Worldwide Interbank Financial Telecommunications*-**"*SWIFT*"**), consórcio bancário com sede em Bruxelas, para o Departamento do Tesouro dos EUA, pelo que a *SWIFT* aderiu, deste modo, aos princípios do "porto seguro". A UE e os EUA também acordaram num mecanismo para a transferência dos **dados dos registos de identificação dos passageiros**: Acordo entre a União Europeia e os Estados Unidos da América sobre o processamento e a transferência de dados contidos nos registos de identificação dos passageiros, pelas transportadoras aéreas, para o Departamento da Segurança Interna dos Estados Unidos. Em 2006, o Tribunal de Justiça da União Europeia anulou um acordo similar sobre a mesma matéria (Parlamento Europeu c. Conselho da União Europeia e Comissão Europeia, 30 de maio de 2006).

Em 2012, esteve em debate **um projeto de regulamento sobre a proteção das pessoas singulares em relação ao processamento de dados pessoais e à circulação desses dados** e um **projeto de diretiva relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados.** O artº 16º do projeto de diretiva prevê o direito à eliminação dos dados pessoais quando o processamento dos dados não cumpra com o normativo.
[Fontes: European Commission. 2012. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).;* Peter Malanczuk. 2009. *Data, Transboundary Flow, International Protection.]*

Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais (CEDH)
O **artº 8º** da Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, de 1950, estabelece o seguinte:

> *1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.*

2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

A Convenção criou a Comissão Europeia dos Direitos Humanos e o **Tribunal Europeu dos Direitos Humanos** para monitorizarem o seu cumprimento. Ambos foram - e este tem sido - ativos na promoção do cumprimento dos direitos à privacidade, tendo, consistentemente, interpretado o artº 8º de forma extensiva e as restrições de forma estrita. No caso de X c. Islândia (*5 Eur. Comm'n H.R. 86.879*) a Comissão considerou, em 1976: *"Para muitos autores Anglo-Saxónicos e Franceses, o direito ao respeito da "vida privada" é o direito à privacidade, o direito a viver, tanto quando se pretenda, protegido da publicidade... Na opinião da Comissão, porém, o direito ao respeito da vida privada não termina aqui. Também abrange, até determinado limite, o direito a estabelecer e desenvolver relações com outros seres humanos, especialmente na esfera emocional para o desenvolvimento e a realização da personalidade."*
(Fonte: Magdalena Sepulveda, Theo van Banning et al. 2009. *Human Rights References Handbook.)*

Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal e Protocolo Adicional

A Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal e Protocolo Adicional, de 1981, tendo entrado em vigor em 1985, encontra-se aberta à assinatura por parte de quaisquer países no mundo. A Convenção, ratificada por 44 Estados até junho de 2012, foi o **primeiro instrumento internacional juridicamente vinculativo** com importância global sobre a proteção de dados. De acordo com a Convenção, os Estados-membros têm de adotar as medidas necessárias, nas suas ordens jurídicas internas, para aplicarem os princípios da Convenção, de forma a assegurar os direitos humanos essenciais relativos ao processamento de dados pessoais.

O Conselho da Europa também se encontra a lançar uma campanha de modernização da Convenção. Considerando que as informações pessoais se encontram constantemente a ser registadas, comunicadas e analisadas, muitas vezes sem o nosso consentimento e conhecimento, é necessário determinar a proteção jurídica dos nossos direitos fundamentais. A revisão da Convenção constitui um processo necessário, mesmo que exigente, numa altura em que as fronteiras entre a privacidade e a liberdade se encontram esbatidas.
Com o aumento da circulação de dados pessoais através das fronteiras nacionais, é necessário assegurar a proteção eficaz dos direitos humanos e das liberdades fundamentais e, em particular, do direito à privacidade. O Protocolo Adicional à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, respeitante às Autoridades de Supervisão e aos Fluxos

Transfronteiriços de Dados, entrou em vigor em 2004 (32 Estados Partes em junho de 2012). O Protocolo Adicional exige que os Estados Partes estabeleçam autoridades de supervisão que exerçam as suas funções em absoluta independência das autoridades estatais e que sejam um elemento para a proteção eficaz dos indivíduos em relação ao processamento dos dados pessoais.

Convenção Americana sobre Direitos Humanos

O artº 11º da Convenção Americana sobre Direitos Humanos descreve o direito à privacidade em termos semelhantes aos da Declaração Universal dos Direitos Humanos. Em 1948, a Organização dos Estados Americanos (OEA) proclamou a Declaração Americana dos Direitos e Deveres do Homem, apelando à proteção de vários direitos humanos, incluindo o direito à privacidade. O Tribunal Interamericano de Direitos Humanos começou a abordar questões de privacidade nos seus processos (por exemplo, Rivas Quintilla c. El Salvador, Oscar Elias Biscet e outros c. Cuba). (Fonte: Magdalena Sepulveda, Theo van Banning *et al.* 2009. *Human Rights References Handbook.*)

Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais

As Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, adotadas em 23 de setembro de 1980, representam o consenso internacional sobre as diretrizes gerais referentes à recolha e gestão de informações pessoais. Ao estabelecerem princípios fundamentais, as diretrizes desempenham um papel fundamental no auxílio a governos, a representantes de negócios e dos consumidores nos seus esforços para a proteção da privacidade e dos dados pessoais.

As diretrizes da OCDE estabelecem regras específicas não vinculativas que abrangem o tratamento de dados eletrónicos. Estas regras estabelecem que as informações pessoais têm de ser protegidas em cada passo, da recolha à armazenagem e disseminação. Os princípios e as formas de proteção dos dados variam nas diferentes declarações e leis, mas todos exigem que as informações pessoais sejam:

- obtidas de forma justa e legal;
- usadas apenas para o propósito específico original;
- adequadas, relevantes e não excessivas para o propósito;
- precisas e atualizadas;
- acessíveis ao sujeito;
- mantidas de forma segura e destruídas findo o seu propósito.

Carta Africana dos Direitos e Bem-Estar da Criança

A Carta prevê a proteção da privacidade no seu **artº 10º** ao referir que *"Nenhuma criança será sujeita a interferência arbitrária ou ilegal na sua privacidade, família ou correspondência, nem a ataques à sua honra ou reputação, desde que os pais ou responsáveis legais tenham o direito de exercer uma supervisão razoável em relação à conduta de seus filhos. A criança tem direito à proteção da lei contra tais interferências ou ataques."*

CONVÉM SABER

1. BOAS PRÁTICAS

Privacy.Org
O *Privacy.Org* é um sítio de notícias diárias, informação e iniciativas sobre a privacidade. Oferece uma visão geral sobre atividades relacionadas com a privacidade, sobre grupos preocupados com assuntos relacionados com a privacidade e sobre publicações. Este sítio é um projeto conjunto do Centro de Informações sobre Privacidade Eletrónica (*Electronic Privacy Information Centre* - EPIC) e da *Privacy International*.

Centro de Informações sobre Privacidade Eletrónica *(Electronic Privacy Information Centre*-EPIC)
O EPIC é um centro de investigação de interesse público, situado em Washington D.C.. Foi estabelecido em 1994, para questões emergentes sobre liberdades civis e para proteger a privacidade, a Primeira Emenda e os valores constitucionais.

Privacy International
É um grupo de direitos humanos constituído em 1990, como vigilante de governos e de empresas. *Privacy International* encontra-se sediada em Londres, na Inglaterra, e tem uma representação em Washington D.C.. *Privacy International* conduziu campanhas pelo mundo, sobre diferentes questões como escutas telefónicas e atividades de segurança nacional até cartões de identificação, vigilância de vídeo, correspondência de dados, sistemas de informação da polícia e privacidade médica.
(Fonte: Peter Malanczuk. 2009. *Data, Transboundary Flow, International Protection.*)

2. TENDÊNCIAS

Listas de Vigilância, Listas de "Não voa"
O tipo mais comum de listas de vigilância refere-se às listas "Não voa/selecionado". Normalmente, estas listas circulam entre as companhias aéreas e os funcionários de segurança, com instruções para deterem e interrogarem qualquer passageiro cujo nome esteja na lista. A amplitude do uso destas listas permanece secreta, porém, nos países onde estes sistemas são supervisionados publicamente têm surgido diversos erros e **preocupações de violações à privacidade**, particularmente, nos Estados Unidos e no Canadá. Permanecem as questões sobre a integridade dos dados, ainda que estas listas sejam verificadas continuamente para deteção de erros, os processos de identificação têm de realizar-se com muito cuidado.
A explicação oficial do motivo pelo qual estas listas são guardadas frequentemente em segredo é a de que poderiam deixar os terroristas suspeitos em sobreaviso. Porém, este sigilo levanta, simultaneamente, problemas de indivíduos a serem, continuamente, sujeitos a escrutínio sem saberem que fazem parte de uma lista e **sem existir uma supervisão independente eficaz**. Esta **vigilância secreta** constitui uma **violação do direito à privacidade**, nos termos do artº 17º do PIDCP. Se estas listas antiterrorismo fossem tornadas públicas, o artº 17º da Convenção seria desencadeado de outro modo. O Comité dos Direitos Humanos concluiu que *"a inclusão injustificada de uma pessoa na Lista Consolidada do Comité 1267 das Nações Unidas constitui uma violação do artº 17º. Considerou que a disseminação de informações pessoais constitui um*

ataque à honra e à reputação das pessoas constantes na lista, devido à associação negativa entre os nomes e o título da lista de sanções."

As listas de vigilância públicas e secretas podem violar, frequentemente, princípios fundamentais de proteção de dados. As informações, uma vez geradas para um propósito, são reutilizadas para propósitos secundários e, nalguns casos, até partilhadas com outras instituições sem o conhecimento ou consentimento das pessoas interessadas. Utilizam-se informações erróneas para decidir sobre as pessoas, o que resulta sobretudo em **restrições a viajar**, recusa de vistos, rejeição nas fronteiras ou proibição de embarcar num avião, sem que sejam apresentadas provas da prática de quaisquer infrações.

(Fonte: United Nations. 2009. *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*.)

Um exemplo é a história do Sr. Abousfian Abdelrazik:

"Abousfian Abdelrazik, um homem de Montreal que foi colocado na lista de vigilância do terror das Nações Unidas em 2006, mas nunca acusado de nenhum crime, continua a levar o seu caso a público. Abdelrazik foi preso, mas não condenado, durante uma visita, em 2003, ao Sudão para ver a sua mãe doente. No verão passado, ele foi, finalmente, autorizado a regressar ao Canadá, depois de seis meses no Sudão, que incluiram duas passagens pela prisão e 14 meses na portaria da Embaixada Canadiana. Impossibilitado de trabalhar por causa das sanções, Abdelrazik disse que tem vivido num limbo desde que foi a casa.

"Não fiz nada de errado", disse aos jornalistas. "Encontrei-me, numa manhã, nesta situação sem quaisquer acusações nem a apresentação de quaisquer provas."

Ottawa tem o poder, segundo uma Resolução do Conselho de Segurança das Nações Unidas, de punir qualquer pessoa que dê apoio material a Abdelrazik. Mesmo que este tivesse um cheque, não podia levantar fundos da sua conta bancária. Depois de uma batalha judicial, ele ganhou uma decisão que lhe permitiu realizar levantamentos mensais limitados, da sua conta da união de crédito.

Tanto a CSIS como a RCMP reconheceram que não têm provas contra Abdelrazik. O Departamento de Justiça Sudanês considerou, em 2005, que ele não tinha quaisquer ligações à Al-Qaida. Porém, os esforços para remover o seu nome da lista foram infrutíferos. O governo federal e outras autoridades têm continuado a aplicar as sanções. Ottawa citou a lista ao recusar a concessão, a Abdelrazik, de documentos para viajar, depois de ele ter sido libertado de uma prisão no Sudão, em que alega que foi torturado. Ele passou meses num limbo judicial na Embaixada Canadiana em Cartum.

Mary Foster, que acompanhou Abdelrazik numa campanha pelo país, disse que os seus problemas fazem parte de uma luta maior contra a islamofobia, o racismo e o "poder governamental arbitrário". Ela disse que "Não se trata apenas de um indivíduo, mas de muitos indivíduos, de países inteiros cheios de indivíduos".

Os advogados de Abdelrazik, com o apoio de grupos de liberdades civis, apresentaram um processo constitucional contra a lista de vigilância, conhecida como a lista 1267 das Nações Unidas. Ele processou

o Ministro dos Negócios Estrangeiros Lawrence Cannon e o Governo Federal, em $27 milhões. No seu processo, ele alega que o governo organizou a sua detenção arbitrária pelas autoridades sudanesas, encorajando ou tolerando a sua tortura às mãos das autoridades sudanesas e obstruindo ativamente o seu regresso ao Canadá, por diversos anos.

Melissa Lantsman, porta-voz de Cannon, disse que não podia comentar as especificidades do seu processo, por este se encontrar nas instâncias judiciais. Porém, disse que "cabe ao Sr. Abdelrazik" seguir os canais próprios para que o seu nome seja retirado da lista de vigilância. O Canadá tentou que o nome de Abdelrazik fosse removido da lista das Nações Unidas, em 2007, porém, tal foi rejeitado. Qualquer membro do Conselho de Segurança pode vetar um pedido de eliminação do nome da lista, sem oferecer explicações."

(Fonte: CBC News. 2010. *Montreal man on watch list rallies supporters.*)

Vista da Rua da *Google*

Quando a *Google* iniciou o seu projeto Vista da Rua, em 2007, levantaram-se muitas preocupações em relação à privacidade, porém, os debates centraram-se quase exclusivamente sobre a recolha e a exibição de imagens obtidas pelas câmaras digitais da Vista da Rua da *Google*. A *Google* também obteve uma quantidade vasta de **dados *Wi-Fi*** de recetores *Wi-Fi* que foram escondidos em veículos da Vista da Rua. Iniciaram-se investigações independentes e a *Google* reconheceu que tinha reunido endereços *MAC* e *SSIDs* de rede (o nome de identificação de rede atribuído ao utilizador), ligados a informações de localização para redes sem fios privadas.

A *Google* cessou a sua recolha ilegal de transmissões de dados *Wi-Fi* devido a muitos protestos em todo o mundo. A *Google* acabou por admitir, com o decurso das investigações, que tinha intercetado e armazenado dados de transmissão *Wi-Fi*, incluindo palavras passe de correio eletrónico e conteúdos de correio eletrónico: "*[...] nalgumas instâncias capturaram-se mensagens eletrónicas integrais e URLs, assim como palavras passe.*"

Em janeiro de 2011, conduziram-se investigações em, pelo menos, 12 países. Pelo menos 9 países consideraram a *Google* culpada de violar as suas leis. Um **tribunal Suíço**, por exemplo, considerou que a Vista da Rua da *Google* viola os direitos de privacidade. O tribunal superior da Suíça decidiu contra o serviço de mapa Vista da Rua da *Google*, forçando-a a ofuscar as caras e as placas de matrículas antes de colocar as imagens na *internet*. O tribunal Suíço referiu *"O interesse do público num registo visual e os interesses comerciais dos arguidos não se sobrepõem, de forma alguma, aos direitos sobre a imagem própria."*. Mais países, tais como o Reino Unido, a França e a Espanha consideraram que a *Google* violou leis de privacidade, na medida em que os carros da Vista da Rua recolheram dados *Wi-Fi* de redes sem fios privadas.

A **Comissão Nacional para Informática e Liberdades Civis da França (CNIL)** multou a *Google* em 100.000 Euros, por violar as regras sobre privacidade de França, a partir do momento em que os carros da Vista da Rua da *Google* recolheram endereços eletrónicos e palavras passe das pessoas, sem o seu conhecimento. A Comissão referiu como fundamentação para condenar à multa mais elevada que alguma vez atribuiu, *"as violações estabelecidas e a sua gravidade, assim como as vantagens económicas ganhas pela Google"*. Depois

de fixar a multa, a CNIL criticou a *Google* pela sua conduta durante a investigação: "*Eles nem sempre estavam dispostos a colaborar connosco, não nos deram todas as informações que pedimos, tal como o código de fonte de todos os dispositivos nos carros da Google*", disse Yann Padova, o diretor executivo da CNIL. "*Eles nem sempre foram muito transparentes.*"
Diversos outros países, incluindo o Reino Unido, o Canadá, a Alemanha e a Espanha, realizaram investigações similares e determinaram que a *Google* violou as suas leis de privacidade.
(Fonte: BBC. 2011. *France fines Google over Street View data blunder.*)

Redes Sociais
Os sítios da Rede relativos a redes sociais tais como o *Facebook*, o *MySpace*, o *Twitter*, o *Google Buzz*, o *LinkedIn* e o *Friendster* são fóruns estabelecidos para manterem em contato antigas amizades e para se conhecerem novas, para a partilha de informações pessoais e para se estabelecerem capacidades de comunicação móvel. Apesar destes sítios da Rede serem ferramentas úteis para a troca de informações, tem havido uma preocupação crescente com as quebras de privacidade, causadas por estes serviços de redes sociais, pois muitos dos utilizadores sentem que os seus dados pessoais estão a circular de uma forma muito mais abrangente do que desejariam.
Alguns fornecedores restringem o acesso ao sítio e, como consequência, o acesso às informações do utilizador. Muitas páginas incluem estipulações de idade nos seus termos de uso (o *Friendster*, por exemplo, exige que todos os seus utilizadores tenham mais de 16 anos de idade, o *Facebook* e o *MySpace* exigem que os utilizadores tenham, pelo menos, 13 anos). Mesmo assim, as informações digitais podem ser copiadas e distribuídas com facilidade a qualquer pessoa autorizada do grupo que passe as informações a outros. Além disso, os sítios são objeto de **partilha rotineira de informações dos utilizadores com terceiros para efeitos comerciais.**
(Fontes: BBC. 2008. *Facebook 'violates privacy laws';* EPIC, *Social Networking Privacy*, http://epic.org/privacy/socialnet/default.html; Irish Data Protection Commissioner. 2011. *Facebook Ireland Ltd – Report of Audit.*)

Base Nacional de Dados de ADN do Reino Unido
Durante os últimos anos, o Comité Especial sobre a Constituição da Câmara dos Lordes, no Reino Unido, aprovou uma expansão na Base Nacional de Dados de ADN, assim como a introdução ou desenvolvimento de novas bases de dados para uma variedade de serviços públicos e um aumento constante no uso de Câmaras em Circuito Fechado (*CCTV*), tanto no setor público como no privado. Tem havido uma expansão significativa e contínua dos aparatos de vigilância, tanto do Estado como do setor privado. Nas últimas décadas, eram relativamente incomuns as bases de dados informáticas e partilha de dados, a monitorização das comunicações eletrónicas, a identificação eletrónica e as Câmaras em Circuito Fechado, em recintos públicos. Hoje, estas tecnologias estão omnipresentes e exercem uma influência sobre muitos aspetos nas nossas vidas diárias. Para além disso, a vigilância continua a exercer uma influência poderosa sobre a relação entre os indivíduos e o Estado e entre os próprios indivíduos. A forma seletiva como, por vezes, é utilizada, ameaça discriminar certas categorias de indivíduos.

(Fonte: Peter Malanczuk. 2009. *Data, Transboundary Flow, International Protection.*)

Declaração Conjunta sobre a Liberdade de Expressão e a *Internet*
Em junho de 2012, os relatores especiais das quatro organizações internacionais a lidar com a liberdade de expressão, nomeadamente, as Nações Unidas, a Organização para a Segurança e Cooperação na Europa (OSCE), a Organização dos Estados Americanos (OEA) e a Comissão Africana dos Direitos Humanos e dos Povos (CADHP), emitiram uma Declaração Conjunta sobre a liberdade de expressão e a *internet*, a dar ênfase a determinados princípios chave para a liberdade de expressão na *internet*. Declararam, por exemplo, que as abordagens para a regulamentação de outras formas de comunicação não pode ser simplesmente transferida para a *internet*, devendo a regulamentação ser concebida de uma forma específica para este efeito.
(Fontes: OAS. 2012. *Press release - Freedom of expression rapporteurs issue joint declaration concerning the internet.;* Matthias C. Kettemann. 2012. *5 punchy principles for regulating the internet.*)

Proteção de Direitos Humanos em linha (*online*) e fora de linha (*offline*)
Em julho de 2012, o Conselho de Direitos Humanos das Nações Unidas confirmou, finalmente, que não existem diferenças entre a proteção dos direitos humanos fora de linha e em linha (UN Doc. A/HRC/20/L.13). A resolução confirma o significado da universalidade e abertura da *internet*. A resolução refere-se à Declaração Universal dos Direitos Humanos e ao PIDCP.

3. CRONOLOGIA

1966 Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), artº 17º

1980 Diretrizes da OCDE para a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais

1981 Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal

1988 Comentário Geral nº 16 do Comité dos Direitos Humanos das Nações Unidas, sobre o direito ao respeito da privacidade, família, domicílio e correspondência e proteção da honra e reputação (artº 17º)

1989 Convenção da Organização das Nações Unidas sobre os Direitos da Criança

1996 Diretiva da UE sobre a proteção de dados 95/46/EC

2001 Regulamento da UE sobre a proteção de dados 45/2001/EC

2002 Protocolo Facultativo à Convenção sobre os Direitos da Criança relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil

2002 Diretiva da UE relativa às comunicações eletrónicas 2002/58/EC

2003-2005 Cimeira Mundial sobre a sociedade da informação

2004 Protocolo Adicional à Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, respeitante às Autoridades de Controlo e aos Fluxos Transfronteiriços de Dados

ATIVIDADES SELECIONADAS

ATIVIDADE I: DADOS PRIVADOS E DADOS PÚBLICOS

Parte I: Introdução

Esta atividade pretende auxiliar na compreensão da necessidade da proteção da privacidade na *internet*.

Parte II: Informação Geral

Tipo de atividade: Trabalho de grupo
Metas e objetivos: Distinção entre dados públicos e privados; reflexão sobre o uso e a partilha de dados privados em redes sociais, etc.
Grupo-alvo: Adolescentes e adultos jovens
Dimensão do grupo: 6 +
Duração: 30-60 minutos
Material: cópias das fichas de trabalho
Competências envolvidas: Reflexão e competências de análise

Parte III: Informações Específicas sobre a Atividade

Instruções:

1. Explicar aos participantes o significado de dados pessoais/privados. A seguir, os participantes, em pequenos grupos de 2 ou 3 pessoas, preenchem então uma ficha de trabalho. Devem debater juntos e apontar quais os dados que devem ser integralmente privados e quais os dados que podem ser partilhados. Deve incentivar-se a apresentação de diferentes argumentos.
2. Cada grupo apresenta os seus resultados aos outros e o moderador constitui uma lista comum. Em caso de desacordo, devem debater-se, no âmbito do grupo, as diferentes perspetivas. No final, deve refletir-se sobre os resultados da lista comum.

Ficha de trabalho:

1. Ler esta lista com atenção:
   A minha idade, o meu endereço, as horas em que não estou em casa, o meu tamanho de sapato, a minha escola/local de trabalho, as minhas informações médicas (alergias, doenças, etc.), o meu número de telefone, as minhas atividades extracurriculares, o meu peso, os meus cosméticos favoritos, o meu prato favorito, a minha série de televisão favorita, o nome do meu melhor amigo, a cor da minha roupa interior, o meu músico favorito, o meu namorado/namorada/cônjuge/noivo, a minha religião, uma imagem minha na banheira, o meu endereço eletrónico, uma imagem minha a mostrar a face, o salário que aufiro/dinheiro de bolso, o nome do meu animal de estimação, a minha alcunha, o meu aniversário.
2. Preencher a tabela com os dados referidos no ponto 1.

Absolutamente privado	Apenas para amigos	Não é claro	Sempre público

Acompanhamento:
Debater a separação dos dados privados e dos dados públicos e por que é tão importante distingui-los. Como podem proteger-se as informações pessoais na *internet*?
Direitos relacionados: Liberdade de expressão e liberdade dos meios de informação e todos os outros direitos humanos.

ATIVIDADE II:
A HISTÓRIA DE MARIANNE K.

Parte I: Introdução
Nós crescemos acostumados à vigilância das câmaras no espaço público; nós já não reparamos na vigilância das câmaras. Mas quais as repercussões para o nosso direito à privacidade, se cada passo puder ser acompanhado pela polícia, pelos funcionários de segurança e mesmo por privados?

Parte II: Informação Geral
Tipo de atividade: Exercício e discussão de grupo
Metas e objetivos: Sensibilizar os participantes para possíveis ameaças ao direito à privacidade; discutir os prós e contras da vigilância das câmaras no espaço público.
Grupo-alvo: Adolescentes e adultos
Dimensão do grupo: 10 +
***Duração*:** 30-60 minutos
Materiais: Uma cópia da história da Marianne; uma imagem da aldeia K. (copiada ou desenhada), uma fotografia das câmaras de vigilância; cartões com duas cores diferentes para o exercício de acompanhamento.
Competências envolvidas: Reflexão e competências analíticas, argumentação

Parte III: Informações Específicas sobre a Atividade
Instruções:
Desenhar a aldeia K. num quadro ou copiar a imagem de baixo e dispô-la na sala de aula de forma a que os participantes a vejam enquanto se lê a seguinte história em voz alta:

Marianne K. deixa o café, na praça principal da aldeia, na companhia de um homem. Limpa algumas lágrimas da sua face. Abraça então o homem que sussurra algo ao seu ouvido. O homem vai-se embora. Quando ele se vira para trás, Marianne acena-lhe com o braço para dizer-lhe adeus. Ela então entra na farmácia. Ao sair de novo, coloca, cuidadosamente, diversas caixas de medicamentos na sua mala de mão. Marianne dirige-se, depois, para o edifício com a placa "Advogado" junto à porta de entrada. Quando sai, de novo, após algum tempo, leva consigo uma pasta e dirige-se à igreja da aldeia. Passa de novo algum tempo até que ela regressa do gabinete do pároco e se dirige ao cemitério. Por fim, vai ao supermercado junto ao café e regressa, de novo, com duas garrafas de vinho tinto e duas garrafas de vinho branco.
Dar aos participantes alguns minutos para refletirem sobre os passos da Marianne. Pedir-lhes que especulem sobre o passado e motivos das suas atividades. Numa sessão a envolver todo o grupo colocá-los a trocar ideias e anotar as assunções no quadro ou cavalete.

Para terminar, ler alto a história integral:
A *Marianne K. vive na aldeia K., juntamente com o seu marido, Martin, e os seus filhos Mary e Marcus. Ela viveu em K. a maior parte da sua vida, realizou os seus estudos secundários em K. e tem alguns familiares a viverem, também, nesta aldeia. O marido de Marianne, Martin, cresceu na cidade de L.. Ele trabalha como gestor para uma empresa internacional e, como consequência, transita diariamente entre K. e a cidade de I.. Recentemente, ele teve de assumir mais e mais deslocações de negócios ao estrangeiro e também dá seminários nos fins de semanas, para empregados e formandos da empresa onde trabalha. Assim, ele não despende de muito tempo com a sua mulher e crianças e Marianne não se encontra muito feliz com a situação. Mais, ela encontra-se à procura de um trabalho, já há bastante tempo, após ter estado em licença de maternidade por alguns anos e a cuidar da sua mãe, após o falecimento do seu pai, há pouco tempo atrás. Marianne é assistente social e não é fácil encontrar trabalho em K. ou nas aldeias vizinhas.*
Após ter recebido mais cartas de recusa, Marianne encontrou o seu colega de escola e amigo próximo no café da aldeia. Eles falaram dos seus problemas e Marianne ficou emocionada. Quando o seu colega de escola teve de se ir embora, eles deixaram o café juntos e Marianne limpou as lágrimas da sua face. Ao despedirem-se abraçaram-se, tendo ele tentado confortar Marianne ao dizer-lhe que tudo irá correr bem no final. Assim que ele a deixou, Marianne ficou a observá-lo e acenou-lhe quando ele se virou.
Ela foi então à farmácia para levantar uma receita para a sua mãe. Ao sair, arrumou as caixas dos medicamentos na sua mala de mão e dirigiu-se ao escritório do advogado para uma consulta sobre uma herança de Martin. Ao sair do escritório do advogado, levou consigo uma pasta com informações jurídicas para Martin. Foi à igreja da aldeia para inscrever a sua filha Mary nas aulas da primeira comunhão. Quando saiu do gabinete do pároco, dirigiu-se ao cemitério para tratar da campa do pai. Por fim, foi ao supermercado junto ao café para comprar algumas garrafas de vinho tinto e branco para um jantar com amigos.
Afixar uma fotografia de câmaras de vigilância junto ao desenho da praça central da aldeia, antes de ler a última frase:
Passou muito tempo antes da Marianne ter notado, pela última vez, as câmaras de vigilância no meio da praça central…
Apresentar aos participantes as assunções que fizeram ao interpretar o comportamento da Marianne. Os aldeães de K. conhecem a sua situação demasiado bem… O que pensaria, por exemplo, um agente da polícia em frente ao monitor? Será que as interpretações e assunções sobre a conduta de Marianne terão consequências para ela? Se sim, que consequências?

Acompanhamento:
Poder-se-á prosseguir com um grupo de trabalho para recolher e debater os prós e contras das câmaras de vigilância no espaço público. Pedir aos participantes para se dividirem em grupos de três a cinco pessoas e dar a cada grupo um par de cartões de cores diferentes (por exemplo, o verde para os prós e o vermelho para os contras). Dar 15 minutos para encontrarem argumentos a favor ou contra as câmaras de vigilância e para concordarem sobre os pontos nos grupos pequenos.
Chamar então os participantes de volta ao grupo e pedir-lhes que afixem os cartões no quadro ou parede e que discutam os ar-

gumentos. Se necessário, poder-se-á complementar as conclusões dos participantes com os seguintes argumentos:

- PRÓS: a eliminação de zonas quentes de pequena criminalidade, a resolução mais fácil dos crimes, a prevenção para possíveis agentes do crime, a deteção e a luta contra ameaças à segurança pública, a contribuição para uma maior eficácia no trabalho da polícia, o fortalecimento do sentimento de segurança das pessoas, a melhoria da reconstrução dos eventos, a identificação de agentes criminosos, etc.
- CONTRAS: a erosão gradual da presunção de inocência, a dessensibilização sistemática da sociedade, a manutenção de uma sociedade homogénea – perda da diversidade através do efeito do observador -, a erosão gradual do primado do Direito, a proximidade a um Estado de vigilância, o fortalecimento do sentimento de insegurança das pessoas, os custos elevados, a monitorização e a supervisão insuficientes, etc.

Direitos relacionados: a liberdade de expressão e a liberdade dos meios de informação, o primado do Direito e o julgamento justo.

(Fonte: Translated and adapted from: Stephanie Deutinger, Lina Dornhofer. 2012. *!?!... is watching you. Menschenrechte und Überwachung*.)

REFERÊNCIAS BIBLIOGRÁFICAS

31st International Conference of Data Protection and Privacy Commissioners. 2009. *Standards on Privacy and Personal Data.* Available at: www.privacyconference2009.org/dpas_space/Resolucion/index-iden-idphp.php

BBC. 2011. *France fines Google over Street View data blunder.* Available at: www.bbc.co.uk/news/technology-12809076

BBC. 2008. *Facebook 'violates privacy laws'.* Available at: http://news.bbc.co.uk/2/hi/7428833.stm

CBCNews. 2010. *Montreal man on watch* list rallies supporters. Available at: www.cbc.ca /montreal-abdelrazik-march.html

Council of Europe. 2012. *Recommendation on the protection of human rights with regard to search engines, Recommendation CM/Rec(2012)3.* Available at: https://wcd.coe.int/ViewDoc.jsp?Ref = CM/Rec(2012)3&Language = lanEnglish&Ver = original&BackColorInternet = C3C3C3&BackColorIntranet = EDB021&BackColorLogged = F5D383

Deutinger, Stephanie and Lina Dornhofer. 2012. *!?!... is watching you. Menschenrechte und Überwachung***.** Available at: www.etc-graz.at/typo3/index.php?id = 1064

European C**ommission. 2012**. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data* and on the free movement of such data (General Data *Protection Regulation), COM(2012) 11 final.* Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Irish Data Protection C**ommissioner. 2011.** *Facebook Ireland Ltd – Report of*

Audit. Available at: http://europe-v-facebook.org/Facebook_Ireland_Audit_Report_Final.pdf

Irish Data Protection Comissioner. 2009. *Case Study 1: Disclosure of personal data due to inappropriate security measures.* Available at: www.dataprotection.ie/viewdoc.asp?DocID = 1068#1

Kettemann, Matthias C. 2012. *5 punchy principles for regulating the internet.* Available at: http://internationallawandtheinternet.blogspot.co.at/2012/07/5-punchy-principles-for-regulating.html?spref = fb

Malanczuk, Peter. 2009. *Data, Transboundary Flow, International Protection.* In: Max Planck Encyclopaedia of Public International Law. Available at: www.mpepil.com/subscriber_article?script = yes&id = /epil/entries/law-9780199231690-e771&recno = 125&searchType = Advanced&subject = Human + rights

Nowak, Manfred. 2005. *CCPR Commentary*, Art. 17 CCPR. Kehl: N.P. Engel Verlag.

OAS. 2012. *Press release - Freedom of expression rapporteurs issue joint declaration concerning the internet.* Available at: www.oas.org/en/iachr/expression/showarticle.asp?artID = 848&lID = 1

Sepulveda, Magdalena, Theo van Banning, Gudrun D. Gudmundsdottir, Christine Chamoun and Willem J.M. van Genugten. 2009. *Human Rights References Handbook*. Ciudad Colon: University for Peace.

United Nations Human Rights Committee. 1988. *General Comment No. 16: The right to respect privacy, family, home and correspondence, and protection of honour and reputation (Art. 17)*. Available at: www.unhchr.ch/tbs/doc.nsf/0/23378a8724595410c12563ed004aeecd?Opendocument

United Nations Office of the High Commissioner for Human Rights (OHCHR). 2007. *Human Rights, Terrorism and Counter-terrorism.* Available at: www.ohchr.org/Documents/Publications/Factsheet32EN.pdf

United Nations. 2009. *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Martin Scheinin, No. A/HRC/13/37/2009

Van Lieshout, Tessa. 2006. *The United Nations and the fight against terrorism.* Nijmegen: Wolf Legal Publishers.

INFORMAÇÃO ADICIONAL

Council of Europe: www.coe.int

Electronic Privacy Information Centre (EPIC): http://epic.org

Electronic Privacy Information Centre (EPIC), Investigations of Google Street View: http://epic.org/privacy/streetview/

Electronic Privacy Information Centre (EPIC), Social Networking Privacy: http://epic.org/privacy/socialnet/default.html

European Court of Human Rights: http://echr.coe.int/echr/

Max Planck Encyclopaedia of Public International Law: www.mpepil.com

OECD: www.oecd.org/

Privacy International (PI): www.privacyinternational.org

Privacy.Org: http://privacy.org/

UN Committee on the Rights of the Child: www.ohchr.org/english/bodies/crc

UN Human Rights Committee: www2.ohchr.org/english/bodies/hrc/index.htm

UN Security Council Committee established pursuant to resolution 1267 (1999) concerning Al-Qaida and the Taliban and Associated Individuals and Entities: www.un.org/sc/committees/1267

UN Security Council Counter Terrorism Committee: www.un.org/en/sc/ctc/rights.html

US Courts Statistics 2011: www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/Table6.pdf