

**Memorando sobre a proteção
de dados pessoais e da privacidade nas redes sociais da Internet,
principalmente em relação às crianças e adolescentes**

Memorando de Montevideo

CONSIDERAÇÕES GERAIS

A Sociedade da Informação e do Conhecimento, com ferramentas como a Internet e as redes sociais digitais, é uma oportunidade inestimável para o acesso e intercâmbio de informação, propagação de ideias, participação cidadã, diversão e integração social, especialmente através das redes sociais.

As crianças e adolescentes têm cada vez maior acesso aos diferentes sistemas de comunicação, permitindo-lhes obter todos os benefícios que estes sistemas oferecem. Entretanto, esta situação também levou a que o equilíbrio entre o exercício dos direitos fundamentais e os riscos ao usar estes sistemas chegasse ao seu limite—em termos de privacidade, honra, reputação, e intimidade, entre outros— da mesma forma como no caso de virem a ser vítimas de abusos —como por exemplo: discriminação, exploração sexual, pornografia— fazendo com que possa haver um impacto negativo para o seu desenvolvimento integral e vida adulta.

Na América Latina e o Caribe, bem como em outras regiões, estão sendo feitos esforços, dentro da diversidade social, cultural, política e normativa existente, para obter consenso e racionalidade visando estabelecer um equilíbrio entre a garantia dos direitos e a proteção diante dos riscos na Sociedade da Informação e do Conhecimento. Nesse sentido, podemos citar, entre outros, os mais recentes documentos: o *Acordo que põe fim à disputa judicial entre o Ministério Público Federal do Brasil e o Google*¹(de 1 de julho de 2008); o *programa Proteção para Crianças online (CPO)*² da União Internacional de Telecomunicações (de 18 de maio de 2009); a *Opinião 5/2009 sobre as redes sociais na Internet*³, do Grupo Europeu de Trabalho do Artigo 29º (de 12 de Junho de 2009); o *Relatório de conclusões da investigação feita a partir de uma denúncia apresentada pela Clínica Canadense de Políticas Públicas para Internet e Interesse Público (CIPPIC) contra Facebook Inc.*⁴ (de 16 de Julho de 2009).⁵

1. http://www.prsp.mpf.gov.br/sala-de-imprensa/noticias_prsp/noticia-7584/

2. <http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html>

3. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf

4. http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.cfm / http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm

5. Outros documentos especialmente considerados: *Resolução de Estrasburgo sobre Proteção da Privacidade nos Serviços de Redes Sociais*(17 de outubro de 2008); “Recomendação sobre redes sociais” da Agência Espanhola de Proteção de Dados, “Estudo sobre a privacidade dos dados pessoais, privacidade e segurança da informação nas Redes Sociais online” , realizado pelo Instituto Nacional de Tecnologias da Comunicação, INTECO e pela Agência Espanhola de Proteção de Dados (2009), "Declaração e Plano de Ação do Rio de Janeiro para Prevenir e Eliminar a Exploração Sexual de Crianças e Adolescentes" (novembro 2008), o Parecer 2/2009 sobre a proteção dos dados pessoais das crianças do Grupo Europeu de Trabalho do Artigo 29º (2009); o Relatório de Análises e Propostas em

As recomendações apresentadas a seguir são uma contribuição para que os diversos atores envolvidos da região se comprometam com essa questão, visando não só ampliar os aspectos positivos da Sociedade da Informação e do Conhecimento, incluindo a Internet e as redes sociais digitais, como também para prevenir aquelas práticas prejudiciais que serão muito difíceis de reverter, incluindo os impactos negativos das mesmas.

Qualquer abordagem sobre o tema requer a consideração de duas dimensões: Por um lado, o reconhecimento de que as crianças e adolescentes são titulares de todos os direitos, e portanto podem exercê-los em função de sua idade e maturidade, sendo suas opiniões consideradas em função da idade e maturidade. Por outro lado, considerar o fato de que por sua particular condição de desenvolvimento, elas têm o direito a uma proteção especial naquelas situações que possam ser prejudiciais para o seu desenvolvimento e os seus direitos.

O direito à privacidade é um valor que toda sociedade democrática deve respeitar. Portanto, para garantir a autonomia dos indivíduos e decidir o âmbito da vida privada, o poder tanto do Estado como da organizações particulares deve ser limitado, visando impedir que cometam intromissões ilegais ou arbitrárias, na esfera pessoal. Em especial, a informação pessoal de crianças e adolescentes deve ser protegida, sem que a sua dignidade seja afetada, já que eles têm uma expectativa razoável de privacidade ao compartilhar sua informação em ambientes digitais, uma vez que consideram estarem em uma área privada.

Neste sentido, é importante recordar a importância de as crianças e adolescentes serem consultados e suas opiniões consideradas em todas as medidas que forem implementadas nesta área.

A sociedade civil espera dos agentes econômicos a declaração de adesão a princípios, atitudes e procedimentos que garantam os direitos das crianças e adolescentes na Sociedade da Informação e do Conhecimento.

Em termos da erradicação da pornografia infantil na Internet, espera-se um esforço conjunto de todos os atores responsáveis —governos, polícia, provedores de acesso e de conteúdo, sociedade civil, setor privado— nacional, regional e internacionalmente para mobilizar e envolver a um número cada vez maior de empresas, organizações públicas e sociedade civil.

Para estas recomendações, foram consideradas as particularidades de gênero e a diversidade cultural existente na América Latina, bem como um leque de políticas e de normativas sobre a forma de enfrentar o fenômeno da

Sociedade da Informação e do Conhecimento, com especial ênfase na Internet e nas suas redes sociais.

Os organismos multilaterais deverão incluir, em seus documentos, diretrizes ou recomendações para as crianças e adolescentes, como sujeitos particularmente vulneráveis e que portanto devem ser especialmente protegidos com respeito ao tratamento de seus dados pessoais. Os organismos devem também concentrar esforços para promover ou fortalecer nas crianças e adolescentes uma cultura de proteção de dados.

Estas recomendações utilizam como referente normativo fundamental a Convenção das Nações Unidas sobre os Direitos da Criança (CDC), instrumento ratificado por todos os países da região, reconhecendo claramente a responsabilidade da sociedade e do Estado, compartilhada dentro dos seus respectivos âmbitos, visando a proteção da infância e da adolescência. As recomendações partem de três considerações fundamentais: o reconhecimento do relevante papel que a família ocupa, ou de quem for responsável pelo cuidado das crianças e adolescentes no processo de educação sobre o uso responsável e seguro de ferramentas como a Internet e as redes sociais digitais, bem como na proteção e garantia de seus direitos; a necessidade de que todas as medidas que forem tomadas priorizem o melhor interesse da criança e do adolescente; guardando um equilíbrio entre as necessidades de proteção contra a vulneração de seus direitos e o uso responsável dessas ferramentas que representam formas de exercício dos seus direitos; e, que todo aquele que de qualquer forma se beneficie através da Internet e das redes sociais digitais seja responsável pelos serviços que fornecer e portanto deverá assumir a responsabilidade nas soluções para a problemática que for gerada.

RECOMENDAÇÕES PARA OS ESTADOS E INSTITUIÇÕES EDUCATIVAS PARA A PREVENÇÃO E EDUCAÇÃO DE CRIANÇAS E ADOLESCENTES

Toda ação em matéria de proteção dos dados pessoais e da vida privada das crianças e adolescentes⁶ deve considerar o princípio do melhor interesse da criança⁷ e o artigo 16 da CDC que determina que: "(1). *Nenhuma criança será objeto de interferências arbitrárias ou ilegais em sua vida particular, sua família, seu domicílio, ou sua correspondência, nem de atentados ilegais a sua honra e a sua reputação*". (2). *A criança tem direito à proteção da lei contra essas interferência ou atentados*".

6. As expressões criança e adolescente são usadas com o sentido dado pela legislação nacional de cada país (conforme o país, a expressão criança poderá se referir a pessoas que não fizeram 12 ou 13 anos de idade, e adolescente a quem tiver mais de 12 ou 13 anos e menores de 18 anos. Nos países onde não foi introduzido juridicamente a categoria "adolescentes", passam a ser considerados os chamados "menores adultos" ou "menores púberes". No caso de Honduras, o menino para ser criança deve ser menor de 14 anos e a menina menor de 12 anos. Os adolescentes são maiores de 14 e as adolescentes maiores de 12 anos respectivamente e ambos menores de 18 anos).

7. Artigo 3.1 da CDC "Em todas as ações relativas às crianças, quer empreendidas por instituições de bem-estar social públicas ou privadas, tribunais, autoridades administrativas ou órgãos legislativos, o melhor interesse da criança será uma consideração principal".

É prioritária a prevenção, —sem negligenciar uma abordagem jurídico-regulamentar— para enfrentar os aspectos identificados como de risco na Sociedade da Informação e do Conhecimento, em especial na Internet e nas redes sociais, principalmente através da educação, considerando a participação ativa das próprias crianças e adolescentes, dos pais ou de quem estiver a cargo do seu cuidado e dos educadores, levando em consideração como princípio fundamental o melhor interesse das crianças e adolescentes.

Para isto, devem ser consideradas as seguintes recomendações:

1. Os Estados e as instituições educativas devem considerar o papel dos pais, ou de quem tiver sob sua responsabilidade o cuidado das crianças e adolescentes, na formação pessoal deles, o que inclui o uso responsável e seguro da Internet e das redes sociais digitais. É tarefa do Estado e das instituições educativas fornecer informação e reforçar as capacidades dos pais e das pessoas responsáveis, com relação aos eventuais riscos que as crianças e adolescentes enfrentam nos ambientes digitais.

2. Qualquer medida que envolva o controle dos meios de comunicação tem que respeitar o princípio de proporcionalidade, portanto deve ser determinado que a mesma vise a proteger e a garantir os direitos que estiverem de acordo ao objetivo perseguido, não existindo outra medida que permita obter os mesmos resultados e seja menos restritiva de direitos.

3. É importante transmitir claramente às crianças e adolescentes que a Internet não é um espaço sem regras, impune ou sem responsabilidades. Devem ser alertados para não se deixarem enganar com a aparente sensação de que ali vale tudo, porque todas as ações têm consequências.

Devem ser educados no uso responsável e seguro da Internet e das redes sociais digitais. Destacando:

3.1. A participação anônima ou usar pseudônimos é possível nas redes sociais digitais. O processo educativo deve refletir sobre os aspectos positivos do uso de pseudônimos como meio de proteção. Um uso responsável —entre outras coisas— implica não utilizar desses recursos para enganar ou confundir as outras pessoas sobre a sua identidade real.

As crianças e adolescentes devem ser advertidos sobre a possibilidade de que quando pensam estar se comunicando ou compartilhando informação com uma pessoa determinada, em realidade pode se tratar de outra pessoa. Ao mesmo tempo é necessário advertir que a participação anônima ou com um pseudônimo permite a suplantação da identidade.

3.2. No processo educativo é necessário enfatizar o respeito à vida privada, à intimidade e à reputação de terceiros pessoas, entre outras questões. É importante que as crianças e adolescentes saibam que aquilo que elas divulguem pode vulnerabilizar os seus direitos e os de terceiros.

3.3. As crianças e adolescentes devem saber que a distribuição de conteúdos proibidos pela lei local e regional (em especial a pornografia infantil), o assédio (em especial o assédio sexual), a discriminação, a promoção do ódio racial, a difamação, a violência, entre outros, são ilegais na Internet e nas redes sociais digitais, sendo puníveis por lei.

3.4. O processo educativo deve dar às crianças e adolescentes o conhecimento do uso responsável e seguro das políticas de privacidade, segurança e alertas com as que contam os instrumentos de acesso dos sites que as crianças e adolescentes são usuários frequentes, como por exemplo as redes sociais digitais.

3.5. É preciso promover uma política educacional —expressa em termos adequados à idade das crianças e adolescentes— que inclua uma estratégia informativa e formativa, visando ajudá-los a gerenciar as potencialidades e os riscos derivados da Sociedade da Informação e do Conhecimento, em especial no uso da Internet e das redes sociais digitais.

3.6. Também é preciso informar sobre os mecanismos de proteção e sobre as responsabilidades civis, penais ou administrativas existentes quando os próprios direitos ou os de terceiros são vulnerados na rede.

3.7. Deve-se advertir do perigo que supõe o denominado roubo e/ou suplantação de identidade, passíveis de ocorrer nos ambientes digitais que induzem ao engano.

3.8. É necessário explicar para as crianças e adolescentes, com uma linguagem de fácil compreensão, o espírito das leis sobre proteção de dados pessoais e sobre proteção da vida privada, de tal modo que possam captar a ideia da importância do respeito à privacidade das informações pessoais de cada um deles e dos demais.

3.9. É necessário educar para a incerteza sobre a veracidade dos conteúdos e a validação das fontes de informação. É preciso ensinar crianças e adolescentes a pesquisar e a discriminar as fontes.

4. Recomenda-se enfaticamente a promoção de uma educação sólida e completa sobre a Sociedade da Informação e do Conhecimento, principalmente focada no uso responsável e seguro da Internet e das redes sociais digitais, por meio de:

4.1. A inclusão nos planos de estudos, em todos os níveis educativos, de informação básica sobre a importância da vida privada e da proteção dos dados pessoais, e demais aspectos indicados no numeral três.

4.2. A produção de material didático, principalmente audiovisuais, páginas web e ferramentas interativas (tais como *jogos online*) onde aparecem as

potencialidades e os riscos. Estes materiais deverão incluir informação sobre os mecanismos de proteção dos direitos.

A natureza destas questões e materiais exige a participação e discussão dos mesmos por parte de todos os atores envolvidos e com isso responder às particularidades locais e culturais.⁸

4.3. Os educadores devem ser capacitados para facilitar a discussão e por em contexto as vantagens e os riscos da Sociedade da Informação e do Conhecimento, e em especial da Internet e das redes sociais digitais; podendo contar para isso com o apoio das autoridades de proteção dos dados pessoais ou de todas aquelas organizações que trabalhem com esta questão em vários países.

4.4. As autoridades educativas —com o apoio das autoridades de proteção de dados (onde existirem), do setor académico, das organizações da sociedade civil, do setor privado e, se necessário, com a cooperação internacional— devem ajudar os educadores e apoiar o trabalho nas áreas descritas.

5. As autoridades competentes devem estabelecer mecanismos para que os centros educativos resolvam os conflitos gerados em consequência do uso da Internet e das redes sociais digitais por parte das crianças e adolescentes, com um sentido didático, sempre considerando o interesse superior dos mesmos, sem vulnerar direitos e garantias, em particular o direito à educação.

RECOMENDAÇÕES PARA OS ESTADOS SOBRE O MARCO LEGAL

O marco legal que regula a Sociedade da Informação e do Conhecimento na região —em particular a Internet e as redes sociais digitais— avança lentamente em comparação com o desenvolvimento de novas aplicações e conteúdos, tendo uma série de vácuos e gerando tensões importantes nos valores que lhe inspira e na forma de proteger os diferentes direitos. No entanto, existe algum nível de consenso, que considera haver suficientes princípios fundamentais e constitucionais para iluminar as decisões que forem tomadas nesta matéria.

É importante fazer a criação, reforma ou harmonização normativa consideradando primordialmente o melhor interesse da crianças e do adolescentes, considerando principalmente:

8. **Orientações da União Internacional de Telecomunicações (ITU) para as decisões políticas.** Itens 3,4: 3. “... É muito importante que a produção de material seja local e que reflita a legislação do lugar, bem como os respectivos padrões culturais, fator essencial em qualquer campanha de segurança dentro da Internet e para qualquer material de capacitação.”; 4. “... Na produção de material educativo é importante levar em consideração que para quem não estiver familiarizado com a tecnologia não será fácil o seu uso. Portanto, é importante garantir que o material relativo à segurança esteja disponível tanto em material impresso como em outros formatos, pensados para fazer com que quem for usá-los possa se sentir mais confortável, como por exemplo, as gravações em vídeo.”

6. Que a proteção dos dados pessoais exige o desenvolvimento de uma normativa nacional, aplicável ao setor público e privado, contendo os direitos e princípios básicos, reconhecidos internacionalmente, bem como os mecanismos para a sua efetiva aplicação. Os Estados deverão considerar principalmente, na criação e no desenvolvimento destas regulamentações, as crianças e adolescentes.

7. A importância de se assegurar que qualquer ação ou omissão contra uma criança ou adolescente, que seja considerada ilegal no mundo real, tenha o mesmo tratamento no mundo virtual, sempre garantindo o bem-estar e a proteção integral dos seus direitos.⁹

8. Os Estados devem legislar o direito que as crianças e os adolescentes têm, seja diretamente ou por meio de seus representantes legais, de solicitar o acesso à informação que for sobre elas mesmas e que estiver nas bases de dados tanto públicas como privadas, bem como a retificação ou o cancelamento de tal informação sempre que for necessário, assim como o direito a se opor ao uso destas informações para qualquer fim.

9. É importante desenvolver uma adequada regulação do funcionamento dos centros de acesso à Internet (públicos ou privados), podendo incluir, por exemplo, a obrigação de se utilizar mensagens de advertência, filtros de conteúdo, acessibilidade para as crianças e adolescentes, etc.

RECOMENDAÇÕES PARA A APLICAÇÃO DAS LEIS POR PARTE DOS ESTADOS

Nos últimos anos, chegaram aos Tribunais de Justiça muitos conflitos ou violações de direitos como consequência da difusão de dados pessoais, invasão da vida privada, difamações pela Internet e pelas redes sociais digitais. Algumas decisões tem mostrado que o papel dos juízes para decidir situações novas está em conformidade com os princípios fundamentais. No entanto, a proporção de conflitos que têm um real acesso à justiça é mínima.

Os sistemas judiciais têm um papel muito importante para assegurar de um bom uso da Internet e das redes sociais digitais. As sanções civis e penais devem ser aplicadas não só para retificar os direitos vulnerados, mas

9. **Orientações da União Internacional de Telecomunicações (ITU) para as decisões políticas.** Item 2: “Estabelecer, *mutatis mutandis*, que todo ato contra uma criança, que for ilícito no mundo real, também seja ilegal no mundo virtual, sendo válida para o mundo virtual a normativa relativa à proteção e privacidade dos dados pessoais de quem for considerado menor de idade.”

também para dar aos cidadãos e às empresas regras claras sobre a interpretação das leis e dos princípios fundamentais.¹⁰

10. Deve-se garantir:

10.1. Que existam processos judiciais e administrativos simples, rápidos, de fácil acesso e que sejam tramitados com prioridade pelos tribunais e autoridades responsáveis.¹¹

É preciso fortalecer o uso da responsabilidade civil extracontratual objetiva como mecanismo regulatório para garantir os direitos fundamentais nas aplicações na Sociedade da Informação e do Conhecimento, na Internet e nas redes sociais digitais. As sanções judiciais pelos danos causados têm a vantagem de ser uma resposta imediata, eficiente e capaz de desencorajar os projetos perigosos. Este tipo de responsabilidade civil se fundamenta no melhor interesse da criança.

10.2. As decisões tomadas nesta área deveriam ter a mais ampla difusão possível, utilizando técnicas de anonimização que garantam a proteção de dados pessoais.

10.3. Devia ser feita e difundida uma base de dados sobre casos e decisões (resoluções judiciais ou resoluções administrativas anonimizadas) vinculada à Sociedade da Informação e do Conhecimento, em especial a Internet e as redes sociais digitais. Esta base de dados seria um instrumento para que os juízes possam considerar o contexto nacional e internacional no qual estão decidindo.

11. É preciso estabelecer um canal de comunicação que permita às crianças e adolescentes apresentarem as denúncias que possam surgir devido à vulneração de seus direitos, em matéria de proteção de dados pessoais.

12. Promover o estabelecimento de organismos jurisdicionais especializados na área de proteção de dados.

13. Desenvolver capacidades nos atores jurídicos envolvidos em matéria de proteção de dados, com especial ênfase na proteção de crianças e adolescentes.

10. [Declaração de Princípios sobre Liberdade de Expressão, da Comissão Interamericana de Direitos Humanos da O.E.A. \(Outubro de 2000\)](#): “10. As leis de privacidade não devem inibir ou restringir a investigação ou difusão de informações que sejam do interesse público. A proteção à reputação deve ser garantida por meio de sanções civis nos casos em que a pessoa ofendida for um funcionário ou indivíduo público ou estiver envolvida, de alguma forma, em um assunto de interesse público. Caso contrário, deve provar-se que o comunicador demonstrou negligência na sua conduta em obter as informações, fossem elas falsas ou verdadeiras, que tinha a intenção de causar danos à pessoa e conhecimento de que estava difundindo notícias falsas.” [Aprovada durante o 108º Período Ordinário de Sessões da CIDH]

11. Neste sentido, destaca-se a intervenção dos Juizados Especiais do Brasil na proteção dos direitos dos cidadãos nas redes sociais na Internet.

RECOMENDAÇÕES EM MATÉRIA DE POLÍTICAS PÚBLICAS

Lembramos a necessidade de que o interesse superior da criança seja considerado como princípio reitor para qualquer ação nesta área, particularmente no desenvolvimento de políticas públicas inclinadas a regular as redes sociais digitais.¹²

14. É recomendado considerar a implementação das seguintes políticas públicas:

14.1 Criação de mecanismos de resposta para o atendimento das vítimas de abusos na Sociedade da Informação e do Conhecimento, particularmente na Internet ou nas redes sociais digitais. Do mesmo modo, deve-se estabelecer sistemas de informação para que aquelas crianças e adolescentes que se sentirem preocupadas com os conteúdos na Internet ou nas redes sociais digitais possam rapidamente ser assessoradas e receber apoio.

Para isto, dever-se-iam criar medidas tais como a ajuda e denúncia *online*, números telefônicos gratuitos, centros de atendimento, etc.

14.2. Elaboração de protocolos para canalizar os conteúdos ilegais denunciados.¹³

15. Deveriam existir mecanismos regionais e internacionais para compartilhar a informação denunciada por particulares sobre estas ocorrências, em tempo real, para poder assim gerar políticas e mecanismos de proteção, de forma antecipada, devido a que os riscos gerados nas redes sociais digitais estão muito dispersos e não são plenamente advertidos.

16. Promover ações de sensibilização e divulgação de informação através da mídia e das próprias redes sociais, entre outros, porque são um veículo efetivo para promover um uso responsável e seguro das ferramentas da Sociedade da Informação e do Conhecimento.¹⁴

17. Promover o compromisso e a participação das associações públicas e privadas, assim como das redes nacionais de centros de acesso à Internet

12. **Opinião 5:** 4. “A Opinião destaca a necessidade de considerar os Melhores Interesses da Criança, estabelecidos pela Convenção das Nações Unidas sobre os Direitos da Criança. O Grupo de Trabalho também quer destacar a importância deste princípio no contexto de Serviços de Redes Sociais (“SNS”, na sigla em inglês).”

13. **Orientações da União Internacional de Telecomunicações (ITU) para as decisões políticas.** Itens 5, 6 e 7: “5. Considerar a implementação de medidas adicionais destinadas a reduzir ou interromper o tráfego em módulos de acesso condicional (“CAM”, na sigla em Inglês). 6. Assegurar que seja estabelecido um mecanismo -e amplamente divulgado- para fornecer um meio de compreensão imediata, a fim de denunciar os conteúdos ilegais encontrados na Internet, como por exemplo uma linha de emergência nacional capaz de responder rapidamente e com a possibilidade de retirar ou deixar inacessível o material que for ilegal. 7. Assegurar a existência de processos a nível nacional para garantir que qualquer CAM encontrado em um país seja canalizado para um recurso nacional e centralizado. Um exemplo é o *National Center on Child Neglect (NCCAN)*.”

14. **Orientações da União Internacional de Telecomunicações (ITU) para as decisões políticas.** Item 2: “É preciso considerar a ajuda da mídia para divulgar e promover as mensagens e campanhas de conscientização.”

(onde houver), para garantir a participação na proteção e nas campanhas de alerta sobre as potencialidades e os riscos da Internet e das redes sociais digitais.

18. Promover a geração de Conhecimento especializado com o fim de elaborar políticas públicas adequadas. Com relação aos comportamentos *online* de crianças e adolescentes, sugere-se investigar qual o papel que elas desempenham na recepção, produção, armazenamento e reprodução de conteúdos ilegais, bem como averiguar quais as medidas de proteção que elas mesmas desenvolvem, as motivações individuais e as coletivas de tais comportamentos, assim como os perigos reais aos que se enfrentam na Sociedade da Informação e do Conhecimento.

RECOMENDAÇÕES PARA A INDÚSTRIA

As empresas provedoras de serviços de acesso à Internet, desenvolvedoras de aplicativos e de redes sociais digitais devem se comprometer decididamente a proteger os dados pessoais e da vida privada —em particular das crianças e adolescentes—, a cooperar com os sistemas de justiça nacionais, a desenvolver campanhas de prevenção e desenvolvimento de capacidades, entre outros instrumentos mediante compromissos ou códigos de conduta, que devem incluir:

19. Não permitir a recopilação, tratamento, difusão, publicação ou envio a terceiros de dados pessoais, sem o consentimento explícito da pessoa em questão. É necessário restringir o uso da informação recoletada para qualquer outra finalidade que não seja o motivo pelo qual a informação foi fornecida, principalmente na criação de perfis comportamentais.¹⁵

No caso das crianças, é fundamental considerar a proibição relativa ao tratamento de dados pessoais. No caso de adolescentes, é necessário considerar os mecanismos de controle parental de acordo com a legislação de cada país, devendo a informação ser dada de forma clara.

20. Proteger a vida privada deveria ser a característica geral e por default em todas as redes sociais digitais, bases de dados e sistemas de comunicação, entre outros. As mudanças feitas no grau de privacidade do perfil de usuário devem ser simples e sem custo algum.

21. As regras sobre privacidade das páginas web, serviços, aplicativos, entre outros, deveriam ser explícitas, simples e claras, explicadas em uma linguagem adequada para crianças e adolescentes.

Dever-se-á fornecer informação sobre os propósitos e finalidades para os quais os dados pessoais serão utilizados, assim como as transmissões de

15. **Opinion 5:** 3.4. Os dados pessoais só podem ser publicados na Internet com o consentimento explícito do titular dos dados, ou se o próprio titular já os tiver tornado públicos

dados para terceiros. Também devem indicar a pessoa ou pessoas responsáveis pelo tratamento da informação.

Também se deve oferecer um link para os “parâmetros de privacidade” no momento da inscrição, contendo uma explicação clara sobre a finalidade destes parâmetros.

Um aviso sobre o fato de que a rede social pré-selecionou os parâmetros também deve estar facilmente acessível, se for o caso, e um alerta de que podem sofrer mudanças a qualquer momento, de acordo com as preferências das crianças e dos adolescentes.

Seria também desejável que sejam alterados os “parâmetros por default” dos conteúdos pessoais, para que só os amigos e as redes que o usuário determinar possam ter acesso a esses conteúdos.¹⁶

22. Toda rede social digital deve indicar explicitamente na parte relativa à “publicidade” contida em sua política de privacidade, sobre os anúncios publicitários e informar claramente, em especial às crianças e adolescentes, sobre o fato de que as informações pessoais dos perfis dos usuários são usadas para enviar publicidade segundo cada perfil. Deve-se evitar a publicidade que não for adequada para as crianças e adolescentes.¹⁷

23. Qualquer rede social digital deve indicar de maneira clara o motivo para exigir certos dados pessoais e particularmente, a data de nascimento no momento da inscrição e da criação de uma conta. Deve-se portanto explicar que a data de nascimento exigida tem como finalidade verificar a idade mínima permitida para se criar uma conta na rede social digital.

Também é preciso especificar como vão ser utilizados estes dados de caráter pessoal que precisam ser obrigatoriamente fornecidos.¹⁸

A indústria deverá implementar mecanismos para uma verificação fidedigna da idade de crianças e adolescentes para a criação de uma conta de usuário e/ou ter acesso a determinado conteúdo.

24. Toda rede social digital, sistema de comunicação ou base de dados deveria contar com formas de acesso à informação, rectificação e eliminação

16. Diretiva de Privacidade do Canadá, Resumo do Caso “PIPEDA” (Lei de Proteção a Informações Pessoais e Documentos Eletrônicos) #2009-008, Relatório sobre a decisão judicial em relação à denúncia apresentada pela Clínica Canadense sobre Políticas de Internet e Interesse Público (CIPPIC, na sigla em inglês) contra Facebook Inc. Conforme a Lei de Proteção a Informações Pessoais e Documentos Eletrônicos, 16 de julho de 2009.

17. *Id.*

18. *Id.*

de dados pessoais, para usuários ou não-usuários, levando em consideração os fatores limitantes da lei.¹⁹

Toda rede social digital deve elaborar uma política acessível aos usuários em matéria de conservação da informação, em virtude da qual os dados pessoais dos usuários que desativaram sua conta sejam suprimidos totalmente dos servidores do serviço, após um período de tempo razoável. Além disso, é importante eliminar a informação de não-usuários, considerando um limite razoável de conservação quando tiverem sido convidados a ser parte das redes. As redes sociais digitais não devem utilizar a informação de não-usuários.

As duas opções que permitirem desativar e suprimir as contas devem ser totalmente visíveis para os usuários, que devem poder compreender o que cada opção significa para a gestão do serviço dos dados contidos em suas contas.²⁰

É preciso informar aos usuários sobre as obrigações de privacidade com relação a terceiros. Esta política deve ser explícita, clara e visível.

25. Deve ser impedida a indexação dos usuários das redes sociais digitais por parte dos motores de pesquisa, a não ser que o usuário tenha optado por esta função. A indexação de informação de crianças deve estar proibida em todas as suas formas. No caso de adolescentes, estes devem autorizar de forma expressa a indexação de seus dados mínimos.

26. Toda rede social digital deve estabelecer as medidas necessárias para que quem desenvolva os diferentes aplicativos oferecidos pelo serviço (jogos, questionários, anúncios, entre outros) tenha limitado o seu acesso aos dados pessoais dos usuários, quando estes não forem necessários nem pertinentes para o funcionamento dos aplicativos.

A rede social tem que garantir que os terceiros que desenvolvem aplicativos em suas plataformas só possam ter acesso aos dados pessoais dos usuários com o consentimento expresso deles. A rede social digital deve garantir que os desenvolvedores de aplicativos solicitem apenas a informação indispensável, pertinente e não excessiva para o uso do aplicativo em questão.

Também é importante que sejam tomadas as medidas necessárias para impedir qualquer comunicação dos dados pessoais daqueles usuários que não tiverem eles próprios decidido expressamente instalar alguma aplicação.

19. O espírito deste último parágrafo é não excluir —pelo tempo que for preciso— a retenção dos dados dos usuários que possam ser necessários na investigação de delitos.

20. Diretiva de Privacidade do Canadá, Resumo do Caso “PIPEDA” (Lei de Proteção a Informações Pessoais e Documentos Eletrônicos) #2009-008, Relatório sobre a decisão judicial em relação à denúncia apresentada pela Clínica Canadense sobre Políticas de Internet e Interesse Público (CIPPIC, na sigla em inglês) contra Facebook Inc. Conforme a Lei de Proteção a Informações Pessoais e Documentos Eletrônicos, 16 de julho de 2009.

27. Estas recomendações se aplicam ao tratamento dos dados pessoais nas redes sociais digitais, mesmo que sua residência legal esteja fora da América Latina e o Caribe. Para facilitar o acesso dos usuários à justiça, cada provedor de redes sociais digitais deve fixar um domicílio ou representante legal nos países onde esta rede social tiver um uso significativo ou de acordo aos requerimentos do Estado.

As redes sociais digitais deverão estabelecer um serviço eficiente e eficaz de suporte aos usuários nestas questões. Este suporte deverá estar nas línguas oficiais utilizadas no país do usuário.²¹

28. Os desenvolvedores de web sites, serviços, aplicativos e plataformas, entre outros, deverão estabelecer filtros de segurança, como meio complementar à educação, sensibilização e sanção.²²

29 A indústria deve estabelecer medidas de índole técnica e operativa para garantir a segurança da informação, em particular a integridade, disponibilidade e confidencialidade.

30. Para a erradicação da pornografia infantil na Internet, a indústria —em um esforço conjunto de todos os atores responsáveis— deve se comprometer no mínimo a:

30.1. Notificar às autoridades competentes todas as ocorrências de pornografia infantil detectadas em perfis de usuários de redes sociais digitais, para que seja possível abrir investigações e ações conforme o caso;

30.2. Preservar todos os dados necessários para a investigação por um prazo mínimo de seis meses ou entregar esses dados para as autoridades competentes, mediante autorização judicial;

30.3. Preservar os conteúdos publicados pelos usuários das redes sociais pelo mesmo prazo, e entregar esses conteúdos para as autoridades públicas, mediante autorização judicial;

30.4. Cumprir integralmente as legislações nacionais relativas a crimes cibernéticos praticados pelos cidadãos dos respectivos países da América Latina e o Caribe, ou feitos através da Internet desde as suas respectivas jurisdições nacionais;

21. Diretiva de Privacidade do Canadá, Resumo do Caso “PIPEDA” (Lei de Proteção a Informações Pessoais e Documentos Eletrônicos) #2009-008, Relatório sobre a decisão judicial em relação à denúncia apresentada pela Clínica Canadense sobre Políticas de Internet e Interesse Público (CIPPIC, na sigla em inglês) contra Facebook Inc. Conforme a Lei de Proteção a Informações Pessoais e Documentos Eletrônicos, 16 de julho de 2009.

22. **Orientações da União Internacional de Telecomunicações (ITU) para as decisões políticas.** Item 13: “Considerar o papel que as ferramentas técnicas como os programas de filtragem e os software de proteção para menores podem desempenhar como apoio e complemento educativo nas iniciativas de educação e conscientização”

30.5. Reformular o serviço de atendimento aos clientes e usuários para dar uma resposta em um tempo razoável a todas as reclamações formuladas por e-mail ou por correio pelas pessoas prejudicadas com a criação de comunidades falsas ou ofensivas;

30.6. Desenvolver uma tecnologia eficiente de filtragem e implementação de moderação humana, para impedir a publicação de fotografias e imagens de pornografia infantil no serviço das redes sociais digitais;

30.7. Desenvolver ferramentas por meio das quais as linhas telefônicas de ajuda a crianças e adolescentes possam encaminhar as denúncias para que os funcionários da empresa analisem, retirem os conteúdos ilegais e informem às autoridades competentes quando houver indícios de pornografia infantil, racismo ou outros crimes de ódio, bem como preservar todas as provas;

30.8. Retirar os conteúdos ilícitos, através de ordem judicial ou por requerimento de autoridade pública competente, preservando os dados necessários para a identificação dos autores desses conteúdos;

30.9. Desenvolver ferramentas de comunicação com as autoridades competentes, para facilitar a tramitação das denúncias, formulação de pedidos de remoção e/ou preservação de dados;

30.10. Informar adequadamente os usuários nacionais sobre os principais delitos cometidos nas redes sociais digitais (pornografia infantil, crimes de ódio, delitos contra a honra, entre outros);

30.11. Desenvolver campanhas de educação para o uso seguro e respeitoso das leis, da Internet e das redes sociais digitais;

30.12. Financiar a publicação de folhetos e a sua distribuição para crianças e adolescentes em escolas públicas, com informação para o uso seguro da Internet e das redes sociais;

30.13. É importante haver nos sites das redes sociais digitais os links de *Sites Úteis*, como por exemplo os de denúncia ou os telefones de ajuda para crianças e adolescentes.

CONSIDERAÇÕES FINAIS

31. As recomendações indicadas para as crianças e adolescentes se extendem às outras pessoas (maiores de idade) que devido à sua condição pessoal estiverem em uma posição de vulnerabilidade.

Grupos vulneráveis são todos aqueles relacionados aos dados sensíveis (conforme cada uma das legislações nacionais) que geralmente incluem

trabalhadores, dissidentes, pessoas com capacidades diferentes e suas famílias, imigrantes e emigrantes, entre outros.

32. Todos os atores envolvidos estão convidados a discutir e a interpretar estas recomendações. Do mesmo modo, é preciso buscar um diálogo constante sobre a questão abordada no presente documento. De maneira especial, apela-se ao cumprimento das obrigações dos Estados e à responsabilidade social empresarial para então encontrar as melhores formas de implementar este documento.

Montevideo, 28 de julho de 2009

Recomendações adotadas no *Seminário Direitos, Adolescentes e Redes Sociais na Internet* (com a participação de Belén Albornoz, Carlos G. Gregorio, Chantal Bernier, Erick Iriarte, Esther Mitjans, Farith Simon, Federico Monteverde, Florencia Barindeli, José Clastornik, Leila Regina Paiva de Souza, Lina Ornelas, María José Viega Miguel Cillero, Nelson Remolina, Ricardo Pérez Manrique, Rosario Duaso e Thiago Tavares Nunes de Oliveira) realizado em Montevideo nos dias 27 e 28 de julho de 2009.