Regulamentação do Marco Civil da Internet

Considerações para o eixo "Privacidade e Liberdade de Expressão"

Actantes
Antivigilância.org
ARTIGO 19
Centro de Estudos da Mídia Alternativa Barão de Itararé
Ciranda Internacional da Comunicação Compartilhada
Clube de Engenharia
Coletivo Digital
HackAgenda
IBIDEM - Instituto Beta para Internet e Democracia
Idec - Instituto Brasileiro de Defesa do Consumidor
IGDD - Instituto Goiano de Direito Digital
Instituto Bem Estar Brasil
Instituto Telecom
Intervozes - Coletivo Brasil de Comunicação Social
Movimento Mega
Proteste - Associação de Consumidores

Projeto Gráfico: Ricardo Kuraoka

Introdução

O Marco Civil da Internet tem sido considerado a Constituição da Internet no Brasil, pois estabelece princípios, garantias, direitos e deveres para o uso da Internet no país. Aprovado na forma da Lei n 12.965 em 23 de abril de 2014, está em vigor desde 24 de junho de 2014. Entretanto, ainda que seus princípios e garantias já estejam claramente estabelecidos e protegidos como direitos e deveres, algumas partes importantes do texto que dizem respeito a procedimentos ainda carecem de regulamentação específica, nos termos do art. 84, inc. IV, da Constituição Federal.

Todo o processo de formulação do Marco Civil foi marcado por amplo debate feito por meio de consultas públicas presenciais e online. Tal processo obteve reconhecimento internacional por seu caráter inovador e foi crucial para que o conteúdo da lei afirmasse importantes direitos para toda a população brasileira no uso da rede mundial de computadores, além de estabelecer regras claras e adequadas para que as empresas que prestam serviços na Internet possam seguir operando com segurança jurídica.

Consideramos que um processo semelhante de consultas abertas e democráticas deve ser implementado também no momento de sua regulação, desta forma, damos boas-vindas a iniciativas neste sentido e apresentamos abaixo nossas considerações referentes à regulamentação dos dispositivos que tratam de privacidade.

Considerações para o eixo privacidade

A discussão da agenda de privacidade é essencial para a proteção intransigente da democracia e dos direitos humanos fundamentais, como a liberdade de expressão e já era tema coadjuvante dos debates do Marco Civil. Diante da conjectura pós-Snowden, a parte do texto que mais sofreu modificações desde que chegou no Congresso Nacional foi justamente a que diz respeito à proteção à privacidade. A partir das revelações sobre práticas de vigilância em massa, o Marco Civil entrou em regime de urgência, teve os dispositivos sobre privacidade incrementados, passou-se a discutir uma possível inclusão de cláusula sobre nacionalização de bancos de dados, que ao final foi descartada e, o resultado final foi que na parte geral da lei vários elementos de proteção à privacidade aparecem como princípios e direitos protegidos pelo Marco Civil:A "proteção à privacidade" e "a proteção de dados pessoais" são afirmadas como princípios.

• A "proteção à privacidade" e "a proteção de dados pessoais" são afirmadas como princípios.

• A "inviolabilidade da intimidade e da vida privada", bem como a "inviolabilidade e sigilo, salvo por ordem judicial, do fluxo das comunicações e das comunicações armazenadas", figuram como direitos assegurados.

• O texto estabelece o direito dos usuários terem "informações claras nos contratos de prestação de serviços, com detalhamento sobre as práticas de proteção aos registros armazenados", bem como sobre "coleta, uso, armazenamento e tratamento de dados pessoais". E ressalta ainda que "dados pessoais apenas poderão ser utilizados para finalidades que a) justifiquem a coleta; b) não sejam vedadas pela legislação e c) estejam especificadas nos contratos ou termos de uso."

• Também são estabelecidos como direitos o "não fornecimento a terceiros de dados pessoais, salvo mediante consentimento livre, expresso e informado". E o direito à, mediante requerimento, "exclusão definitiva dos dados pessoais que tivermos fornecido a determinada aplicação de internet, ressalvadas as hipóteses de guarda obrigatória". Trata-se, portanto, de uma previsão genérica, do direito ao esquecimento, referente apenas aos dados que o usuário cede ao provedor de aplicação (não se trata de dados publicados por terceiros) e aplicável apenas no término da relação entre as partes.

• Por fim, o artigo 8º reconhece que a "garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet" e, como tal, declara que serão nulas as cláusulas contratuais que impliquem na "ofensa à inviolabilidade e ao sigilo das comunicações ou que não ofereçam o foro brasileiro como opção para solução de controvérsias.

• Como se pode ver, a parte geral do Marco Civil, onde se estabelecem princípios, direitos e deveres dos usuários (capítulos I e II), ficou recheada de referências ao direito à privacidade. Mas, para além de algumas cláusulas que tratam de certos requisitos contratuais (principalmente transparência e consentimento informado), tais menções são principiológicas. Mais detalhes sobre como implementar a proteção da privacidade estão previstos no capítulo III, que trata da provisão de conexão e aplicações de internet ou ainda pendentes de regulação. Passando dos princípios à prática, observamos que de acordo com o capítulo III da Lei:

• Provedores de conexão devem manter registros de conexão por 1 ano, nos termos do regulamento. E são vedados de guardar registros de acesso a aplicações.

• Autoridade policial ou administrativa ou Ministério Público podem requerer guarda por prazo superior. Tal requerimento será mantido em sigilo pelo provedor responsável pela guarda dos re-

[1]Fonte: "Marco Civil é aprovado durante o NetMundial, mas ainda precisa ser regulado: o que esses dois marcos históricos nos dizem sobre a proteção da privacidade no Brasil?", Boletim Antivigilancia, Edição 09 https://antivigilancia.wiki.br/boletim_antivigilancia/9

gistros, desde que depois do pedido cautelar da autoridade haja ordem judicial para autorizar o acesso aos dados.

• Provedores de aplicação "constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet". É vedada a guarda de registros de acesso a outras aplicações se não houver consentimento do usuário e de dados pessoais excessivos em relação à finalidade do consentimento.

• Ordem judicial poderá determinar a guarda obrigatória de registros específicos para provedores que não se encaixam nesse perfil, desde que por período determinado.

• Autoridade policial ou administrativa ou Ministério Público podem requerer guarda por prazo superior. Aplicam-se aqui os mesmos critérios de acessos aos dados previstos para os registros de conexão.

• Parte interessada poderá requerer o fornecimento de registros de conexão ou de acesso a aplicações com o propósito de formar provas em processo cível ou penal, desde que apresente a) indícios da ocorrência de ilícito, b) justificativa da utilidade de tais registros e c) período dos registros requeridos.

• "O provedor responsável pela guarda somente será obrigado a disponibilizar os registros de conexão e de acesso a aplicações de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial."

• O conteúdo das comunicações privadas também só poderá ser disponibilizado por ordem judicial.

• Dados cadastrais poderão ser disponibilizados para "autoridades administrativas que detenham competência legal para sua requisição."

• Notamos, portanto, que já temos um sistema de proteção de alguns tipos de dados pessoais pré-estabelecido, mas que ainda carece de regulamentação que defina ainda mais as responsabilidades, métodos, periodicidade ou prazos para execução de algumas medidas específicas, que sejam compatíveis também com previsões gerais sobre a proteção de dados pessoais, como o APL de Dados Pessoais que está sendo debatido pelo Ministério da Justiça.

Cabe destacar que o fortalecimento dessa pauta específica, com a regulação do Marco Civil e retomada do debate do APL de Dados Pessoais, é, inclusive, indispensável para o adequado alinhamento entre a política interna e a agenda da diplomacia brasileira, a qual tem sido desenvolvida com elogiável notoriedade no plano internacional desde as revelações sobre a vigilância em massa de comunicações eletrônicas, seja como país sede e idealizador do processo do NETMundial; como patrocinador da Resolução da Assembleia Geral da ONU sobre Privacidade na Era Digital e sua atualização[2]; co-patrocinador de resolução na UNESCO para estudo sobre o tema[3]; trazendo a discussão da proteção este direito durante os debates das várias resoluções da Conferência Plenipotenciária da União Internacional de Telecomunicações – ITU[4], entre outros.

Tendo em vista o previsto nos dispositivos do Marco Civil que tratam da proteção da privacidade, destacamos a seguir algumas sugestões de como tais dispositivos poderiam ser regulamentados ou implantados.

[2] *https://antivigilancia.wiki.br/boletim_antivigilancia/10/01-ativismo-politicas#aprovada_revisao_da_resolucao_privacidade_na_era_digital*

[3] *https://antivigilancia.wiki.br/boletim_antivigilancia/10/01-ativismo-politicas#oficina_antigivilancia_submete_contribuicoes_a_consulta_da_unesco_para_estudo_compreensivo_sobre_assuntos_de_internet*

[4] *https://antivigilancia.wiki.br/boletim_antivigilancia/10/01-ativismo-politicas#brasil_levanta_o_tema_da_privacidade_na_conferencia_pleniponciaria_da_uit*

Propostas de regulamentação dos artigos do Marco Civil da Internet que tratam de privacidade e liberdade de expressão

1. O Art. 5º dispõe que:

> *(...)*
> *VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;*
> *(...)*
> *VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.*

Proposta:

Definição clara dos elementos que compõe registros de conexão e aplicações

A definição do artigo 5º sobre os elementos que compõe registros de conexão e de acesso a aplicações de internet deve ser considerada para fins do disposto nos artigos 13 e 15. Ou seja, para registro de conexão, não deverão ser mantidos dados para além de: a) data e hora de início e término de uma conexão à internet; b) duração; c) o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados. No mesmo sentido, entende-se como "o conjunto de informacões" do registro de acesso a aplicações a) data e hora de uso de uma determinada aplicação de internet; b) duração e c) endereço IP utilizado.

2. O Artigo 7º dispõe que:

> *Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:*
> *(...)*

> *VI – informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;*
> *VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;*
> *VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:*
> *a) justifiquem sua coleta;*
> *b) não sejam vedadas pela legislação; e*
> *c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;*
> *IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;*
> *X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;*
> *XI – publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;*
> *XII – acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e*
> *XIII – aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.*

Propostas:

Transparência, clareza, publicidade e proporcionalidade nas cláusulas contratuais (Incisos VI, VIII, XI)

A fim de atender o disposto no artigo, devem ser estabelecidos critérios mínimos para os contratos de prestação de serviços com base na legislação consumerista e com o objetivo de evitar prá-

ticas abusivas. Todavia, as preocupações legais relativas à transparência e à clareza não serão efetivamente atendidas se o foco estiver centrado somente nos contratos de prestação de serviço. Informações relevantes sobre coleta, uso, armazenamento, tratamento de dados pessoais devem ser apresentadas também por meio de outros mecanismos, mais explícitos e simplificados, ao longo da utilização da aplicação com configurações personalizáveis, cujo padrão seja o de maior proteção à privacidade ("privacy by design" e "privacy by default").

As condições ligadas à coleta e à utilização de dados pessoais podem ser objeto, ainda, de seção específica que organize tais informações de maneira mais interessante visualmente. Para além do estabelecimento de parâmetros regulamentares a partir dessas considerações, o poder público, e mesmo o CGI.br, podem avaliar e incentivar boas práticas de contratos de serviço e apresentação das informações, como realizando estudos comparativos e premiações a boas práticas.

Sobre o princípio da finalidade, a interpretação do art. 7º, VIII, a deve trazer a dimensão da proporcionalidade à sua aplicação. Isto é, os dados pessoais dos usuários só poderão ser utilizados para finalidades que se justifiquem diante do serviço/produto oferecido. Neste sentido, a finalidade informada, que vincula o provedor de conexão ou de aplicações, deve ser compatível ao que está sendo coletado. Por exemplo: um aplicativo sobre condições climáticas dificilmente terá justificativa para coletar dados referentes a SMS. A Diretiva 95/45/CE do Parlamento Europeu e do Conselho da União Europeia, que agora passa por processo de revisão, estabelece em seu art. 6º que os dados pessoais devem ser "adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e tratados posteriormente". Assim, além da informação e consentimento do usuário, é preciso que se explicite na regulamentação que a coleta e utilização de dados deve ser compatível, proporcional, ao serviço/produto oferecido.

Consentimento para a utilização de dados pelo provedor de aplicações (IX)

O inciso IX estabelece que o consentimento do usuário sobre coleta, uso, armazenamento e tratamento de dados pessoais deve ser expresso e ocorrer de forma destacada das demais cláusulas contratuais. Portanto, a lei deixa claro que o consentimento é anterior e condição para a realização de quaisquer dessas atividades, seguindo o modelo de opt-in. A regulamentação deverá observar, ainda, a segunda orientação prevista no inciso - de que o consentimento aqui referido seja destacado das demais cláusulas contratuais. Para o cumprimento dessa orientação não basta que haja um termo de uso enorme contendo uma cláusula específica para esse fim, mesmo que destacada em negrito, por exemplo. É preciso que a autorização em si seja específica e separada, informando da coleta, do uso, do armazenamento e do tratamento de dados pessoais, bem como de suas finalidades.

Ademais, de forma a evitar que uma série de funcionalidades sejam agregadas ao serviço/produto apenas para justificar a coleta excessiva de dados, é importante que o consentimento não seja único e para todas as funcionalidades ao mesmo tempo. A aplicação deve conter um núcleo básico e funcionalidades opcionais que o usuário decide utilizar ou não a partir de informações sobre funcionamento, vantagens, coleta e tratamento de dados pessoais. Isso é mais simples de ser adotado em serviços e produtos já existentes, quando passam a oferecer outras ferramentas, mas é relevante estabelecer parâmetros que permitam essa separação de maneira mais generalizada.

Em linha com esse entendimento, é preciso separar também o serviço oferecido e a publicidade direcionada. Eles devem constar de contratos e consentimentos independentes. A autorização em relação à segunda deve resultar da compreensão do usuário de que o direcionamento da publicidade representa uma vantagem para ele, sendo interessante que, após autorizado, o consumidor

consiga identificar a publicidade que resulta desse serviço. Sabe-se que a maior parte das aplicações online são financiadas por meio de publicidade e não se quer minar esse modelo de negócio. Porém, a publicidade direcionada passa pela utilização dos dados dos usuários para a composição de um perfil individualizado, algo que não ocorre com a publicidade comum. Não é razoável que aplicações de Internet possam condicionar a utilização de seu serviço à criação de um perfil de preferências e de navegação para cada um de seus usuários, o que não impede que ela por padrão divulgue anúncios não direcionados.

Consentimento para fornecimento de dados a terceiros (VII)

Ao consentimento do usuário para o fornecimento de seus dados a terceiros deve se aplicar tudo o que foi descrito acima para o art. 7º. Porém, há elementos específicos no inciso VII que não podem ser desprezados. O primeiro deles é a afirmação de que o consentimento deve ser LIVRE, qualificação que não consta do inciso IX. Isso significa que o fornecimento de seus dados a terceiros não pode ser condição para o usuário conseguir utilizar o serviço online, a não ser que esse fornecimento seja imprescindível à realização do serviço (como o fornecimento do endereço do cliente para que ele possa receber o produto comprado pelos Correios).

Outro elemento relevante é a repetição de que o consentimento deve ser expresso. Para garantir a efetividade do consetimento livre, é necessário que a autorização para o fornecimento de dados a terceiros seja nos moldes do opt-in e apartada dos demais consentimentos, informando-se quais são os terceiros e qual a razão do fornecimento dos dados do usuário. Em caso de prestação contínua de serviço (provedor de e-mail, redes sociais, entre outros), deve estar sempre disponível ao usuário a possibilidade de consultar os terceiros que estão recebendo seus dados e revogar as autorizações concedidas a cada um deles, ainda que esta opção desabilite determinada funcionalidade periférica do serviço.

Exclusão definitiva de dados fornecidos (inciso X)

De acordo com o art. 16, II, é vedada a guarda de dados pessoais excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular. Ademais, o próprio artigo 7º, VII, determina que a coleta de dados deve ser justificada. Nesse sentido, não se justifica a manutenção de dados após o término de contrato com o provedor de serviço. Tomando isso em consideração, pode-se considerar excessiva a guarda de dados pessoais após o término de contrato de aplicação de Internet, a não ser que o usuário a autorize expressamente. Assim, ao findar um contrato, o usuário deve ser avisado que os seus dados serão excluídos, dando-lhe a opção de mantê-los caso prefira assim.

O direito de excluir os dados disponibilizados deve se estender também aos terceiros que receberam informações sobre o usuário mediante consentimento específico. Além da possibilidade de revogar a autorização anteriormente concedida para que seus dados fossem transferidos a um terceiro determinado, o usuário deve ter o direito de excluir definitivamente seu banco de dados também em poder desses terceiros.

Por fim, é relevante que se fomente o uso de tecnologias que permitam ao usuário verificar se seus dados realmente foram excluídos dos bancos de dados. Por exemplo, o uso de chaves criptográficas para acessar determinado aplicativo, no qual apenas o usuário, nem mesmo o servidor, detém sua chave privada.

3. O artigo 10 dispõe que:

> *Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.*
>
> *§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autô-*

noma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado o seu direito de confidencialidade quanto a segredos empresariais.

Propostas:

Conceito de autoridade administrativa que tenham acesso a dados cadastrais (Art 10 § 3º)

O escopo da expressão "autoridade administrativa" no § 3º deverá seguir o mesmo entendimento do art. 17-B da Lei de Lavagem de Dinheiro – n.9613/1998:

"Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito. (Incluído pela Lei nº 12.683, de 2012)".

O regulamento deve explicitar esse entendimento para que não haja risco dessa competência ser atribuída a uma gama maior de autoridades.

Quebra de sigilo de comunicações (art 10 § 2º)

A regulamentação do parágrafo 2º do art. 10 deve deixar claro que a expressão "na forma que a lei estabelecer" faz referência ao inciso XII do artigo 5º da Constituição Federal e sua regulamentação, Lei 9.296 de 1996, que trata de interceptação de comunicações

Acesso a dados cadastrais (art. 10 § 3º)

Trata-se de exceção que possibilita acesso a dados bastante significativos e que impactam a privacidade. Sendo assim, é fundamental elencar de forma exaustiva as hipóteses que autorizem a quebra de garantia estabelecida no caput do art. 10.

Além disso, em respeito ao princípio da ampla defesa, a regulamentação deve estabelecer que o cidadão será informado a respeito do processo investigativo, admitindo-se como exceção apenas os casos em que se trate de apuração de crimes.

As medidas e os procedimentos de segurança (Art 10 § 4º)

O regulamento deve definir como padrões mínimo de segurança a encriptação obrigatória de banco de dados compostos por todas as informações de usuários e registros de conexão e acesso à aplicação armazenados, seja por requerimento desta lei ou por opção dos prestadores de serviços. Os provedores de conexão e aplicações apenas fornecerão a chave criptográfica diante de ordem judicial que requer acesso aos dados armazenados.

4. O artigo 11 dispõe que:

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das

comunicações privadas e dos registros.

§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Propostas:

Escopo e conceito de "oferta ao público brasileiro"

A regulamentação do Marco Civil deve deixar clara a relação entre os dois primeiros parágrafos do art. 11, evidenciando o âmbito de incidência desse dispositivo e conferindo segurança jurídica à sua aplicação. Neste sentido, os critérios para a sua incidência devem contemplar cumulativamente:

- operação de coleta, armazenamento, guarda ou tratamento de dados pessoais ou de comunicações realizados em território nacional; e

- um dos terminais da interação online localizado no país. No caso de pessoa jurídica sediada no exterior, o caput aplica-se se, além dos dois requisitos acima, ao menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil OU por pessoa jurídica sediada no exterior cujo serviço que possibilitou a operação se enquadre como "oferta ao público brasileiro".

Quanto ao enquadramento como "oferta ao público brasileiro", presente no §2º do art. 11, o principal para a sua caracterização é a identificação de elementos que denotem o direcionamento da oferta aos brasileiros. O idioma utilizado (português do Brasil) ou a entrega de produtos em território nacional podem ser parâmetros a se ter em consideração, assim como outras referências que atraiam especificamente consumidores brasileiros.

Já no que se refere ao §3º, a prestação de informações nele prevista deve ocorrer mediante solicitação da autoridade competente (ver item final desta contribuição) em razão de indícios de descumprimento da legislação nacional relacionada à privacidade e proteção de dados pessoais. É temerário estabelecer à totalidade de provedores de aplicações que se enquadrem nos critérios estabelecidos acima uma obrigação a priori e periódica de prestação de informações, tendo em vista que muitos deles não teriam estrutura para fazê-lo de maneira adequada e tempestiva.

Por fim, considerado o interesse público envolvido na verificação do cumprimento da legislação e do acesso às informações prestadas, as solicitações realizadas pela autoridade competente deverão ser objeto de relatórios periódicos que indiquem o que foi solicitado, por qual autoridade e qual a resposta recebida. Os relatórios devem ser divulgados pelas autoridades que solicitarem e pelos provedores que receberem a solicitação dentro da periodicidade definida para o relatório (anual, no máximo).

5. O art. 12 dispõe que:

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I – advertência, com indicação de prazo para adoção de medidas corretivas;

II – multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos,

considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III – suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV – proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Proposta:

Balanço entre direito de acesso a serviços, privacidade de usuário e monitoramento de infrações

O monitoramento de possíveis infrações deve considerar que não se estabeleçam medidas desproporcionais, a fim de evitar que qualquer provedor seja considerado um potencial infrator da legislação e acabe acarretando ou em exclusão de usuários brasileiros de determinadas plataformas ou em um monitoramento do próprio usuário. Dessa forma, deve ser estabelecido que o método prioritário de investigação e monitoramento não se dê pela análise ostensiva dos dados acumulados pelos provedores.

6. O Artigo 13 dispõe que:

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Proposta:

Determinação para exclusão de log de conexão a internet

Como o prazo de 1 ano é o prazo máximo para a guarda de registros de conexão, os registros de conexão de mais de um ano, bem como eventuais cópias, devem ser excluídos definitivamente, salvo se houver solicitação para guarda por período superior, atendendo aos requisitos do artigo 13, caso em que a exclusão dos dados acompanhará o prazo estipulado no pedido de extensão.

Guarda cautelar: prazo e autoridade competente (Art 13, 2º)

A regulamentação deve deixar o parágrafo 2º mais claro, estabelecendo quais autoridades administrativas tem competência para requerer guarda cautelar e explicitando o limite de tempo para essa guarda.

Entende-se pelo artigo 3º que a guarda cautelar dos registros de conexão sob pedido de autoridade administrativa ou policial não poderá exceder 60 dias, sendo que um período maior só poderá ser estabelecido por um juiz. Caso a ordem judicial após esse processo autorize a manutenção da guarda, ela também deverá ter prazo determinado e proporcional à finalidade.

7. O Artigo 15 dispõe que:

> *Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.*
>
> *§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.*
>
> *§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.*
>
> *§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.*
>
> *§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.*

Propostas:

Limitação do escopo de provedores de aplicação com obrigação de guarda e retenção de dados

As alterações do artigo 15 no processo de aprovação do Marco Civil foram alvo de críticas severas, pois, ao mesmo tempo em que os dispositivos que ampliam a proteção à privacidade no Marco Civil foram fortalecidos, a ampliação da obrigação de guarda de registros para os provedores de aplicações (algo que não estava previsto nas versões anteriores do texto) acaba enfraquecendo a proteção deste direito, pois, quanto mais dados são armazenados, maior a probabilidade de que sejam utilizados ou vazados em ameaça à privacidade de usuários. Ou pior, se o entendimento da obrigação da guarda se estende a qualquer provedor estabelecido como pessoa jurídica com fins lucrativos, o Brasil acaba impedindo o desenvolvimento de uma indústria de aplicativos que tenham como objetivo a proteção da privacidade.

Por outro lado, entende-se que o legislador optou por deixar explícito que os "grandes players" da indústria de TI que já monetizam esses dados deverão fazê-lo respeitando o Marco Civil. Portanto, entendendo tal necessidade, é importante que a regulamentação deixe mais explícito o escopo da obrigação da guarda apenas para esses "grandes players", que lucram justamente com a guarda destes dados pessoais. Nesse sentido, a regulamentação deve deixar claro que a obrigação prévia de guarda se aplica ao provedor cuja a monetização destes dados pessoais seja o seu negócio, ou ao menos, pode-se limitar o perfil da obrigação por meio de requisitos como teto de faturamento, finalidade das atividades (assim, se uma pessoa jurídica com fins lucrativos tenha a finalidade de proteger a privacidade, não terá tal obrigação de guarda) e necessidade de login, em que efetivamente se configura a existência de um usuário cadastrado que realiza ações. Considerando que as aplicações que mais geram pedidos de acesso a dados possuem essas características, a generalização da obrigação de guarda prévia pode justamente colocar em risco o que o Marco Civil procurou proteger em um de seus pilares – a privacidade do usuário.

Guarda cautelar: razão, prazo e autoridade competente

No caso do parágrafo 1º, a concessão da ordem judicial para provedores não comerciais guardarem deve estar condicionada a requisitos mínimos fixados em regulamentação. O pedido da guarda deve ser específico a determinado serviço, proporcional e justificado por indícios de ilícito que se relacionam com o uso de tal serviço. A notificação ao usuário sobre o pedido da guarda

cautelar deve ser a regra, podendo haver exceções, desde que justificadas pelo sigilo da investigação.

Além disto, assim como o que elencamos no artigo 13, a guarda precaucionaria dos registros de aplicação sob pedido de autoridade administrativa ou policial não poderá exceder 60 dias, sendo que um período maior só poderá ser estabelecido por um juiz. Caso a ordem judicial após esse processo autorize a manutenção da guarda, ela deverá ser renovada periodicamente. O conceito de autoridade administrativa com competência para requerer tal guarda também deve ser especificado em regulamentação.

Encriptação e exclusão de dados depois de 6 meses

Assim como o elencado no artigo 10, obrigações de guarda devem ser acompanhadas de obrigações de encriptação de bancos de dados. E, de acordo com o inciso X do artigo 7, a possibilidade de pedir a exclusão definitiva de dados armazenados após 6 meses também deve estar disposta na regulamentação.

Determinação para exclusão de log de aplicação

A obrigação de guarda de 6 meses para os provedores estabelecidos no caput do Artigo 15º não pode ensejar uma guarda excessiva de dados por provedores de aplicação que não necessitam armazenar tais registros de acesso.

Sendo assim, findado o prazo de 6 meses, os dados armazenados pela obrigação de guarda deverão ser definitivamente excluídos, salvo se comprometerem a prestação do serviço. Ou seja, caso haja manutenção da guarda, esta deve ser justificada por atender aos princípios estipulados no artigo 7º, entre eles, a vedação à guarda de dados excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular. A opção por regulamentar a exclusão de dados armazenados como padrão, sendo a exceção a guarda justificada, visa proteger direitos do consumidor e a

privacidade dos usuários de internet, evitando que sejam criadas situações de vulnerabilidade excessiva pela compilação de seus registros de conexão.

8. Artigo 16 dispõe que:

> *Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:*
>
> *I – dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou*
>
> *II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.*

Proposta:

Fiscalização

Como o Marco Civil já está em vigor, a garantia da implementação do disposto na sessão de privacidade também já está em prática e pode ser fiscalizada por entidades como os Procons, o MP e a SENACON. Contudo, consideramos importante debater no âmbito do APL de dados pessoais uma autoridade específica que garanta a proteção de dados pessoais.

Para auxiliar na fiscalização por meio de evidências empíricas, deve-se incentivar e fomentar o uso de softwares ou aplicativo para usuário poder monitorar o cumprimento, além da fiscalização do poder público.

Por exemplo, o desenvolvimento de um software e/ou aplicativo pelo NIC.br, público e de código aberto, que permita qualquer usuário de internet verificar quem está recebendo o tracking de sua navegação tem eficácia limitada, mas permite um grau mínimo de controle dos usuários de como suas atividades na internet são monitoradas. Inclusive, tal mecanismo poderia facilitar o contato do usuário com os receptores dessas informações, caso desejasse.

Já existem alguns exemplos de mecanismos que estão disponíveis na rede para que o usuário comum possa ter noção de quem está observando-o. Além disso, existem diversos aplicativos que garantem maior privacidade para o usuário.

O Detekt é uma ferramenta gratuita que vasculha o computador em busca de algumas ferramentas de vigilância (spywares) comerciais que podem estar sendo empregadas por interessados e é um resultado da parceria entre a Anistia Internacional, a Privacy International, a Digitale Gesellschaft e a Electronic Frontier Foundation.

Um outro exemplo de ferramenta interessante presente na rede é um Programa de Autorregulação para Propaganda Comportamental da Digital Advertissem Alliance (DAA). A página serve para que os consumidores optem por não serem alvos de propaganda comportamental dentro de uma lista de sites já participantes do projeto. O opt out oferecido é uma resposta de diversas companhias que buscam alinhamento com os padrões internacionais de privacidade, transparência e escolha.

Plataforma simples, presente em websites acessíveis e integradas são o Trace My Shadow e O Trackography, ambas presentes no Me & My shadow , iniciativa que objetiva de maneira didática conscientizar e ajudas usuários a administrarem melhor os seus rastros deixados na rede. O primeiro analisa quais são os rastros que o usuário deixa na rede com base nos seus históricos de navegação online. Já o segundo objetiva demonstrar como funciona a indústria de informações sobre os usuários no mundo através do uso de rastreio, ou tracking, em sites de notícia. A prática tem como objetivo definir perfis baseados nos comportamentos observados.

Uma plataforma desenvolvida pelo NIC.br poderia unificar todos esses exemplos e ainda ir além.

[5] *https://resistsurveillance.org/*
[6] *http://www.aboutads.info/choices/*

9. Artigo 19 dispõe que:

> *Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.*
>
> *(...)*
>
> *§ 3o As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.*
>
> *§ 4o O juiz, inclusive no procedimento previsto no § 3o, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.*

Proposta:

Observação do interesse da coletividade

A regulamentação do Marco Civil deve deixar clara a relação entre o inciso 3o e 4o, evidenciando "o interesse da coletividade na disponibilização do conteúdo na internet" principalmente quando se tratar de pleitos realizados por pessoas de notoriedade pública no exercício de sua atividade. Isso se faz necessário uma vez que os expedientes relacionados à honra, à reputação ou a direitos de personalidade são recorrentemente utilizados para limitar a crítica e reprimir o debate público.

10. O Artigo 21 dispõe que:

> *10. Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.*

Propostas:

Procedimento para retirada de materiais contendo cenas de nudez e atos sexuais

Conforme o art. 21 estabelece, um material apontado como violador da intimidade deve ser especificamente apontado e posteriormente retirado. Uma plataforma inteira não poderá ser retirada do ar por conta de um conteúdo em específico.

Para que o conteúdo violador seja retirado, a notificação deve ser feita conjuntamente à apresentação de documento pessoal ou por representante legal com procuração, além de uma declaração da vítima confirmando que é mesmo a participante do conteúdo violador.

A pessoa que publicou o conteúdo deverá ser notificada a fim de que possa tomar as medidas cabíveis caso considere que a remoção do conteúdo foi indevida e afeta seu direito à liberdade de expressão.

11. Mecanismos e instâncias de defesa

Qualquer exercício de regulamentação dos dispositivos sobre privacidade do Marco Civil da Internet deixa evidente que para a implementação do previsto, principalmente nos artigos 7, 8, 10, 13, 14, 15 e 16, depende de uma autoridade de proteção de dados pessoais.

Não há de se ignorar que órgãos de proteção de defesa do consumidor e o Ministério Público terão um papel importante, mas, à luz das boas práticas, particularmente em países da Europa, conhecido por alto padrão de proteção da privacidade, outro tipo de autoridade seria necessário. Entre suas atribuições estariam assegurar que estes dados são guardados com segurança; que o consentimento foi feito de forma clara, livre e expressa, ou até mesmo para que se estabeleçam procedimentos para o fornecimento das "informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados", de maneira que possa haver efetividade quanto ao cumprimento da lei e garantias de que tais procedimentos não estejam sendo usados de maneira abusiva contra os usuários, com eventuais compartilhamentos de dados para fins comerciais ou possíveis violações do direito à privacidade por parte do Estado.

Nesse sentido, é bem vinda a discussão da regulamentação do Marco Civil de forma paralela ao debate do Anteprojeto de Lei de Dados Pessoais, que deverá analisar qual a melhor composição deste tipo de autoridade de proteção de dados, mas cuja existência deveria er referência, ainda que ampla, na regulamentação do Marco Civil da Internet.