OFICINA
ANTIVIGILÂNCIA

DADOS PESSOAIS:

Como contribuir para o debate público

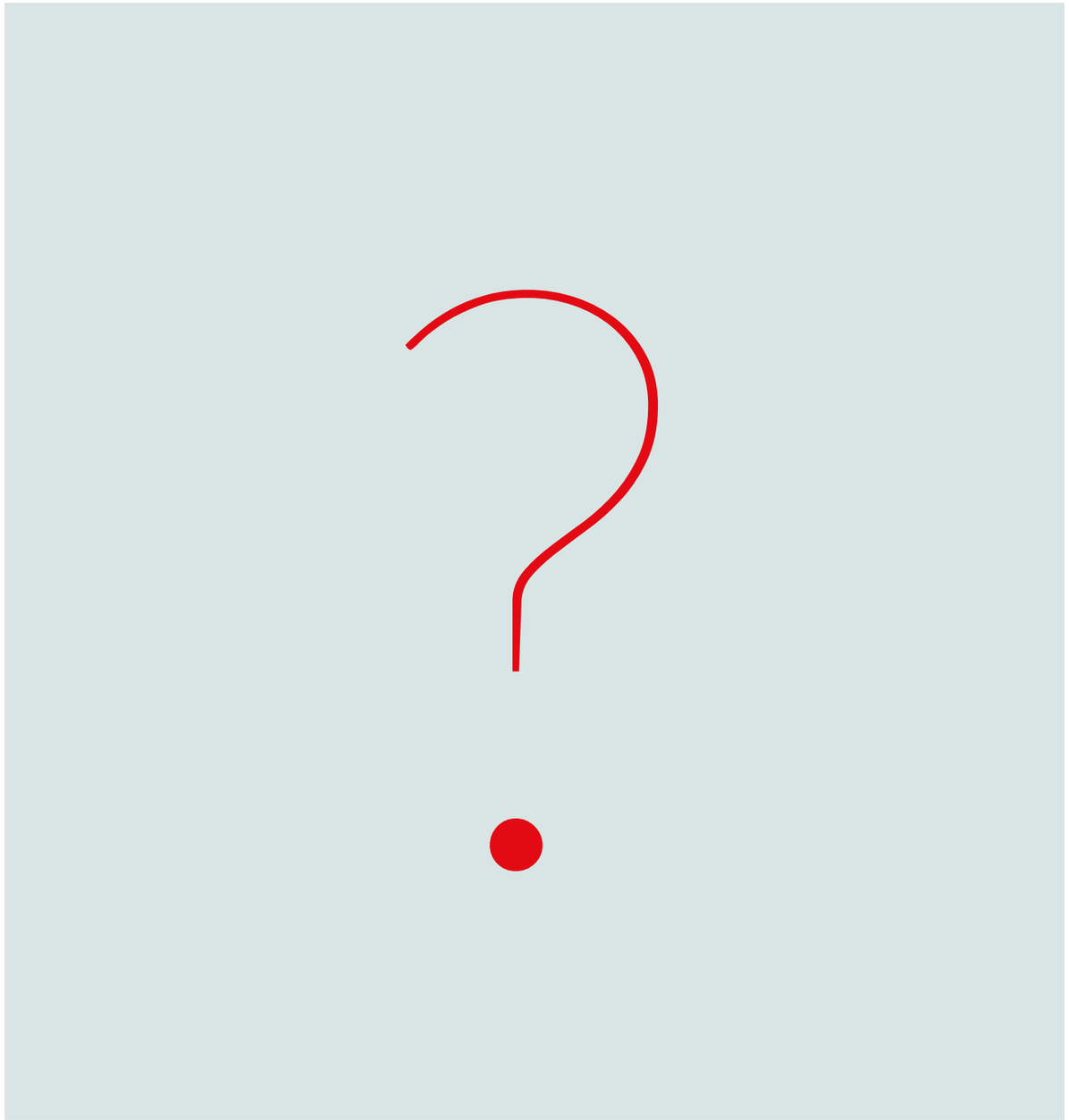
1 Apresentação

A intenção desta cartilha é ajudar o cidadão a entender o Anteprojeto de Lei de Proteção de Dados Pessoais, que foi colocado em debate público na internet pelo Ministério da Justiça em 28 de fevereiro de 2015 no site: ***http://participacao.mj.gov.br/dadospessoais/***

A cartilha está dividida em capítulos, cada um dos quais corresponde a um dos eixos em torno dos quais se estrutura o debate.

Índice

2/ Introdução



Por que proteger dados pessoais?

Uma lei sobre proteção de dados permite que o cidadão tenha controle sobre como suas informações são utilizadas por organizações, empresas e pelo governo. Ela estabelece padrões mínimos a serem seguidos quando dados pessoais são utilizados, como a limitação a uma finalidade específica, a criação de um ambiente seguro e controlado. O impacto de uma lei sobre proteção de dados pessoais é evidente quando empodera o cidadão de forma a equilibrar certas assimetrias de poder existentes entre aquele que é o titular dos dados pessoais e aqueles que usam e compartilham seus dados.

Como participar do debate público sobre o anteprojeto de lei sobre dados pessoais?

*A participação no debate público é feita pela plataforma **dadospessoais.mj.gov.br**. Para participar, primeiro, deve-se fazer o cadastro na plataforma para obter nome de usuário e senha.*

Há três diferentes formas de participar:

1.

Comente cada ítem do texto de lei sugerido no site. Você pode comentar capítulos, artigos, incisos, parágrafos e alíneas.

2.

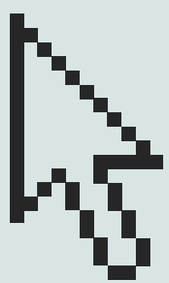
Comente os eixos temáticos sugeridos que refletem algumas das principais ideias a serem contempladas em uma lei geral de proteção de dados pessoais.

3.

Envie comenários ou contribuições consolidadas em formato de PDF.

Você ainda pode interagir com demais participantes do debate ao reagir e responder a comentários feitos por eles.

www.dadospessoais.mj.gov.br



3/ Eixos

Escopo e aplicação

/ arts. 1º a 4º

O Anteprojeto é de uma lei geral sobre proteção de dados pessoais. Como é geral, deve ser válida para todo tratamento de dados pessoais que seja relevante, independentemente de ser realizado pelo setor público ou pelo setor privado, seja por qual setor econômico ou sob quais justificativas. Se o objetivo do Anteprojeto é a proteção do cidadão, esta proteção deve ser garantida sempre que seus dados pessoais são tratados.

Somente o cidadão é protegido. A pessoa jurídica não, já que seus dados estão protegidos por outros instrumentos (sigilo, segredo comercial, industrial etc).

A lei protege o cidadão sempre que o tratamento de seus dados ocorrer em território nacional.

Algumas exceções à aplicação da lei são previstas. A primeira é o tratamento de dados pessoais por um cidadão para fins estritamente pessoais , como é o caso de uma agenda telefônica para uso estritamente pessoal, por exemplo.

A segunda exceção é a utilização de dados pessoais para fins exclusivamente jornalísticos. Neste ponto procurase evitar que a proteção de dados limite a atividade jornalística e, consequentemente, a colisão com os direitos de liberdade de informação e de expressão.

A terceira exceção diz respeito às atividades de segurança pública, defesa, segurança do Estado ou atividades de investigação e repressão de crimes. Exceções desta natureza estão previstas em praticamente qualquer norma de proteção de dados pessoais, mas condicionadas à diferentes situações. No caso do Anteprojeto em consulta, exceções à proteção de dados por fins de segurança estão previstas em casos (i) em que há referência à legislação específica para regular o tratamento de dados pessoais nessas atividades, e (ii) em que os princípios de proteção de dados pessoais e os direitos do titular dos dados previstos no Anteprojeto sejam observados.

Destaque: *Atividade jornalística, exceção à proteção para atividades de segurança pública.*

Questões: *Quais os limites da atividade jornalística? Ela compreende blogs pessoais? Intervenções em redes sociais poderiam ser protegidas? O Anteprojeto deixa margem para ser utilizado como instrumento limitador da liberdade de expressão e de informação? Os limites que se estabelecem para a exceção à proteção de dados para atividades de segurança pública são suficientes?*

Definições
/ arts. 5º

O Anteprojeto de lei sobre proteção de dados traz um conteúdo de relativa tecnicidade. As definições presentes no Anteprojeto funcionam, portanto, como uma espécie de glossário dos temas recorrentes em matéria de proteção de dados. Esta é a primeira vez que procura-se legislar sobre o assunto. Sendo assim, embora algumas das definições possam ser ancoradas em entendimentos e conceitos já presentes no ordenamento brasileiro, muitas outras são novidade na legislação e não são facilmente referenciáveis. O que somente aumenta a importância deste capítulo das definições.

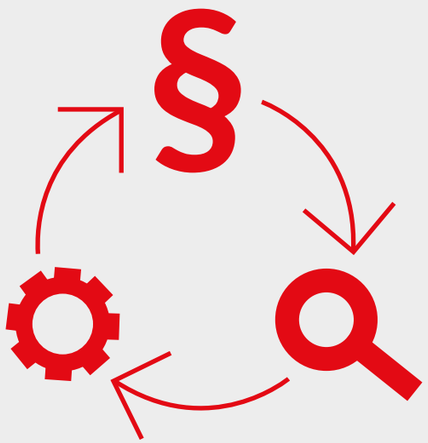
Qualquer dado que possa ser associado a um indivíduo pode ser considerado dado pessoal. Mas será que tudo quanto é dado que pode ser atribuído a uma pessoa deve ser protegido? Esta definição é fundamental para delimitar o escopo de aplicação da lei, e pode influenciar no equilíbrio de poder entre o cidadão e aquele que coleta e utiliza seus dados. Colabore nesta definição!

De forma quase oposta à ideia de associação com um indivíduo, os dados anônimos, por sua vez, são dados que não permitem a identificação de pessoas, ainda que sejam referentes a uma pessoa ou grupo. Um exemplo de dados anônimos são os dados estatísticos.

No debate sobre a definição de dados pessoais, há ainda a necessidade de se considerar o que seriam "dados sensíveis", ou seja, dados cujo tratamento pode gerar a discriminação do seu titular por se referirem, por exemplo, à opção sexual, convicções religiosas, filosóficas ou morais, ou opiniões políticas. Os dados sensíveis, pelo potencial discriminatório que apresentam, de acordo com a proposta em questão, deveriam ser protegidos de forma mais rígida.

{ ***Destaque:*** *Definição de dado pessoal e de dados anônimos*

Questões: *Os dados anônimos devem simplesmente ficar fora do escopo da lei, ou seria necessário que fossem tratados em alguma medida? Tendo em vista a possibilidade de que a evolução das tecnologias torne possível re-identificar dados anônimos, ou que tais dados ainda podem ser utilizados para compor perfis sócio-econômicos, como lidar com o conceito de dado anônimo?*



Princípios

/ *art. 6º*

Os princípios de proteção de dados presentes no texto sob consulta são uma espécie de espinha dorsal de todas as lei de dados pessoais. Eles garantem a homogeneidade e eficácia da lei, a comunicação de seu conteúdo e também a compatibilidade com legislações de outros países que utilizam princípios semelhantes.

Princípios não são apenas direcionamentos ou sugestões, são normas e devem ser aplicados diretamente, ainda que não exista maior detalhamento sobre seu conteúdo. Por exemplo, em uma situação futura, na qual a coleta e tratamento de dados aconteça de alguma forma impossível de ser prevista no momento de elaboração da lei, podemos entender que se a lei tiver uma previsão garantindo o princípio da transparência, que assegura que o titular tenha sempre informações claras sobre o que é feito com seus dados, o problema estaria resolvido.

Além deste caráter normativo, os princípios de proteção de dados também são importantes pelo seu conteúdo didático. Uma lei de proteção de dados, como a proposta no Anteprojeto, apresenta um grande número de instrumentos e técnicas novas para o jurista e para a própria sociedade se apropriarem. Mas um olhar atento aos seus princípios permite compreender, com maior facilidade e rapidez, as diretrizes básicas de interpretação de todo o texto da lei e os valores que se procura proteger. É o caso do princípio da finalidade que condensa grande parte dos efeitos desejados da lei ao deixar claro que a informação pessoal somente poderá ser utilizada de acordo com a finalidade para a qual foi colhida, após o prévio conhecimento e autorização de seu titular. Nesta simples previsão, o princípio da finalidade não apenas exige eficácia à transparência e ao consentimento, como também traça um nítido limite entre o uso lícito e o uso abusivo dos dados pessoais.

Alguns dos princípios hoje descritos no Anteprojeto já estão presentes na Constituição ou em outras normas, é o caso dos princípios de livre acesso, transparência, proporcionalidade ou segurança. Outros estão especificamente ligados à proteção de dados, como o: a) princípio da necessidade, que procura coibir o tratamento de dados sem que ele esteja ligado a um objetivo específico; b) princípio da não discriminação, que faz a ponte entre a proteção de dados e a proteção de outros direitos fundamentais; c) o princípio da prevenção, que faz a interseção entre privacidade e segurança da informação, tornando clara a preferência por uma série de medidas técnicas que visem a evitar danos no uso de dados pessoais, como, por exemplo, as técnicas de privacidade na concepção (privacy by design) ou de privacidade como padrão (privacy by default).

{ ***Destaque:*** *Princípio da prevenção*

Questões: *A presença do princípo da prevenção, por si só, pode favorecer a inserção da proteção da privacidade e dos dados pessoais no projeto de novos produtos e serviços (privacy by design), ou seria necessário que disposições legais específicas tratem do assunto?*

Consentimento

/ arts. 7º a 11

O controle do cidadão sobre o que é feito com seus dados pessoais é a finalidade e razão de ser do Anteprojeto, e o consentimento para o tratamento destes dados é um dos instrumentos que lhe permite exercer este controle. Sendo assim, o Anteprojeto dispõe que o tratamento de dados pessoais somente é legítimo (i) se houver o consentimento do titular, ou (ii) se houver prévia autorização legal.

O consentimento é o instrumento através do qual o cidadão pode expressar livremente sua vontade em relação ao que possa ser feito com os seus dados pessoais. Por isso, especificou-se alguns atributos para que o consentimento seja válido: ele deve ser livre, expresso, específico e informado. A vontade só é livre se refletir uma opção real, sem constrangimentos, diante de um cenário que é conhecido pelo cidadão. Daí a necessidade de que o consentimento seja informado, isto é, de que o cidadão conheça as circunstâncias, e possíveis consequências, do tratamento de seus dados antes de tomar qualquer decisão a respeito de consentir ou não com a sua utilização. Ele deve ser também expresso e específico, para evitar que se deduzam autorizações diante de situações nas quais o cidadão de fato não manifestou a sua vontade.

Em alguns casos excepcionais, o Anteprojeto determina que poderá ser dispensado o consentimento. Trata-se, geralmente, de quando a sua exigência conflitar com outro direito, ou quando o risco concreto ao titular for mínimo. São os casos de utilização de dados de acesso público, cumprimento de obrigação legal, proteção da saúde e vida e outros. Por outro lado, há também casos específicos em que o consentimento poderia ser ainda mais relevante, como no caso dos dados sensíveis.

Outro ponto relevante em relação à exceção ao consentimento é que o Estado poderá realizar o tratamento de dados pessoais sem que solicite o consentimento do titular, dentro das competências institucionais e previstas em legislação de cada órgão da administração pública. Esta exceção pressupõe que a atuação do Estado sempre é pautada pelo princípio da legalidade que, por sua vez, caminha junto com o dever de transparência, além da obrigação de seguir as demais regras aplicáveis ao tratamento de dados.

Destaque: *Consentimento e autodeterminação informativa. Consentimento e tratamento de dados pelo setor público.*

Questões: *O consentimento é o único instrumento possível para o exercício da autodeterminação de cada cidadão em relação a suas informações pessoais? Que outros instrumentos existem, e quais as mudanças que poderiam ser feitas ao consentimento, segundo previsto no Anteprojeto, para que possa espelhar melhor a vontade livre do cidadão? Faz sentido restringir o consentimento no caso de tratamento de dados pelo setor público ou deveriam haver outras limitações?*

Término do tratamento

/ arts. 14 e 15

A noção de que o armazenamento de dados pessoais pode representar algum tipo de risco para o cidadão, assim como o entendimento de que qualquer tratamento de dados deva ser devidamente justificado, são alguns dos pressupostos do Anteprojeto. Assim, é possível evitar que dados sejam tratados indefinidamente, com potencial risco ao deveres de segurança e sujeitando o cidadão a abusos.

Desta forma, a regra geral é que os dados pessoais devem ser cancelados após o esgotamento da finalidade para a qual foram coletados e tratados. O que, por exemplo, diminui o risco da apropriação indevida por terceiros.

Há situações, no entanto, em que legítimos interesses podem justificar a manutenção destes dados para além da finalidade do seu tratamento. São casos em que algum interesse específico sugere que eles possam ser relevantes, por exemplo, para finalidades de pesquisa histórica, caso em que estes dados deverão ser mantidos, em geral, na sua integridade. Há outros casos nos quais os dados pessoais podem ser relevantes, porém não precisem mais ser necessariamente ligados as seus titulares. Nesses casos, os dados podem ser submetidos a um processo de dissociação, no qual devem perder o vínculo com seus titulares, de forma a não ser mais possível identificar a quem um determinado dado se refere. Considerando um processo de dissociação eficiente, tais dados podem ser úteis e mantidos para finalidades de pesquisa científica e estatística, por exemplo.

Destaque: *Consentimento e autodeterminação informativa. Consentimento e tratamento de dados pelo setor público.*

Questões: *Um argumento que muitas vezes é levantado por setores da indústria e mesmo da comunidade científica é o de que o armazenamento de dados pessoais, dadas as possibilidades tecnológicas, pode ser um bem em si, posto que futuramente podem ser identificadas utilidades para estes dados que não eram claras ou previsíveis no momento da sua coleta. Como este argumento pode, se for o caso, dialogar com uma regra geral que prevê o cancelamento de dados cuja finalidade esteja exaurida?*

Direitos do titular
/ arts. 16 a 21

Os direitos do cidadão em relação aos seus dados pessoais, ou seja, do titular destes dados, são tratados em uma seção específica do Anteprojeto. Eles podem ser resumidos como os direitos ARCO, isto é, direitos de Acesso, Retificação, Cancelamento e Oposição.

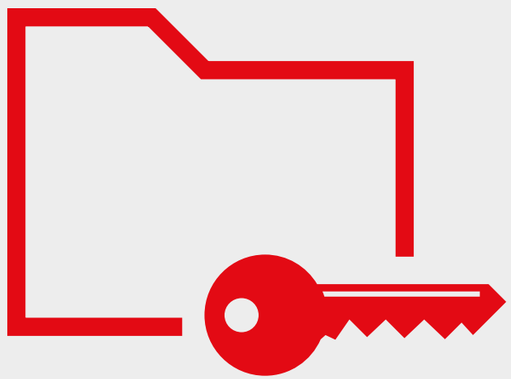
Cada um destes direitos significa respectivamente que: a) o cidadão deve poder acessar livremente os seus dados pessoais e tem o direito de ser informado sobre qualquer operação de tratamento desses dados; b) tem o direito de corrigir e retificar os dados pessoais que estejam incorretos ou imprecisos; c) tem o direito de solicitar o cancelamento de operações de tratamento que não sigam os parâmetros estabelecidos pela lei; d) tem o direito de se opor a um tratamento de dados pessoais que não tenha autorizado previamente.

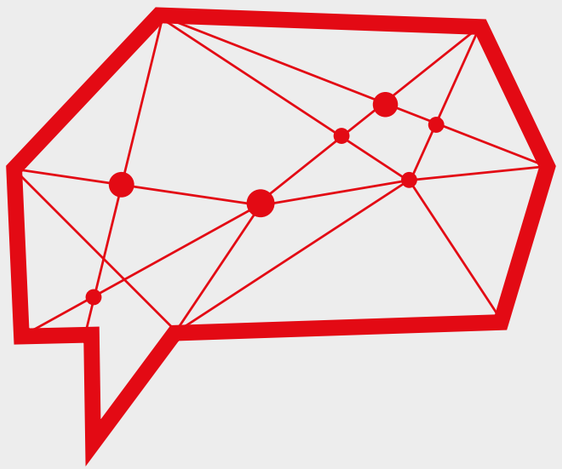
Também fazem parte dos direitos do titular o poder de solicitar o bloqueio do tratamento, até que seja averiguada a sua legitimidade, ou mesmo a dissociação dos seus dados pessoais, que passariam a ser dados anônimos.

Além de garantir direitos para que os titulares garantam um nível elevado de proteção de dados, o Anteprojeto também prevê obrigações que independem de ação do titular do dado para que aqueles que tratam dados pessoais sejam monitorados e fiscalizados pelas autoridades competentes. Desta forma, evita-se uma situação na qual o ônus integral do acompanhamento e monitoramento dos tratamentos de dados pessoais fique a cargo somente do cidadão.

Destaque: *O direito à portabilidade dos dados pessoais, previsto de art. 18, § 3°.*

Questões: *Os direitos previstos no Anteprojeto proporcionam efetivo controle ao cidadão sobre seus dados, ou há outros direitos que lhe deveriam ser atribuídos?*





Comunicação, Interconexão e Uso Compartilhado de dados

/ arts. 22-27

A comunicação de dados pessoais se dá quando estes são transferidos a um novo responsável; já a interconexão ocorre quando os dados pessoais passam a integrar um novo banco de dados. Em ambos os casos, há mudanças que podem ser relevantes para o titular dos dados, como a mudança do responsável pelo tratamento, ou a utilização de sua informação em um novo banco de dados, que pode ter finalidades e efeitos diferentes.

De acordo com o texto do Anteprojeto de lei de dados pessoais, quando estas operações são realizadas, tanto o cedente (aquele que comunica os dados pessoais), quanto o cessionário (aquele que recebe), são responsáveis pelo que for realizado com esses dados. O objetivo de tal previsão é evitar que essas operações limitem a possibilidade do titular do dado fazer valer seus direitos contra quem lhe for mais próximo ou conveniente.

Mas, de acordo com o Anteprojeto, o consentimento a ser requerido varia de acordo com os atores envolvidos nestas operações. Para que a comunicação ou interconexão ocorra entre empresas privadas, é necessário que o titular dos dados as autorize de forma livre, expressa e informada. Para que órgãos públicos compartilhem ou realizem interconexão de dados pessoais com empresas privadas, a autorização também é necessária. Mas este consentimento pode ser dispensado em algumas hipóteses, como, por exemplo, depois de avaliação e autorização por órgão competente, como seria o caso de uma autoridade de proteção de dados pessoais, desde que condicionada à verificação de interesse público e, por vezes, prevista alguma contrapartida, como a necessidade de publicidade da operação ou mesmo o cumprimento de alguma outra obrigação.

Destaque: *A transparência na comunicação e interconexão de dados é ressaltada sempre que não é necessária a obtenção do consentimento do titular.*

Questões: *Para que a transparência sobre a comunicação e interconexão seja eficaz, de que forma ela deve ser feita?*

Transferência internacional de dados

/ arts. 28 a 33

A transferência de dados pessoais entre diferentes países foi tremendamente facilitada pelas novas tecnologias da informação. Como esta transferência não costuma apresentar custos ou barreiras técnicas mais relevantes do que aquela realizada dentro das fronteira de um país, surgem problemas concretos relativos à jurisdição e à própria eficácia de uma legislação de proteção de dados.

A eficácia da legislação está diretamente relacionada à proteção dos cidadãos: caso uma legislação permita que dados pessoais transitem para outro país cuja legislação não possua normas semelhantes, há o risco de que as atividades de tratamento de dados pessoais sejam realocadas para este outro país, fazendo com que os cidadãos, de fato, não possam usufruir de seus direitos, e sofram os efeitos do um eventual tratamento abusivo.

Para evitar uma situação como esta, que poderia minar a eficácia de uma legislação de proteção de dados, o Anteprojeto condiciona o fluxo internacional de dados pessoais dos cidadãos brasileiros a países que possuam níveis equiparáveis de proteção da privacidade e de dados pessoais. Desta forma, temos maior ênfase na transparência de acordos internacionais, bilaterais ou regionais que versem sobre o tema e no incentivo a adoção de padrões contratuais internacionalmente conhecidos.

O favorecimento da utilização lícita de dados pessoais, observadas as garantias de seus titulares, é um dos incentivos que se pretende criar com esta proposta, fazendo com que a utilização de dados pessoais seja realizada por agentes responsáveis e fomentando o desenvolvimento de setores econômicos ligados, por exemplo, às tecnologias de informação.

{ ***Destaque:*** *Padrões equiparáveis de proteção da privacidade*

Questões: *O que seriam níveis equiparáveis de proteção de dados pessoais? Como serão tomadas as decisões referentes a autorizações e permissões para transferência internacional de dados? É necessário uma autoridade especializada, ou essa função pode ser desempenhada por órgãos já existentes?*

Responsabilidades dos agentes

/ arts. 34 a 41

No texto do Anteprojeto de lei sob consulta, os agentes do tratamento de dados pessoais são o responsável e o operador. O responsável é aquele em nome de quem os dados pessoais são tratados, que o faz em seu interesse e toma as decisões acerca do tratamento. Já o operador apresenta um caráter marcadamente técnico em relação ao tratamento, executando-o no interesse e de acordo com as instruções que lhe são fornecidas pelo responsável.

Por fim, o encarregado, mencionado no art. 41, não é propriamente um agente de tratamento de dados por não realizar operações de tratamento e nem assumir qualquer grau de responsabilidade quanto a isso. Sua importância, no entanto, é instrumental, ao ser ele tanto um ponto de contato da organização com os titulares de dados, como também por atuar como uma referência dentro de sua organização para questões referentes à proteção de dados.

A definição das responsabilidades dos agentes é muito importante para que o cidadão possa ter suas eventuais demandas satisfeitas, e para que aqueles envolvidos no tratamento de dados possam saber quais os limites das suas responsabilidades. A proposta do Anteprojeto é, basicamente, estabelecer uma cláusula geral de responsabilidade, seja por dano material, moral ou coletivo, originado do tratamento de dados pessoais. Um outro ponto fundamental é que, reconhecendo a dificuldade aliás, muitas vezes, a impossibilidade do cidadão conseguir provar a existência do tratamento abusivo de seus dados, é facilitada ao cidadão a inversão do ônus da prova. Com isto, caso verifique-se a razoabilidade da alegação do cidadão ou a dificuldade dele produzir a prova, o juiz pode determinar que a parte acusada de tratamento abusivo dos dados pessoais seja obrigada a provar que o dano não ocorreu.

Destaque: *Competências e responsabilidades relativas à gestão de base de dados nos órgãos públicos. Obrigação de definição de um encarregado.*

Questões: *O artigo 38 dispõe que as competências e responsabilidades relativas à gestão de bases de dados no órgãos e entidades públicos, bem como a responsabilidade por atos administrativos referentes a dados pessoais, serão definidas nos atos normativos que tratam da definião de competências destes órgãos. Tal tipo de responsabilidade é clara o suficiente para o cidadão? Qual seria o órgão competente para deliberar sobre a necessidade da definição de um encarregado e suas atribuições?*

Segurança e sigilo de dados pessoais

/ arts. 42 a 47

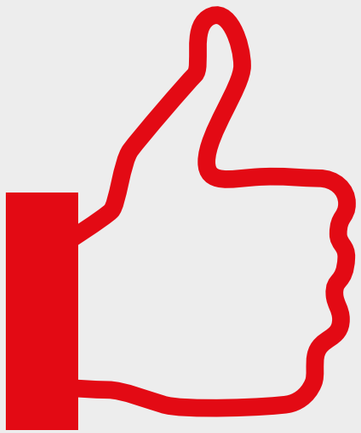
A segurança da informação procura, basicamente, disciplinar e controlar o acesso a dados e fluxo de informações e, portanto, possui ligação estreitíssima com a proteção de dados pessoais.

Segurança e privacidade não são temas dicotômicos, nem excludentes, uma vez que a garantia de um deles está diretamente relacionada com a do outro. Nesse sentido, este capítulo do Anteprojeto introduz padrões básicos de segurança e sigilo que posteriormente poderão ser tratados em normas específicas.

Nessão sessão são discutidos também os incidentes de segurança, que são conhecidos como "vazamento de dados", para os quais são propostos procedimentos que devem ser seguidos para evitá-los e mitigar seus efeitos como, por exemplo, determinar se os vazamentos devem ser tornados públicos ou não, além de incentivar os responsáveis pelo tratamento de dados a tomar medidas eficazes para que, quando houver um vazamento de dados ou outro incidente, se minimize os efeitos negativos que possam ser sentidos pelos titulares dos dados.

Destaque: *Procedimentos para o vazamento de dados pessoais*

Questões: *A lei deve estabelecer regras claras sobre segurança da informação ou deixar a definição destes parâmetros a cargo de normativas e organizações do setor? Quando ocorrer um incidente de segurança no qual dados pessoais sejam comprometidos, é necessário que todos os titulares envolvidos sejam comunicados ou, eventualmente, caso o risco para estes não seja relevante, não há tal necessidade?*



Boas práticas

/ arts. 48 e 49

As regras de boas práticas de que trata o Anteprojeto são, na verdade, uma série de regras que o responsável pelo tratamento de dados pode, voluntariamente, adotar e divulgar para possibilitar que os titulares tenham, além da proteção de dados proporcionada pela lei, um conjunto adicional de garantias a respeito de seus próprios dados. Neste sentido, as boas práticas são um compromisso que o responsável assume perante os titulares de dados pessoais.

As normas de boas práticas podem ser identificadas por diversos nomes: códigos de conduta, normas deontológicas ou outras denominações. Como tem caráter complementar em relação à legislação e normativa, somente abrangem empresas, grupos de empresas ou entidades que voluntariamente se submeterem a elas.

Sendo assim, os compromissos assumidos por uma empresa ou entidade em seus documentos de boas práticas possuem natureza contratual, no sentido em que integram o conjunto de compromissos assumidos pelo responsável ao realizar uma operação de tratamento de dados pessoais. Assim, o titular dos dados pode, justificadamente, alegar que o não cumprimento de um compromisso assumido em regras de boas práticas é uma violação das obrigações assumidas pelo responsável pelo tratamento dos dados pessoais.

O anteprojeto abre ainda a possibilidade de que as regras de boas práticas venham a ser reconhecidas e mesmo divulgadas por um órgão competente.

Na única ocasião em que o Anteprojeto refere-se especificamente ao tratamento de dados pessoais pela internet, é proposto que o órgão competente tenha a possibilidade de estimular a adoção de padrões técnicos que favoreçam o exercício dos direitos dos titulares sobre seus próprios dados pessoais.

Destaque: *A possibilidade de que o poder público incentive a adoção de padrões para aplicações na internet que impeçam o rastreamento.*

Questões: *A adoção de boas práticas por parte dos responsáveis pelo tratamento de dados pode efetivamente proporcionar maiores direitos e garantias ao cidadão?*

Autoridade competente e sanções administrativas

/ art. 50

Muitas vezes a introdução de uma nova lei pode não bastar para mudar condutas e práticas já estabelecidas. Pode ser que, para que os objetivos pretendidos pela lei sejam atingidos, seja necessário não somente estabelecer um conjunto de direitos e deveres, mas também criar instrumentos e mecanismos que garantam a sua eficácia, através de mecanismos de educação, divulgação, fiscalização, monitoramento, investigação de denúncias e outros.

A proteção de dados pessoais está diretamente ligada a processos tecnológicos extremamente dinâmicos e mutáveis. Esses processos são também, muitas vezes, difíceis de serem compreendidos e avaliados pelo cidadão, que pode nunca saber se e como seus dados pessoais são utilizados. O tratamento de dados pessoais não é visível para o cidadão, no entanto, os efeitos deste tratamento podem ser sentidos em sua vida.

Em situações como essa, pode ser necessário levar em conta a desvantagem em que o cidadão se encontra diante de quem pode tratar seus dados, e, portanto, elaborar mecanismos para que ele possa fazer valer os seus direitos.

Para isto, uma das alternativas possíveis é o estabelecimento de uma autoridade pública responsável para proteção, fiscalização e aplicação da lei de dados pessoais. Há quem defenda que um modelo sancionatório dinâmico, veloz e adequado às mudanças e inovações tecnológicas é imprescindível para que a proteção de dados pessoais se imponha como política pública em seu sentido integral, procurando modelar condutas na sociedade que visem à proteção da pessoa a partir do estabelecimento de meios legítimos para o tratamento das informações.

Destaque: *Autoridade de proteção de dados pessoais*

Questões: *É necessária a criação de um novo ente estatal para que uma legislação sobre proteção de dados seja eficaz? E, caso seja, qual seria o formato deste ente?*

Realização:

OFICINA ANTIVIGILÂNCIA

Um projeto do:

ITS Instituto de Tecnologia & Sociedade do Rio

Autoria:
Oficina Antivigilância e CSLab

Edição:
Joana Varon

Design e diagramação:
Marlena Szczepanik

Revisão:
Larissa Ribeiro

{ Mais informações via antivigilancia.org ou no Twitter @antivigilancia.

Apoio:

APC

FORDFOUNDATION
Na Linha de Frente das Mudanças Sociais

GLOBAL PARTNERS DIGITAL