PROTEÇÃO DE INFORMAÇÕES E DADOS PESSOAIS

PREFEITURA DE
SÃO PAULO
CONTROLADORIA GERAL

Índice

Apresentação

A partir da década de 1980, com a rápida expansão das redes digitais e das tecnologias da informação e comunicação, houve mudanças significativas na relação entre o indivíduo com o público e privado. Por exemplo: a maioria das pessoas tende a acreditar que nossos e-mails, telefonemas e conversas são privados e invioláveis; entretanto, o avanço da tecnologia permite também a **constante vigilância das nossas comunicações**. Nosso comportamento nas redes sociais, o que compramos, onde fomos e o que conversamos com nossos amigos, são **informações que ficam armazenadas**.

A privacidade é um direito fundamental, e esse novo contexto de comercialização de dados (principalmente pessoais) adiciona uma nova discussão sobre o tema. Isso pode ser constatado, por exemplo, nas **Diretrizes sobre Direito à Privacidade e Fluxos Transnacionais de Dados Pessoais** (1980) da OCDE; na **Diretriz 95/46/EC** da União Europeia, e na **Resolução sobre a Privacidade na Era Digital**, realizada pela ONU, em 2013. Atualmente, cerca de 109 países possuem leis de proteção de dados pessoais, e pelo menos 90 destes possuem órgãos públicos específicos para tratar do tema.

No Brasil, a principal legislação que trata da proteção de dados pessoais é o **Marco Civil da Internet**. Nele, a privacidade aparece como um dos três princípios norteadores do uso da internet, junto à neutralidade da rede e a liberdade. Outros dispositivos legais que preveem, ao menos superficialmente, a privacidade de dados pessoais são o **Art° 5 da Constituição Federal** de 1988, o **Art. 31 da Lei de Acesso à Informação** (também conhecida como "LAI") e o **Projeto de Lei n° 5276/16**, que se encontra em tramitação no Legislativo federal.

Atualmente, a Prefeitura de São Paulo recebe cerca de 1300 pedidos de acesso à informação por trimestre. Naturalmente, dentre os vários conjuntos de dados produzidos e custodiados pela Prefeitura de São Paulo - incluindo suas parceiras e contratadas -, estão dados pessoais de indivíduos que submeteram suas informações para uso de algum serviço público.

É fundamental, portanto, que servidores e cidadãos conheçam a importância do tema da privacidade e fomentem uma gestão adequada das informações pessoais, sem implicar retrocessos nas atuais políticas de transparência do município. Nesta cartilha, o leitor encontrará algumas diretrizes para refletir sobre uma **política de proteção de dados pessoais** para o setor público e também para o setor privado.

A privacidade possui uma importante dimensão econômica: nosso comportamento, as informações pessoais coletadas de perfis de redes sociais, aplicativos e outros dispositivos personalizáveis, tornaram-se objetos de venda entre grandes corporações. Assim, a questão da proteção de dados atrai o interesse de empresas de diferentes segmentos da economia, além de ter dimensões políticas que envolvem

distintos setores da burocracia e dos poderes do Estado (Polícias, Ministério Público, Judiciário etc), bem como grupos da sociedade civil.

A questão da privacidade não envolve apenas concepções morais ou visões ideológicas. A exposição dessas informações pode gerar constrangimento, submissão, discriminação, entre outros fatores negativos.

Muitas vezes, pessoas são perseguidas por suas convicções, sua religião, sua orientação sexual ou simplesmente por suas opiniões. Quando a privacidade é violada, ideias são bloqueadas e direitos humanos são desrespeitados.

Informações e dados pessoais: o que são?

Você já parou para pensar no conjunto de características que faz com que o governo, empresas e organizações saibam quem você é? Não estamos falando apenas de características físicas, mas principalmente daquelas que se referem ao seu comportamento, ao seu cotidiano, à sua condição social e às suas escolhas.

Informações pessoais são aquelas relacionadas à pessoa natural identificada ou identificável. Ou seja: informações que podem revelar aspectos sobre a sua intimidade, sua vida privada e sua imagem, e permitam **identificar quem você é**.

Neste sentido, informações pessoais podem ser números identificativos, dados locacionais, identificadores eletrônicos, ou ainda informações mais subjetivas e mais sensíveis, que podem estigmatizar pessoas. Desta maneira, podem ser consideradas informações pessoais: o número do seu RG, seu endereço, senhas, o número do seu Bilhete Único, bem como religião, raça, etnia, condições de saúde, orientação sexual, ideologia e muitos outros que possam gerar exposições e constrangimentos.

Mas atenção! No caso do setor público, há uma exceção importante na definição

de informações pessoais. **Informações que dizem respeito ao trabalho de servidores públicos não são consideradas informações pessoais passíveis de proteção** nos mesmos termos citados anteriormente. Como essas informações dizem respeito ao exercício da função pública e à aplicação de recursos públicos, segundo o artigo 8° da LAI, elas são consideradas informações públicas. O endereço do local de trabalho, o horário do expediente, as informações de contato e até os valores de remuneração dos agentes públicos podem ser disponibilizados ativamente pelos órgãos públicos, ou podem ser solicitados via pedido de acesso à informação.

Muitas vezes as informações pessoais são referências a um indivíduo em um contexto. Nesses casos, informações pontuais podem representar um baixo potencial para identificar alguém, mas quando combinadas com outros conjuntos de dados, é possível reconhecer a(s) pessoa(s) que atende(m) àquele perfil. Este é um ponto de especial atenção para os servidores públicos que lidam diretamente com pedidos de acesso à informação.

Imagine que alguém deseja descobrir quantos loteamentos irregulares existem em São Paulo e onde aparecem com mais frequência. Suponhamos que o atendente do pedido tenha essas informações organizadas por CEP e por distrito. Neste caso, disponibilizando a informação segregada por CEP, o servidor pode expor pessoas em situação de vulnerabilidade social, o que pode constrangê-las de diversas formas. Nesta situação, a melhor opção seria disponibilizar o dado desagregado por distrito.

Quem os possui?

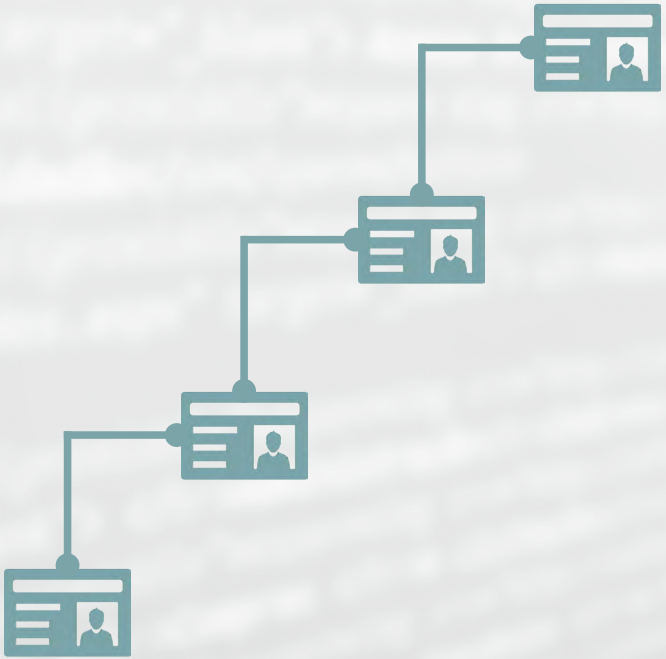
Empresas, organizações sociais e entidades públicas coletam informações pessoais o tempo todo para os mais diferentes fins. No caso das empresas, essas informações normalmente servem para conhecer seus clientes, para identificar novos perfis interessados no que elas têm para oferecer e para negociar com outras empresas. Já para a Administração Pública, é importante ter informações sobre as pessoas para **conhecer seus cidadãos e elaborar melhores políticas públicas**.

Todas as vezes em que há a utilização de algum tipo de serviço, por exemplo, você concorda em ceder algumas informações a seu respeito para quem fornece aquele serviço. Onde estuda, quais meios de transporte utiliza, a qual hospital vai quando fica doente são exemplos de serviços que utilizam suas informações.

Via de regra, é comum o uso de termos de ciência, termos de serviço ou políticas de privacidade quando há a cessão de informações pessoais. Esses documentos

funcionam como **contratos entre você e a instituição que armazenará suas informações pessoais**. Sempre procure saber como seus dados podem ser utilizados, por quem e para quais finalidades. Desta maneira, é possível evitar consentir com usos de suas informações que você não aprova.

No caso das informações custodiadas pelo Estado, se não estiver evidente para você como ocorre a gestão das suas informações pessoais, **recorra à LAI e realize um pedido de acesso à informação**, solicitando esclarecimentos sobre a coleta de dados de alguma política específica.



Casos em que podem ser publicados

Informações públicas são todas aquelas coletadas, produzidas, administradas ou simplesmente custodiadas pelos órgãos públicos. Neste sentido, muitas informações pessoais são, sim, informações públicas, **mas isso não significa que elas serão indiscriminadamente disponibilizadas**.

A Lei de Acesso à Informação (Lei Federal nº 12.527/11) define, por meio de seu artigo 31, um conjunto de regras sobre o acesso à informações pessoais em posse do poder público. Segundo a LAI, a manipulação desse tipo de informação é restrita aos agentes públicos por pelo menos 100 anos a contar de sua data de produção - exceto quando houver consentimento expresso da pessoa em questão ou previsão legal. O uso inadequado dessas informações é passível de responsabilização, segundo a lei.

O acesso de terceiros às informações pessoais somente é autorizado mediante justificativa prevista na LAI. As razões aceitáveis são: realização de pesquisa científica de interesse público; o tratamento de saúde de pessoas física ou legalmente incapazes; cumprimento de ordem judicial; defesa de direitos humanos ou proteção do interesse público.

Um bom mecanismo que a Administração Pública pode utilizar para assegurar, ao mesmo tempo, a privacidade dos cidadãos e o direito à informação pública, nos termos da lei, é **empregar procedimentos de anonimização**. A prática consiste na análise de um determinado conjunto de informações, e na supressão de dados específicos que podem identificar indivíduos com maior facilidade, como nomes, endereços, números de RG e CPF etc.

Como podem ser protegidos?

Do ponto de vista de ferramentas tecnológicas, a **criptografia** é uma das formas mais seguras de proteger seus dados. Trata-se de uma técnica que transforma um conteúdo em códigos que só podem ser compreendidos por destinatários específicos.

A criptografia pode ser utilizada para vários fins e por qualquer pessoa, inclusive leigos. Atualmente, existem diversos aplicativos que podem te ajudar a aplicar criptografia em determinadas funções do seu celular, como apps de mensagens instantâneas.

Técnicas de criptografia podem ser aplicadas aos conjuntos de informações gerados em um programa de computador. Deste modo, esses dados ganham uma camada extra de proteção contra invasões. Quanto mais complexo o processo de codificação, mais protegida é a informação e menor a probabilidade de utilizarem seus dados pessoais sem seu consentimento.

Outro método para fortalecer a segurança das informações pessoais é estabelecer procedimentos de identificação dos agentes públicos com acesso a esses dados e manter os registros de acesso.
É importante que esses registros sejam atualizados constantemente, evitando, por exemplo, que ex-servidores mantenham acesso a essas informações sensíveis.

Este mecanismo pode ser empregado tanto na gestão de informações em formato físico, quanto nos digitais. Em algumas plataformas de gerenciamento digitais, é possível ainda desenvolver cadastros individuais e registros de atividade, que permitem acompanhar como exatamente o servidor utilizou os dados.

O que fazer em caso de exposição indevida?

No caso da Administração Pública, devido ao volume de informações, é ainda mais importante que os cidadãos conheçam essas leis e técnicas de proteção de dados, e cobrem de seus governantes métodos de gerenciamento da informação mais seguros.
Caso a Prefeitura de São Paulo exponha dados pessoais injustificadamente, o indivíduo que se sentir afetado pode **encaminhar uma denúncia por meio do formulário disponibilizado pela Controladoria Geral do Município**, ou, dependendo da gravidade, acionar outras instâncias da justiça e buscar indenização por danos morais.

Controladoria Geral do Município

Formulário de denúncia:

http://www.prefeitura.sp.gov.br/cgm/formdenuncia/

PREFEITURA DE
SÃO PAULO
CONTROLADORIA GERAL