ARTIGO · JOTA_IMPORT

Proteção de dados na Administração Pública

Autor(a): Mateus Piva Adami
Publicado em: 14 de maio de 2018
Publicação: jota_import
Link JurisTube:
https://juristube.com.br/colunistas/mateus-piva-adami/protecao-de-dados-na-administracao-publica
Fonte original: https://www.jota.info/opiniao-e-analise/artigos/dados-administracao-publica
Identificador citável:
juristube.com.br/colunistas/mateus-piva-adami/protecao-de-dados-na-administracao-publica#ep-4dc19aae

Resumo

Podem dados de mobilidade de indivíduo ser utilizados para fins de segurança pública? É necessária ordem judicial?

Texto integral

Em continuidade à série sobre direito e Internet das Coisas (IoT) que nosso escritório Pereira Neto, Macedo está produzindo para o JOTA , abordaremos nessa semana a proteção de dados em soluções de Internet das Coisas quando aplicadas pelo poder público, como, por exemplo, o uso de dispositivos em cidades inteligentes. Esta série de artigos é parte do Estudo para o Plano Nacional de IoT que nosso escritório elaborou junto com a McKinsey e com o CPqD, comissionado pelo BNDES e MCTIC. Boa parte dos desafios para a proteção de dados em ambientes públicos passam pela necessidade de edição de uma lei de proteção de dados pessoais que estipule critérios e obrigações ao Poder Público, como se verá abaixo. +JOTA: Faça o cadastro e leia até dez conteúdos de graça por mês! Proteção de dados e a Administração Pública A crescente utilização de dispositivos tecnológicos dispersos pelo espaço urbano, capazes de coletar dados sobre os cidadãos, monitorar suas atividades e até mesmo identificá-los, traz à tona diversas questões referentes à proteção da privacidade de indivíduos. Os riscos abrangem questões como vigilância em massa e acesso e compartilhamento não autorizado de informações pessoais. É o caso de dispositivos como sensores capazes de obter informações sobre tráfego, umidade do ar, índice de poluição, volume de ruídos, temperatura, pressão atmosférica, radiação, dentre outros. Nesses casos, como não se trata de dados pessoais, o administrador público não estaria sujeito às obrigações legais de proteção de dados. A preocupação é mais pungente quando o Poder Público coleta informações que identificam ou sejam potencialmente capazes de identificar um indivíduo (o que se define como “dados pessoais”). Nessas hipóteses, vale notar os modelos normativos mais novos sobre proteção de dados não fazem distinção quanto a dados coletados pelo poder público ou pelo setor privado. Esse é o caso, por exemplo, da GDPR, aplicável na Europa. No Brasil, esse também é o caso. O Marco Civil da Internet (Lei nº 12.965/2014) e seu Decreto nº 8.771/2016 não diferenciam dados privados coletados online pelo setor público ou pelo setor privado. Em nosso estudo de IoT, propomos como modelo para tratar dessa questão que o Poder Público não precisa do consentimento para coletar dados pessoais dos usuários, desde que esses dados sejam coletados para fins específicos de propiciar a administração de serviços públicos, especialmente serviços essenciais. A razão é que esses dados, na medida em que avança a tecnologia, são

inerentes à prestação e melhoria dos serviços. +JOTA: O Direito da Internet das Coisas – desafios e perspectivas de IoT no Brasil +JOTA: Neutralidade da rede e Internet das Coisas no Brasil: uma relação harmônica No entanto, apesar do consentimento não ser obrigatório, a coleta desses dados deve ser feita estritamente para prestação e melhoria daquele serviço especificamente. Outros usos e outras finalidades estão vedados, exceto se houver consentimento. Nesse sentido, os dados não podem ser cedidos para entidades privadas, nem podem ser enviados para outros órgãos públicos que prestam outros serviços diferentes daquele para os quais os dados foram coletados. A exceção a essa regra só seria admissível em casos de ordem judicial. Serviços de segurança pública são um bom exemplo para o qual o consentimento prévio comprometeria a efetividade do serviço. Nesse caso, a coleta será feita sem consentimento, mas o uso deverá se ater à finalidade específica para a qual foi obtido. 1 Mais do que isso, a coleta de quaisquer dados pelo Poder Público deve atender aos princípios da necessidade e da proporcionalidade. Não devem ser coletados mais dados do que o necessário e a coleta deve ser absolutamente necessária. Obviamente, os dados coletados para fins de segurança pública não poderão ser usados para qualquer outra finalidade, nem cedidos para quaisquer outros órgãos governamentais com finalidades distintas. A exceção, mais uma vez, é a ordem judicial. Um caso recente do metrô paulistano é ilustrativo, tendo sido abordado por outro artigo desta mesma série. A concessionária da Linha-4 Amarela instalou em abril um mecanismo de reconhecimento facial em “portas interativas”, com o fim imediato de contar o número e otimizar o fluxo de passageiros. 2 Também planeja utilizar as informações obtidas para oferecer anúncios personalizados. Se a primeira parte é legítima, para a segunda parte que prevê anúncios baseados nesses dados, há violação clara dos princípios da necessidade e proporcionalidade. Mais do que isso, há violação clara do princípio da finalidade, que se desviaria da estrita administração do serviço. Seria assim necessário obter o consentimento livre, prévio, expresso e informado dos usuários para essa atividade. +JOTA: Qual o conceito de M2M e por que isso importa para o desenvolvimento de IoT? +JOTA: A necessidade de investimentos na infraestrutura de telecomunicações Mais do que isso, o Poder Público não está isento da obrigação de elaborar políticas de privacidade. Toda cidade, Estado e o próprio governo federal deveria ter uma política de privacidade pública para os dados que coletam. Essa obrigação decorre do princípio da transparência na administração pública e do princípio da estrita legalidade. Há casos, também, em que um sensor ou dispositivo poderia obter dados pessoais, mas o regime de proteção de dados é afastado, uma vez que as informações coletadas são “anonimizadas”, ou seja, qualquer indicativo da titularidade é mascarado definitivamente por técnicas de criptografia. Essa anonimização deve ser obrigatoriamente de alto nível, impedindo a reversão ou reidentificação dos usuários. Em razão dos desafios e riscos possíveis, é essencial que o Poder Público crie soluções tecnológicas que protejam a privacidade a partir do próprio desenho da solução. Trata-se da chamada “privacidade por desenho” (ou “ privacy by design ”). E, nesse contexto, a saída mais protetiva envolve a conjugação de todas essas práticas e princípios: finalidade, proporcionalidade, necessidade, anonimização 3 , consentimento e aplicação de técnicas de privacidade diferencial 4 , dentre outras. Por um lado, fomenta-se uma nova geração de serviços públicos eficientes, sem no entanto eliminar as garantias fundamentais à privacidade. +JOTA: Principais desafios tributários do ambiente de Internet das Coisas +JOTA: Segurança da informação e IoT no Brasil: prioridades, modelos e alternativas Cruzamento de dados no âmbito da Administração Pública Outro aspecto central no debate são os questionamentos sobre as possibilidades de compartilhamento de bancos de dados pessoais entre órgãos e autoridades no âmbito da Administração Pública. Podem os dados de mobilidade de um indivíduo ser utilizados para fins de segurança pública, sendo compartilhados com a polícia? É

necessária uma ordem judicial para esse compartilhamento? Ou ainda, podem os dados dos cidadãos obtidos a partir de espaços urbanos serem utilizados para fins como fiscalização e customização de cobranças? Seria necessária ordem judicial prévia para esse fim? Uma hipótese para resolver essa questão é que o cruzamento deve ser necessariamente e expressamente previsto em lei, como é o caso das hipóteses previstas na Lei de Lavagem de Dinheiro, Lei de Combate às Organizações Criminosas e Lei de Acesso à Informação. Mesmo como previsto em lei, essa autorização de ser limitada às finalidades para as quais a coleta está prevista. Leis que suprimam totalmente o consentimento ou o tornem inútil seriam inconstitucionais. O corolário da proteção da privacidade na Constituição Federal é justamente de tornar a privacidade um direito fundamental inalienável. A lei não tem o condão de suprimir esse direito ou torna-lo inútil. A administração pública está assim sujeita a balizas legais e constitucionais que delimitam como pode ocorrer a coleta e o compartilhamento de dados pessoais. +JOTA: O Brasil precisa de uma autoridade de proteção de dados? +JOTA: Internet das coisas e mobilidade urbana: Desafios regulatórios na modernização da gestão de trânsito Cautelas na relação entre o Poder Público e a iniciativa privada Outra dificuldade é a relação entre o administrador público e a iniciativa privada. Para viabilizar um serviço, pode ser necessário estabelecer fluxo de dados entre o Administrador e o parceiro envolvido. É o caso do projeto SmartSantander , focado em incentivar turismo e lazer no município de Santander, Espanha. A coleta de dados por sensores distribuídos no município e o cruzamento das informações entre a Prefeitura e a iniciativa privada permitem identificar pontos turísticos de interesse e customizar ofertas de entretenimento, de acordo com o perfil do cidadão. Esse relacionamento implica cautela. Primeiro , antes de receber os dados pessoais coletados por um parceiro, o administrador público deve verificar se houve consentimento adequado do titular (a despeito de serviços públicos essenciais, como abordado acima) ou se os dados foram anonimizados de forma definitiva e segura. Uma medida positiva nesse sentido seria definir critérios na contratação pública desses parceiros, tais como: (1) o respeito a medidas mínimas técnicas e gerenciais de segurança, (2) a criação de ferramentas para que o usuário manifeste sua vontade sobre a coleta de dados (opt-in) ou o término do tratamento (opt-out) ou, ainda, (3) a divulgação de política de privacidade ao público. Segundo , a transferência de dados pessoais do Poder Público ao ente privado deve ser restrita aos casos em que haja previsão legal expressa para tanto, bem como a obtenção de consentimento livre e informado dos cidadãos ou, alternativamente, caso haja autorização por ordem judicial. Com a proliferação de dispositivos “inteligentes” para facilitar atividades do dia-a-dia, muitas vezes desprovidos de medidas de segurança, o descuido pode significar o acesso não autorizado ou o vazamento de dados de cidadãos. O caso da identidade biométrica digital Aadhaar , na Índia, é ilustrativo. Nascido de parceria entre empresa de grande porte e o governo indiano, o programa cadastrou 1,2 bilhão de cidadãos para permitir o acesso a serviços públicos. Se a iniciativa representou um avanço enorme na melhoria dos serviços públicos, sua arquitetura apresentou falhas com relação a segurança dos dados. 5 A centralização dos serviços públicos, que é desejável, deve ser conjugada com a descentralização dos bancos de dados e com medidas de proteção à privacidade cada vez maiores. É o que o governo indiano está fazendo neste momento, ao aperfeiçoar a arquitetura do sistema. +JOTA: Internet das coisas e segurança pública +JOTA: Internet das coisas e infraestrutura: desafios regulatórios na implementação de redes elétricas inteligentes Contornos de uma lei de proteção de dados Para que o planejamento público das cidades inteligentes seja uma realidade bem-sucedida, é imprescindível que a privacidade dos cidadãos seja encarada como prioridade. Não há cidades inteligentes, Internet das Coisas no setor público ou mesmo o emprego de aplicações de inteligência artificial sem uma lei geral de proteção

de dados. Seria irresponsável avançar nessa área sem ter primeiro construído o alicerce para todos esses tipos de aplicação. A legislação sobre proteção de dados deve implementar uma série de garantias aos cidadãos. Entre elas, deve constar o consentimento, o princípio de legítimo interesse que é capaz de mitiga-lo quando necessário, o princípio da finalidade, da transparência, além do princípio da necessidade e proporcionalidade. É preciso, também, aplicar o regime de proteção dados de forma “integral” à Administração Pública, sem distinções irrealistas. A Constituição não distinguiu a proteção de dados no setor privado ou no setor público. Não cabe à lei fazer essa distinção. Isso envolve limitar o uso de dados pela Administração Pública às finalidades específicas inerentes à prestação do serviço em questão, de forma em que o uso para finalidades distintas daquelas informadas dependeria de ordem judicial ou de autorização legal específica, respeitados os limites constitucionais. Qualquer movimentação contrária por parte do legislador brasileiro teria o impacto de distanciar o país ainda mais dos modelos mais recentes de proteção à privacidade. Isso isolaria o país, dificultando a troca de dados internacionais e colocando o país na contramão das melhores práticas internacionais. 6 ---------- 1 ■ Como exemplo, o Poder Público pode coletar dados pessoais necessários para a gestão de um sistema de bilhetagem eletrônica (como o “Bilhete Único” da cidade de São Paulo) no âmbito do transporte público municipal. Como esses dados são essenciais para a prestação do serviço, o consentimento ficaria dispensado. No entanto, os dados devem ser usados apenas para a finalidade específica de gestão do serviço. 2 ■ Conforme divulgação pela concessionária ViaQuatro. Disponível em https://goo.gl/KzELcP . Destacamos que não localizamos ou tivemos acesso aos termos da política de privacidade adotada pela companhia. 3 ■ A anonimização é a forma mais rígida de proteção de dados pessoais. Através de “chave” criptográfica, os dados são anonimizados, e, por consequência, podem perder sua característica de “dados pessoais” e, desse modo, ser processados, armazenados e compartilhados sem risco de identificação de seus titulares. O objetivo imediato é, portanto, assegurar que os dados armazenados não permitam a identificação dos cidadãos, escondendo de forma permanente informações que os individualizem. Ainda, o uso de criptografia para a codificação de dados evitaria que atores mal-intencionados tenham acesso a informações coletadas por meio de soluções IoT, de forma a resguardar a identidade do titular de dados. 4 ■ A técnica de privacidade diferencial permite que o responsável pelo tratamento e armazenamento dos dados seja capaz de disponibilizar, de forma anonimizada, estatísticas e consultas a partir da base de dados original, que, contudo, permanece inalterada. 5 ■ Chinmayi Arun, ‘Privacy is a fundamental right’, 2018, disponível em http://www.thehindu.com/opinion/lead/lead-article-on-aadhaar-bill-by-chinmayi-arun-privacy-is-a-fundamental-right/article8366413.ece . 6 ■ Veja, nesse sentido, o Regulamento Geral sobre Proteção de Dados da União Europeia.

Como citar este documento

As citações abaixo seguem os padrões ABNT NBR 6023:2018, APA 7ª edição, Chicago Author-Date (17ª ed.) e BibTeX (LaTeX). Copie o formato exigido pelo periódico ou gerenciador bibliográfico (Zotero, Mendeley, EndNote).

ABNT (NBR 6023:2018)

ADAMI, Mateus Piva. Proteção de dados na Administração Pública. jota_import, 14 maio 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/dados-administracao-publica. Acesso via: JurisTube — Acervo Digital de Direito. Disponível em: https://juristube.com.br/colunistas/mateus-piva-adami/protecao-de-dados-na-administracao-publica. Acesso em: 20 ago. 2026.

APA 7ª edição

Adami, M. P. (2018, May 14). Proteção de dados na Administração Pública. *jota_import*. https://www.jota.info/opiniao-e-analise/artigos/dados-administracao-publica

Chicago Author-Date (17ª ed.)

ADAMI, Mateus Piva. 2018. “Proteção de dados na Administração Pública.” *jota_import*, May 14. https://www.jota.info/opiniao-e-analise/artigos/dados-administracao-publica

BibTeX

```
@article{mateus-piva-adami-prote-o-de-dados-na-administra-o-p-blica-2018,
author = {Adami, Mateus Piva},
title = {Proteção de dados na Administração Pública},
journal = {jota_import},
year = {2018},
url = {https://www.jota.info/opiniao-e-analise/artigos/dados-administracao-publica},
urldate = {2018-05-14}
}
```


JurisTube — Acervo Digital de Direito
https://juristube.com.br/colunistas/mateus-piva-adami/protecao-de-dados-na-administracao-publica
PDF gerado em 2026-08-20 19:06 UTC