

Internet das coisas e segurança pública

Autor(a): Mateus Piva Adami

Publicado em: 17 de abril de 2018

Publicação: jota_import

Link JurisTube: <https://juristube.com.br/colunistas/mateus-piva-adami/internet-das-coisas-e-seguranca-publica>

Fonte original: <https://www.jota.info/opiniao-e-analise/artigos/internet-das-coisas-e-seguranca-publica>

Identificador citável:

juristube.com.br/colunistas/mateus-piva-adami/internet-das-coisas-e-seguranca-publica#ep-081de4f6

Resumo

Modernização tecnológica com garantia de direitos fundamentais

Texto integral

Na sequência da série de publicações sobre Internet das Coisas (“Internet of Things” ou “IoT”), fruto da parceria entre o Pereira Neto | Macedo Advogados e o JOTA , continuaremos a tratar de alguns setores que poderão se beneficiar da implementação de soluções de IoT. 1 Estes artigos têm por objetivo divulgar as conclusões do estudo que deverá embasar o Plano Nacional de Internet das Coisas, realizado por nosso escritório, em conjunto com a McKinsey e o CPqD, e comissionado pelo BNDES e MCTIC. Como observamos em publicações anteriores , a tecnologia exerce papel relevante na oferta de melhores serviços às pessoas que residem nas áreas urbanas e isso não é diferente em relação ao sistema de segurança pública. A modernização progressiva dos mecanismos de segurança urbana já pode ser observada em diversas cidades ao redor do país. Uma delas é Águas de São Pedro , no Estado de São Paulo, que é destaque em inovação no ambiente urbano, uma vez que conta com um complexo de câmeras de alta resolução para garantir a segurança de seus cidadãos no trânsito. +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 Outra referência é a cidade de Xerém, localizada no Rio de Janeiro, na qual foi instalada o Ambiente de Demonstração de Tecnologias para Cidades Inteligentes , iniciativa que reúne esforços da Agência Brasileira de Desenvolvimento Industrial – ABDI e do INMETRO. Por meio desse projeto, novos produtos e soluções serão avaliados e qualificados quanto, entre outros aspectos, à sua interoperabilidade, desempenho e segurança. Em linhas gerais, o aprimoramento do sistema de segurança pública perpassa pela adição, àqueles tradicionais circuitos de CCTV, de equipamentos audiovisuais e microfones de alta definição e sensibilidade, de novas câmeras com tecnologia OCR (que conseguem reconhecer caracteres de placas de veículos, por exemplo) e tecnologia de reconhecimento facial, além de sensores dos mais variados tipos. +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 Segurança pública e privacidade . As entidades públicas brasileiras encontram-se autorizadas pela Constituição Federal a implementarem tecnologias IoT em mecanismos de segurança. Da mesma forma que a instalação de câmeras de segurança em vias públicas é prática corrente pelos órgãos públicos, novas ações de monitoramento se encontram igualmente respaldadas pelo art. 144 do texto constitucional, 2 segundo o qual o Estado deve garantir segurança aos cidadãos através da execução de políticas públicas eficientes.

Entretanto, o uso dessas novas tecnologias acaba por gerar situações que testam as fronteiras entre dois deveres constitucionais do Estado: o de garantir a segurança da população e o de assegurar seus direitos fundamentais – em especial o direito à privacidade. E não são poucas as circunstâncias recentemente divulgadas na mídia que demonstram certa intrusão na intimidade das pessoas e que poderiam, inclusive, desestimular os cidadãos a participarem da vida pública – em verdadeiro chilling effect (“efeito inibidor”). 3 Na última semana, por exemplo, um cidadão chinês foi preso após ter sido reconhecido entre mais de 60 mil pessoas na plateia de um show na cidade de Nanchang, na China. Tudo isto porque a organização do evento se utilizou de sistema preciso de reconhecimento facial para vigiar o ambiente. Em um contexto no qual os indivíduos podem ser reduzidos a números e características rastreáveis (como já alertou o Comissário de Segurança no Reino Unido em diferentes oportunidades), é necessário refletir sobre como permitir que o aperfeiçoamento dos sistemas de segurança pública ocorra sem que o Estado abuse de suas prerrogativas e coloque em xeque os direitos fundamentais de seus cidadãos. Ainda que o poder de polícia represente uma faculdade da qual dispõe a Administração Pública para condicionar ou restringir direitos individuais, as medidas não devem ser utilizadas para além do estritamente necessário e proporcional para a consecução das finalidades visadas – isto é, a garantia da segurança aos cidadãos sem que o direito à privacidade e intimidade seja indevidamente restringido. É por este motivo que as entidades públicas deve agir com cautela ao colocar em prática medidas como as plataformas interativas com reconhecimento facial, anunciadas recentemente pela concessionária da Linha 4 – Amarela do metrô de São Paulo. Ao aplicar de forma concreta as noções de necessidade e proporcionalidade, o Poder Público fica, por exemplo, vedado a fazer uso dos dados coletados por equipamentos de segurança para finalidades outras que não aquelas que justificarem sua coleta e esta não pode, de maneira alguma, ser feita de forma arbitrária ou genérica. +JOTA: Principais desafios tributários do ambiente de Internet das Coisas +JOTA: Segurança da informação e IoT no Brasil: prioridades, modelos e alternativas Ademais, os dados deverão ser armazenados sob medidas adequadas de segurança e aqueles não utilizados (ou encerrada a finalidade para a qual foram coletados) deverão ser descartados. Deve ser também proibido o acesso dos dados por terceiros ou a cessão dos dados para outras entidades. Ainda, no tratamento desses dados, não poderá haver qualquer possibilidade de discriminação com base em raça ou outras características socioeconômicas. Especificamente em relação à questão do consentimento no tratamento de dados, a regra geral da legislação brasileira, aplicável tanto a entes privados quanto públicos, é a necessidade de obtenção do consentimento prévio, expresso e informado dos indivíduos para o tratamento de seus dados pessoais. Entendemos, porém, que não será necessária a obtenção de consentimento pelo Poder Público – ou, alternativamente, autorização judicial –, caso os dados pessoais coletados pelos equipamentos de segurança sejam tratados de forma estritamente necessária e proporcional à finalidade a que se destinam (a garantia do serviço público de segurança), bem como esse tratamento seja realizado apenas por autoridades que componham o sistema de segurança pública. O Uruguai, por exemplo, permite o tratamento de dados pessoais pela Administração sem a obtenção prévia de consentimento quando o processamento for necessário para a prestação de “funções de Estado”. Na União Europeia, por sua vez, a General Data Protection Regulation – GDPR, que entra em vigor neste maio, estabelece que entidades públicas podem tratar dados pessoais coletados sem consentimento caso o processamento seja necessário, de acordo com o interesse público ou no exercício das atribuições da autoridade pública. +JOTA: O Brasil precisa de uma autoridade de proteção de dados? Efetividade dos sistemas de segurança. Além disso, o Poder Público deve estar atento às falhas na execução desses sistemas tecnológicos de monitoramento, uma vez que a

existência de irregularidades pode gerar questionamentos sobre a real necessidade de sua implementação. O sistema paulista “Detecta”, voltado à identificação de veículos e atividades suspeitas (como furtos e roubos) por meio de câmeras de monitoramento e câmeras com tecnologia OCR, já teve sua eficiência contestada pelo Tribunal de Contas do Estado de São Paulo . Entre outros aspectos, o Tribunal de Contas discutiu as capacidades do sistema de reduzir a quantidade de pessoal envolvido no monitoramento e de garantir a confiabilidade e a segurança das informações. De modo geral, a decisão entendeu que havia: (a) falhas de planejamento na contratação do serviço; (b) o serviço era pouco utilizado pelas unidades policiais; (c) e existem imperfeições nas medidas de segurança da informação. Nos Estados Unidos, falhas nas técnicas de identificação facial também trouxeram à tona questionamentos sobre a efetividade da tecnologia IoT. O sistema de reconhecimento facial da cidade de Boston não foi capaz de identificar suspeitos em atentado ocorrido em 2013. Imagens de dois possíveis culpados encontravam-se disponíveis em banco de dados públicos, mas os dispositivos não foram capazes de detectá-los . Esses exemplos demonstram, por um lado, a necessidade de estudo prévio e treinamento dos agentes públicos quanto ao uso da solução tecnológica, e, por outro, que a tecnologia não pode ser vista como única solução para o problema da segurança pública, mas como um auxiliar cada vez mais importante – principalmente com seu avanço.

+JOTA: Internet das coisas e mobilidade urbana: Desafios regulatórios na modernização da gestão de trânsito Como garantir o respeito aos direitos fundamentais e a efetividade? As noções de necessidade e proporcionalidade vem sendo incorporadas nos textos legislativos e documentos de intenções que tratam da modernização da segurança pública. Um modelo a ser seguido pelas autoridades brasileiras pode ser o sistema de freios e contrapesos proposto pelo Fórum Europeu para a Segurança Urbana (EFUS) na Carta de Uso Democrático da Videovigilância . Nesse texto são apresentados princípios gerais para a concepção e funcionamento de sistemas de segurança pública por vídeo, entre eles, os de legalidade, necessidade e proporcionalidade. A Carta sugere que o emprego de soluções tecnológicas de vigilância deve respeitar as leis locais e os tratados internacionais que tratem da proteção da privacidade, do monitoramento das comunicações e do uso de dados pessoais. Ainda, sugere que a decisão pública sobre a instalação desses dispositivos deve ser estritamente baseada na necessidade. O termo “necessidade” é identificado no documento como o balanço adequado entre, de um lado, circunstâncias e urgência, e, de outro, o tipo de resposta – no caso, o uso de equipamentos de segurança pública de vídeo. Com o objetivo de também garantir equilíbrio entre segurança pública e direitos individuais, foi recentemente publicada na União Europeia a Diretiva 2016/680 , que estabelece preceitos gerais para o tratamento de dados pessoais pelas autoridades competentes na prevenção, investigação, detecção ou repressão de infrações penais. É imprescindível que essa agenda também avance no Brasil, para que sejam criadas balizas e diretrizes no tratamento de dados pessoais, especialmente aquele realizado por órgãos nacionais de segurança pública – os quais não devem ser excepcionados, sob pena da legitimação de abusos pelo poder público. Não por outro motivo que a aprovação de lei específica acerca da proteção de dados pessoais e a criação ou designação de uma autoridade de proteção de dados pessoais são medidas imprescindíveis para o país . Para além dessa essencial iniciativa legislativa, é interessante que haja a ampliação do arcabouço de boas práticas por parte do Poder Público . Dentre as iniciativas possíveis está a adoção de documento de avaliação do impacto na proteção de dados (ou Data Protection Impact Assessment – DPIA), a fim de identificar problemas de privacidade e decidir quais procedimentos seguir para garantir que os riscos sejam gerenciados. Outra possibilidade é a concepção de um código de conduta que estabeleça diretrizes sobre como os órgãos de segurança

pública devem implementar e operar os atuais e futuros sistemas de monitoramento por câmeras e sensores. É o caso do Código de Conduta em Monitoramento por Câmeras que entrou em vigor no Reino Unido em 2013, com o objetivo de ditar as práticas da polícia e autoridades locais no que diz respeito ao uso de câmeras e dispositivos OCR. O município de Perth, na Austrália, também possui um Código de Conduta sobre as Operações de CCTV , com regras para a operação de mecanismos de vídeo nos espaços públicos da cidade. Esse código pode descrever, entre outros assuntos: (a) quais são as melhores práticas em monitoramento e vigilância; (b) os parâmetros para o tempo de guarda de dados em cada hipótese de monitoramento (em algumas hipóteses pode não ser necessário nem mesmo reter dados, como no caso de sensores de captação de áudio em logradouros públicos); e (c) políticas de compartilhamento de dados entre os órgãos de segurança pública, que não permita o compartilhamento para além das finalidades de segurança. No próximo artigo da série, seguiremos tratando de obstáculos e potencialidades decorrentes da implementação de dispositivos de IoT para a prestação de serviços públicos. Até lá! ----- 1 ■ Os setores priorizados pelo Estudo de Internet das Coisas foram Cidades Inteligentes, Rural e Saúde. 2 ■ Constituição Federal, art. 144, caput . A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos (...). 3 ■ KLITOU, Demetrius. Privacy-invading technologies and privacy by design : Safeguarding privacy, liberty and security in the 21st century. The Hague: Asser Press, 2014, p. 119.

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. Internet das coisas e segurança pública. *jota_import*, 17 abr. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/internet-das-coisas-e-seguranca-publica>. Acesso via: JurisTube — Acervo Digital de Direito. Disponível em: <https://juristube.com.br/colunistas/mateus-piva-adami/internet-das-coisas-e-seguranca-publica>. Acesso em: 20 ago. 2026.

APA 7ª edição

Adami, M. P. (2018, April 17). Internet das coisas e segurança pública. **jota_import**. <https://www.jota.info/opiniao-e-analise/artigos/internet-das-coisas-e-seguranca-publica>

Chicago Author-Date (17ª ed.)

ADAMI, Mateus Piva. 2018. "Internet das coisas e segurança pública." **jota_import**, April 17. <https://www.jota.info/opiniao-e-analise/artigos/internet-das-coisas-e-seguranca-publica>

BibTeX

```
@article{mateus-piva-adami-internet-das-coisas-e-seguran-a-p-blica-2018,  
author = {Adami, Mateus Piva},  
title = {Internet das coisas e segurança pública},  
journal = {jota_import},  
year = {2018},  
url =  
{https://www.jota.info/opiniao-e-analise/artigos/internet-das-coisas-e-seguranca-publica},  
urldate = {2018-04-17}  
}
```



Licença de Uso — CC BY-NC-SA 4.0

Este conteúdo está licenciado sob a licença Creative Commons Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional (CC BY-NC-SA 4.0). O uso para fins acadêmicos e educacionais é permitido, desde que citada a fonte original (JurisTube) conforme as normas técnicas indicadas neste documento.

Termos completos:

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.pt-br>