

---

## **Relatório**

**Mesa: “Proteção de Dados na Administração Pública”**

**VIII Fórum da Internet no Brasil**

**Novembro de 2018**

---

### **PROPONENTES**

*Ana Carolina Rodrigues*  
*Juliana Novaes*

### **MEDIADORA**

*Juliana Novaes*  
juliananbc@gmail.com  
São Paulo/SP

Graduada em Direito pela USP. Trabalha no Centro de Referência Legal da ARTIGO 19. Co-organizadora do capítulo de São Paulo do Legal Hackers. Co-fundadora do Grupo de Estudos em Inovação, Direito e Autoria na Faculdade de Direito da USP. Chefe da Comissão de Projetos do Youth Observatory. Co-organizadora do nets@USP. Membro do Núcleo de Estudos em Internet e Sociedade. Pesquisadora em Direito Autoral e Internet.

### **RELATORA**

*Ana Carolina Rodrigues*  
rds.anacarolina@gmail.com  
São Paulo/SP

Graduação em Direito pela USP. Monitora acadêmica nos cursos de especialização em Direito Empresarial e Tributação dos Negócios da Economia Digital da FGV-SP. Co-fundadora e co-organizadora do São Paulo Legal Hackers.

### **DEBATEDORES**

*Bruno Bioni (Academia)*  
bioni.bruno@gmail.com  
São Paulo/SP

Doutorando em Direito Comercial e Mestre em Direito Civil. Foi *study visitor* do Departamento de Proteção de Dados Pessoais do Conselho da Europa e pesquisador visitante no Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa. Atualmente é pesquisador da Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade/LAVITS e advogado do Núcleo de Informação e Coordenação do Ponto Br/NIC.br. Fundador do Data Privacy Br.

***Eugênio Antunes (Emprel)***

eugenio.antunes@recife.pe.gov.br  
Recife/PE

Analista de sistemas formado pela Universidade Católica de Pernambuco – UNICAP, com especialização em Gestão de Tecnologia da Informação e Mestre em Ciência da Computação pela Universidade Federal de Pernambuco – UFPE. Iniciou profissionalmente na iniciativa privada na multinacional UNISYS em 1990. Diretor Executivo de Informática da Secretaria de Trabalho e Ação Social do Estado de Pernambuco nos anos de 1995, 1996 e 1997. Ingressou no Ministério Público de Pernambuco como analista concursado no ano de 1997, exercendo dentre outras funções a Coordenação da área de Tecnologia da Informação durante os anos de 2001 a 2012. Assumiu a Presidência da EMPREL em janeiro de 2013.

***Laura Tresca (ARTIGO 19)***

laura@article19.org  
São Paulo/SP

É diretora-executiva interina da ARTIGO 19. Graduada em Jornalismo e Ciências Sociais e mestre em Comunicação Social. Foi professora substituta da Universidade de Brasília (UnB), pesquisadora no estudo sobre celulares e desenvolvimento socioeconômico na América Latina.

***Ricardo Guimarães (CityTech)***

ricardo@citytech.ai  
Salvador/BA

Co-founder da CityTech, empresa inovadora que utiliza inteligência artificial para tornar as cidades mais inteligentes e cognitivas. Tem mais de 14 anos de experiência em Tecnologia e já atuou nos mercados financeiro e de desenvolvimento de softwares. Na CityTech, é responsável pela operação do Urban Insights - o assessor inteligente do gestor público que utiliza inteligência artificial para entender, analisar e gerar insights sobre as manifestações urbanas das pessoas na internet.

## MESA: PROTEÇÃO DE DADOS NA ADMINISTRAÇÃO PÚBLICA<sup>1</sup>

### RESUMO

Inserida num contexto de rápido crescimento do ecossistema de Internet das Coisas e das chamadas “Cidades Inteligentes”, a Administração Pública começa a implementar mecanismos de tratamento de dados pessoais dos cidadãos, tanto para a consecução de políticas públicas quanto para a celebração de parcerias público-privadas. Isso, é claro, gera uma série de debates polêmicos, tais como a compatibilidade da natureza dos serviços públicos com o tratamento de dados pessoais, a desigualdade de poder entre Administração e Administrados, e, conseqüentemente, os vícios contidos na manifestação de vontade dos usuários.

Esta mesa se propôs a debater e refletir sobre os limites da utilização do tratamento de dados pessoais pela Administração Pública e pelo Setor Privado, buscando pensar em alternativas regulatórias, a partir de uma olhar crítico.

### JUSTIFICATIVA

Diante do desenvolvimento do ecossistema de Internet das Coisas e da Computação Cognitiva, com seus potenciais empregos na modelagem das “*Smart Cities*” (visando, especialmente, a melhoria dos serviços públicos), a tendência é que haja um aumento exponencial na coleta e tratamento de dados pessoais dos cidadãos.

A coleta de dados pelo Setor Público, bem como o eventual tratamento e utilização por parceiros privados, são temas sensíveis à Governança da Internet, tendo em vista tanto as questões relativas aos direitos individuais e fundamentais dos cidadãos quanto a debates mais amplos sobre transparência, consentimento e concorrência, razões pelas quais o debate sobre esse tema mostra-se imprescindível.

### OBJETIVOS PROPOSTOS E ATINGIDOS

A mesa reuniu especialistas multissetoriais para discutir questões relativas à coleta, uso e tratamento de dados pessoais coletados no âmbito da Administração Pública, explorando aspectos legais, limites e controvérsias.

Os convidados (um acadêmico, uma representante do terceiro setor, um executivo de uma empresa pública e um empreendedor) compartilharam seu conhecimento, suas visões e experiências.

Nesse contexto, a sessão buscou tratar dos impactos da Internet e das novas tecnologias nos serviços públicos e as conseqüentes implicações disso em discussões relativas à privacidade e segurança.

---

<sup>1</sup> Disponível em: [https://www.youtube.com/watch?v=WseH0B6UZ\\_Y&index=20&list=PLQq8-9yVHyObAICNGEYjEaHcRdCnd84B8](https://www.youtube.com/watch?v=WseH0B6UZ_Y&index=20&list=PLQq8-9yVHyObAICNGEYjEaHcRdCnd84B8) (acesso em 10.12.2018)

Temos por objetivos atingidos: o compartilhamento e visões de cada debatedor; a reflexão sobre os ganhos, limites e aspectos controversos da matéria; a proposição de um olhar crítico sobre esse cenário de mudanças e as expectativas para o futuro; o debate sobre alternativas regulatórias, à luz da recém-aprovada Lei de Proteção de Dados Pessoais.

Pretendia-se ter adentrado mais o mérito de alguns casos concretos.

### ESTRUTURA DA MESA

- 5 min. - Boas-vindas e apresentação dos convidados da mesa
- 15 min. - Apresentação dos resultados parciais de um mapeamento feito pelo São Paulo Legal Hackers<sup>2</sup>, sobre o estado da arte da proteção de dados na América Latina
- 40 min. - Perguntas e respostas
- 10 min. - Perguntas da audiência presencial e remota
- 15 min. - Respostas às perguntas da audiência
- 5 min. - Considerações finais e agradecimento

### SÍNTESE DO DEBATE<sup>3</sup>

- **Moderadora:** Tendo em vista a natureza dos serviços públicos e os princípios que os regem, tais como a universalidade e a não discriminação entre os usuários, como é possível conciliar a idéia de cidades inteligentes com a autodeterminação informacional dos cidadãos?

- **Ricardo Guimarães:** A tecnologia não pode potencializar a marginalização de indivíduos da sociedade. É possível combinar o conceito de cidades cognitivas com o mecanismo de autodeterminação informacional, promovendo uma mudança de *mindset* de todos os atores que fazem parte de sua construção.

- **Moderadora:** Considerando a atuação da Emprtel (empresa de tecnologia da Prefeitura de Recife/PE), quais os limites da aplicação de novas tecnologias diante da proteção da privacidade dos cidadãos?

- **Eugênio Antunes:** A empresa pública é operadora dos dados, em nome do controlador, isto é, a Prefeitura. Os limites estão no próprio poder de delegação do ente estatal. O Poder Público não precisa do consentimento do portador para fazer uso desses dados, desde que sua finalidade seja para o cumprimento das funções públicas. Com a Lei de Proteção de Dados Pessoais, a Emprtel passa a ser obrigada a informar o indivíduo sobre quais dados armazena, bem como qual seu uso (o que inclui o compartilhamento com terceiros). É também imprescindível a criação e o estabelecimento das prerrogativas da Autoridade Nacional de Proteção de Dados.

---

<sup>2</sup> <http://sp.legalhackers.org/>

<sup>3</sup> O debate foi realizado antes da edição da MP nº 869/2018.

- **Moderadora:** Como o conceito de *privacy by design* deve ser encarado na modelagem das cidades cognitivas?

- **Ricardo Guimarães:** Hoje não há nenhuma garantia de que as tecnologias e soluções desenvolvidas pelas empresas atenderão ao conceito de *privacy by design*. Nesse sentido, é importante a discussão sobre os dilemas éticos e a proposição de princípios. Exemplos como o modelo chinês de *score* social a partir da coleta de dados levantam o questionamento sobre qual o limite aceitável.

- **Moderadora:** Como aplicar o conceito de *privacy by design* na anonimização dos dados, considerando as vulnerabilidades desse processo?

- **Eugênio Antunes:** Os dados abertos devem ser publicizados somente após sua despersonalização. Isso depende do cuidado na modelagem dos algoritmos, mas a sociedade civil também pode e deve contribuir na fiscalização e sugestão de mudanças na forma de divulgação.

A LGPD estimula o compartilhamento de dados entre diferentes agentes públicos. No entanto, o titular do dado pode, de forma facilitada e gratuita, indagar a empresa sobre se seus dados estão sendo armazenados, como são tratados, com quem são compartilhados e para quais finalidades.

- **Moderadora:** Quais as conseqüências sociais, a longo prazo, do tratamento massivo de dados pela Administração Pública?

- **Laura Tresca:** O Poder Público precisa tratar dados. Isto está na base da oferta e melhoria dos serviços públicos. O problema surge quando o tratamento de dados adquire outros objetivos que não a finalidade pública previamente estabelecida. Soma-se a isso os riscos no tratamento em áreas mais sensíveis, como a Segurança Pública.

Devem ser observados os direitos do titular, os princípios gerais da LGPD, a proporcionalidade e o devido processo legal para que o tratamento de dados pelo Poder Público não seja abusivo.

- **Moderadora:** A Lei Geral de Proteção de Dados tem um capítulo específico sobre a proteção de dados na Administração Pública. Gostaria de saber se, na sua opinião, o capítulo abarca suficientemente as relações envolvendo o Poder Público para evitar usos abusivos de dados dos usuários de serviços públicos.

- **Bruno Bioni:** Quem acompanhou o debate viu que o capítulo IV foi quase retirado da lei. Ele ainda é objeto de muitas disputas interpretativas, porque traz mais perguntas do que respostas.

Da legislação como um todo, ele é o menos técnico e existem alguns pontos que não fazem muito sentido e que utilizam conceitos pouco específicos que deixam muita margem para dúvida.

Esses casos da Serpro e da Linha 4 não são completamente respondidos pelo capítulo IV, sendo necessário retornar aos princípios gerais de proteção de dados.

Nesse cenário de parcerias público-privadas, muito do equilíbrio financeiro dessas

iniciativas vem do tratamento de dados, o que traz o equilíbrio entre as normas que regem a Administração Pública, o aproveitamento econômico e a proteção dos titulares dos dados.

- **Moderadora:** Ocorreu um veto presidencial a alguns dos dispositivos previstos no texto original. Na sua visão, como os vetos se relacionam com a dinâmica de proteção de dados dentro do setor público? Quais são os impactos desse veto à privacidade do cidadão e à transparência estatal?

- **Laura Tresca:** Muito se fala sobre o veto da autoridade nacional, mas houve também um veto à proteção da identidade pessoal dos requerentes de informação pública. O ARTIGO 19 trabalha acompanhando violações à liberdade de expressão, tais como ameaças, processos judiciais e violência, e é muito comum que os agentes públicos se sintam intimidados por pedidos de informação e ameacem os requerentes.

- **Moderadora:** Ainda sobre os vetos, mas mais especificamente sobre a Autoridade Nacional de Proteção de Dados, quais você acredita serem os impactos da não existência de uma autoridade independente para o setor público, considerando o princípio da prestação de contas?

- **Bruno Bioni:** Especificamente em relação ao papel da autoridade frente à Administração Pública, o diálogo é feito em alguns artigos da lei que determinam que a autoridade pode requerer informações, emitir normas complementares, determinar boas práticas e solicitar relatórios de impacto sobre o tratamento de dados pelo setor público.

O princípio da prestação de contas, porém, é uma conduta ativa para adoção de medidas demonstrativas da adequação à lei, independente da existência de uma autoridade.

## PARTICIPAÇÃO DA AUDIÊNCIA - PERGUNTAS E RESPOSTAS

### Audiência presencial:

- **Jamila Venturini:** Como a mesa vê, de modo geral, a possibilidade de regulações locais de proteção de dados e modelos internacionais que já adotam esse tipo de estratégia?

Gostaria também de ouvir comentários da mesa sobre a interação do poder público com agentes privados, inclusive no que diz respeito a mecanismos de comunicação e utilização de redes sociais e ferramentas.

Além disso, acordos com empresas como Google para prover serviços de *e-mail* e hospedagem têm sido uma tendência nesses últimos dois anos, o que implica também acesso por parte dessas empresas a dados de funcionários públicos, estudantes e, inclusive, dados sensíveis à pesquisa acadêmica. Como vocês enxergam esta questão?  
(Dirigidas à Mesa)



**Audiência remota:**

- **Não identificado:** Como tratar da questão da proteção de dados em relação aos servidores públicos e fazer isso se tornar um assunto para todos os órgãos e servidores? **(Dirigida ao Eugênio Antunes)**

- **Bruno:** Em que situações é legítimo e aceitável o compartilhamento de dados coletados em posse do poder público com agentes privados e em quais situações é ilegítimo e inaceitável?

Qual é o lugar da governança de dados e quais aspectos são essenciais para que as estratégias de governança contribuam para proteção de dados pessoais? **(Dirigidas à Mesa)**

- **Eugênio Antunes:** Do ponto de vista de internalização dessa legislação no ambiente público, deve haver um esforço no meio técnico, para que pouco a pouco vá para os órgãos de controladoria do município, que trabalham com transparência e devem ter um cuidado. Isso irá requerer muito trabalho interno, seja em termos de legislação interna seja para regular a ação do poder público.

Isso vai envolver tanto uma parte de tratamento interno dos dados, como também a atuação de agentes externos que tratam dados do setor público. Ou seja, vamos ter que catalogar dados para proteger e estruturá-los.

Vamos também ter que prestar contas quando formos questionados pelos usuários, mas também pela Autoridade de Proteção de Dados.

Além disso, temos que ter controle efetivo sobre a execução dos serviços por terceiros contratados. Vamos ter que fazer uma regulação, inclusive com gigantes, que não costumam gostar muito de ser regulados.

- **Bruno Bioni:** sobre as iniciativas de PLs municipais, acho que é importante verificarmos a competência legislativa dessas outras entidades da federação, inclusive porque a Constituição diz que os Municípios têm competência para regular o que for de interesse local.

Se for possível dizer que há interesse local, então há constitucionalidade dessas iniciativas. O que temos visto nas experiências internacionais sobre o tema é (i) uma figura familiar no contexto brasileiro, que seria um ouvidor ou um ponto de contato dentro do Município, com quem o município poderia fazer reclamações e (ii) estruturação de conselhos municipais, como em vários Municípios do Brasil, não devendo ser diferente no contexto de uma lei de proteção de dados.

O caso de Seattle é muito simbólico, porque foi diagnosticada a necessidade de criação de um conselho municipal e o conselho foi chamado para fazer reuniões trimestrais e relatórios sobre as políticas de proteção de dados.

- **Ricardo Guimarães:** Respondendo a pergunta sobre o papel da governança dos dados no processo de construção das cidades inteligentes, acho que tudo o que está acontecendo de inovação, partindo de sistemas transacionais até o *big data*, passa pelo papel da gestão de dados.

Acredito que o papel desse gestor dos dados precisa estar muito forte desde a concepção do produto, garantindo modelos de negócios para monetizar em cima disso. Devemos também garantir o *compliance* dessa aplicação tecnológica com diversos *stakeholders* envolvidos no processo.

Um outro ponto aqui muito relevante é o fato de que todos os dados têm um nível de criticidade quando se fala de privacidade e é papel do gestor dos dados identificar os processos necessários para a segurança e privacidade dos titulares.

Dentro desse processo de construção de cidades inteligentes, a governança dos dados se torna cada vez mais importante.

- **Laura Tresca:** Internacionalmente, o que me chama atenção é o fato de que a autoridade que trata de dados pessoais é a mesma que trata de acesso à informação, e isso é interessante porque estamos falando de dois direitos fundamentais.

De um lado temos o direito à privacidade e do outro temos o direito à liberdade de expressão e acesso à informação sendo tratados pelo mesmo órgão. No Brasil, é difícil definir se seria um conselho municipal ou uma controladoria.

Não é muito claro pra mim se esse modelo funcionaria e serviria para enfrentar os problemas que levantamos aqui. Com certeza a questão da proteção do requerente deveria estar na lei geral, porque não me parece ser algo optativo de ser aplicado ou não numa localidade ou outra. Em âmbito federal, isso de alguma forma vai se resolver, mas não sabemos em âmbito municipal.

- **Não identificado:** Como garantir a segurança de quem requer dados públicos? Seria a livre disponibilização dos dados? (**Dirigida à Laura Tresca**)

- **Laura Tresca:** Uma crítica que fizeram para nós quando propusemos a emenda é a de que o anonimato é vedado pela Constituição. Porém, o que estávamos propondo não era que os pedidos fossem feitos de maneira anônima, mas sim que os dados pessoais do requerente não ficassem na base de dados daquele que responde o pedido.



### Audiência presencial:

- **Não identificado:** Qual é a visão de vocês sobre a utilização de dados pessoais para implementação de políticas de segurança pública? De um lado, temos que a segurança pública é assegurada na Constituição, mas também envolve uma opressão sobre o indivíduo, pois o poder de polícia é, por si só, ofensivo e pode se voltar contra o próprio indivíduo.

A primeira pergunta é mais genérica sobre a **opinião da mesa** sobre essa compatibilização e a segunda pergunta é direcionada ao **Eugênio**: Na sua carreira pública, você tem algum exemplo de utilização de dados da administração para investigações?

E para o **Ricardo**, você tem algum projeto de utilização de dados para políticas de segurança?

- **Ricardo Guimarães:** Não temos hoje na CityTech nenhum projeto específico sobre isso, pois tomamos a decisão de não trabalhar com dados sensíveis. Tomamos essa decisão, pois acreditamos que esse tema é extremamente delicado e, conforme falei anteriormente, depende muito do contexto de cada país e cada local.

No caso da China, existe uma utilização massiva com o intuito de melhorar a vigilância e segurança pública, em que as pessoas têm até *scores* relacionados a todos os tipos de atividades que elas desenvolvem.

Não podemos perder a nossa própria privacidade em nome da facilitação das atividades do poder público. Existe uma linha tênue aí e não estamos maduros o suficiente enquanto sociedade. Tem muitas coisas ainda para serem feitas com dados públicos que não ferem a integridade de ninguém.

- **Eugênio Antunes:** Diversas vezes, enquanto presidente de empresa pública, já recebi pedidos de informações pessoais no âmbito de inquéritos policiais e processos judiciais. Nós respondemos às solicitações e acho que a própria lei coloca algumas situações em que é possível ceder o dado pessoal.

- **Bruno Bioni:** Acho que temos uma disputa interpretativa. Uma possível interpretação a ser feita é a de que, apesar de estar fora do escopo da aplicação da lei, não quer dizer que ela não se aplique na integralidade.

Eu acho que é possível sustentar que, embora a lei como um todo não se aplica na integralidade, talvez os princípios se aplicam para essas atividades como um todo. Esses princípios dialogam muito com princípios internacionais que prezam pela necessidade, transparência etc.

- **Laura Tresca:** No caso dos 23 que foram presos porque iriam protestar durante as Olimpíadas, tivemos acesso ao inquérito e a base desse inquérito eram rondas virtuais.

Da mesma forma que temos a polícia circulando pelas ruas para pegar atividades suspeitas, foram feitas rondas virtuais para investigar atividade "suspeita", levando à prisão das pessoas que tinham apenas a intenção de protestar.

### CONSENSOS:

- O uso de dados na construção das chamadas “cidades inteligentes” não deve ser feito a partir da discriminação de indivíduos da sociedade;
- Necessidade da criação da ANPD;
- Necessidade de estabelecimento de princípios éticos que orientem a modelagem dos dados e do *privacy by design*;
- A sociedade deve participar da fiscalização sobre o tratamento dos dados pessoais dos cidadãos, contribuindo também para melhorias no processo;
- Espera-se que a ANPD elabore relatórios de impacto, emita normas complementares, estipule diretrizes e determine boas práticas, em constante diálogo com as empresas, a sociedade civil e a comunidade técnica e acadêmica.

### PONTOS A APROFUNDAR:

- Aprofundar o conceito e as atribuições do “encarregado do tratamento de dados”, definido pela Lei de Proteção de Dados Pessoais.