IoT

E SEUS **IMPACTOS** À PROTEÇÃO DE DADOS PESSOAIS

BAPTISTA LUZ
ADVOGADOS

SETEMBRO 2020

IoT e os impactos à proteção de dados pessoais

Autora

/ Gabriela Brum Davoli

Revisoras

/ Luiza Balthazar

/ Nathalia Dutra

1. Introdução

Diante da chegada da Covid-19 e da necessidade de evitar o contágio do vírus, o mundo se deparou com a necessidade de buscar meios eficazes para evitar que as pessoas saíssem de casa, bem como de conferir segurança para que os profissionais pudessem voltar para suas atividades o quanto antes e com menor risco possível. Consequentemente, ao mesmo tempo em que essa realidade aproximou os indivíduos de temas relacionados à vida doméstica, fez com que empresas investissem em tecnologia para criar mecanismos para o retorno seguro às atividades de trabalho[1].

Tanto dentro quanto fora de casa, percebe-se a presença de aplicativos que envolvem desde aplicações domésticas, como controle remoto de objetos, até aplicações em ambientes externos como sensores de temperatura que utilizam a Internet das Coisas (*Internet of Things* – IoT). Para essa série, escolhemos abordar assuntos que, em um primeiro momento, estarão mais ligados ao ambiente doméstico e à vida em quarentena, como a utilização da tecnologia dentro de casa e a potencial influência da utilização dessa tecnologia em resposta aos prejuízos causados pela pandemia do coronavírus.

Com o decorrer do tempo, diante da possível flexibilização da quarentena e da crescente expectativa de retorno à antiga realidade, serão cada vez mais debatidos tópicos relacionados à vida externa, partindo-se de uma visão de utilização da tecnologia a favor dos direitos humanos. O objetivo dessa série é trazer uma reflexão sobre os impactos que a tecnologia tem trazido para a vida em quarentena e para esses direitos, e sobre como ela pode ajudar nas próximas etapas de retomada da economia e da vida em sociedade.

[1] MACEDO, Fausto. Desenvolvimento de soluções em IoT sustentáveis é impulsionado pela pandemia. Estadão. São Paulo, 24 ago. 2020. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/desenvolvimento-de-solucoes-em-iot-sustentaveis-e-impulsionado-pela-pandemia/

2. IoT

Um dos resultados dessa intersecção da tecnologia com o cotidiano das pessoas é a Internet das Coisas – ou Internet of Things (IoT) em inglês. Por ela são englobados os pontos acima dispostos, tanto *indoor* quanto *outdoor*. Conhece-se como IoT toda a tecnologia que permite conectar o mundo real e o mundo virtual, sendo tal expressão comumente usada para designar os objetos conectados à internet.

Com as infinitas possibilidades que esse tipo de tecnologia pode oferecer à sociedade, bem como os benefícios econômicos que o seu desenvolvimento pode proporcionar[2], os países têm investido cada vez mais na sua implementação. Nesse sentido, referida implementação é inclusive considerada como uma das medidas auxiliares para a alcançar os Objetivos de Desenvolvimento Sustentável da Organização das Nações Unidas[3].

Levando em conta tais fatores, em 25 de junho de 2019, foi publicado o Decreto nº 9.854, que institui o Plano Nacional de Internet das Coisas no Brasil[4], o qual estabelece conceitos, diretrizes e dispõe sobre a Câmara de Internet das Coisas. O Decreto considera IoT como "*a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade*".

Como interoperabilidade, entende-se a característica referente à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficiente[5]. Essa característica proporciona, por exemplo, que sejam criados dispositivos capazes de, em conjunto com inteligência artificial, fazer diagnósticos prévios de maneira rápida e sem a necessidade de se aguardar pelo resultado de um exame[6].

---

[2] BNDES. Produto 8: Relatório do Plano de Ação: Iniciativas e Prohjetos Mobilizadores. 2017. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/269bc780-8cdb-4b9b-a297-53955103d4c5/relatorio-final-plano-de-acao-produto-8-alterado.pdf?MOD=AJPERES&CVID=m0jDUok

[3]. BIGGS, Phillippa, GARRITY, John. Harnessing the Internet of Things for Global Development: A contribution to the UN Broadband Comission dor Sustainable Devepolment. Disponível em: https://www.itu.int/en/action/broadband/documents/harnessing-iot-global-development.pdf

[4] BRASIL. Decreto nº9.894/19. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm

[5] GOVERNO DIGITAL. Governança de dados: conceito interoperabilidade, 25 mai. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/interoperabilidade

[6] ROCHA, Marcus Vinícius. Pandemia cria oportunidades para o desenvolvimento de soluções em IoT sustentáveis. ABINC: Associação Brasileira de Internet das Coisas. 9 jun. 2020. Disponível em: https://abinc.org.br/pandemia-cria-oportunidades-para-o-desenvolvimento-de-solucoes-em-iot-sustentaveis/

Um bom exemplo dessa situação é a recente invenção da Universidade de Stanford, o sanitário inteligente[7]. Trata-se de dispositivo de análises clínicas dos pacientes no seu cotidiano, capaz de descartar a necessidade de exames laboratoriais, consistente de um banheiro equipado com tecnologia que pode detectar uma série de marcadores inteligentes de doenças nas fezes e urina e até de alguns tipos de câncer.

Parece uma opção atraente para indivíduos geneticamente predispostos a certas condições de saúde e que desejam se manter atualizados sobre tais condições. Da mesma forma, parece um grande passo para o caminho pelo qual a tecnologia e a saúde provavelmente trilharão juntas.

Invenções como essas só são possíveis a partir da identificação de determinados padrões a partir da análise de dados, sendo que, para esta identificação, é preciso que haja o tratamento sistematizado de dados em grande escala. Diante dessas circunstâncias, faz-se necessária a reflexão sobre qual é o impacto que esse tipo de tratamento de dados pode ter na vida das pessoas e como as organizações podem avançar tecnologicamente de modo que esse impacto seja o menor possível.

3. Proteção de Dados

O Plano Nacional de Internet das Coisas define, em seu primeiro artigo, que terá como finalidade implementar e desenvolver a Internet das Coisas no país, com base na livre concorrência e na livre circulação de dados, observadas as diretrizes de segurança da informação e de proteção de dados pessoais. Deve-se então observar a Lei Geral de Proteção de Dados Pessoais (LGPD)[8], que dispõe de princípios, orientações e regras relacionadas ao tratamento de dados pessoais, incluindo as penalidades em caso de descumprimento.

Entre os objetivos basilares da nova legislação de proteção de dados, estão a ampliação dos direitos de todos em relação aos seus dados pessoais e a maior responsabilização das organizações que realizam o tratamento de dados pessoais. Um dos principais fundamentos da legislação, além da preservação da privacidade das pessoas, é a definição destas como titulares dos dados pessoais, podendo exercer seus direitos em relação a essa titularidade frente a terceiros que fazem o tratamento das suas informações.

---

[7] ARMITAGE. Hinae. 'Smart toilet' monitors for signs of disease. Stanford Medicine: News Center. 6 abr. 2020. Disponível em https://med.stanford.edu/news/all-news/2020/04/smart-toilet-monitors-for-signs-of-disease.html#:~:text=and%20maternal%20health-,'Smart%20toilet'%20monitors%20for%20signs%20of%20disease,a%20new%20Stanford%20study%20reports.&text=The%20smart%20toilet%20automatically%20sends,cloud%2Dbased%20system%20for%20safekeeping.

[8] BRASIL. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Por outro lado, se antes só havia uma base legal possível para o tratamento de dados pessoais em ambiente online, o consentimento[9], hoje, a LGPD possibilita outras nove hipóteses[10] em seu artigo 7º. Frente a essas circunstâncias, vale a identificação de quais podem ser os desafios encontrados pelas empresas que desenvolvem IoT em relação ao tratamento de dados pessoais, bem como quais são as formas de mitigar os riscos encontrados para viabilizar o desenvolvimento seguro da tecnologia em conformidade com a legislação.

4. Desafios da aplicabilidade da IoT em conformidade com a legislação de proteção de dados

Imagine um dispositivo IoT que tenha a funcionalidade de ligar automaticamente as luzes ao final da tarde. Agora, imagine que, por algum motivo, o dispositivo foi programado para não ligar as luzes durante um feriado e que essas informações ficaram salvas em algum sistema conectado à internet. Pode se afirmar que, caso esse sistema tenha algum acesso indevido, pessoas não autorizadas podem se aproveitar da informação da provável ausência de alguém em casa para finalidades criminosas.

Há diversas situações como essa que ilustram os riscos aos quais os usuários estão expostos quando se fala em IoT. Em 2017, por exemplo, aproximadamente, 500 mil americanos receberam a informação de que precisariam atualizar seus dispositivos "marca-passo" em função de uma possível invasão do aparelho por hackers[11]. Os dispositivos eram conectados à internet e precisaram ser atualizados para evitar que parassem de funcionar, de modo que os dispositivos tiveram que passar por um recall, colocando em risco a vida de seus usuários.

Problemas relacionados à segurança da informação e vazamento de dados são apenas um dos desafios encontrados quando se fala do tratamento de dados pessoais em grande escala para desenvolvimento de IoT em conformidade com a legislação. Outras questões encontradas podem incluir a falta de controle das informações pelos usuários; a dificuldade de se obter um consentimento válido dos usuários quando este consentimento é necessário – como no caso dos dados de saúde; o tratamento de dados pessoais gerados por inferência em relação aos dados originalmente tratados e o consequente uso de dados para fins diversos dos quais foram originalmente coletados; as definições de padrões de comportamento de forma intrusiva; e a dificuldade de anonimização de dados quando da utilização dos serviços[12].

---

[9] BRASIL. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

[10] Há uma discussão sobre os requisitos para o consentimento no ambiente online, visto que a LGPD não revogou expressamente essa seção do Marco Civil da Internet e, portanto, para as atividades de coleta de dados por meio do consentimento na internet, haveria dúvida sobre a como a lei deveria ser aplicada. O Marco Civil da Internet conta com apenas uma Base Legal – o consentimento – e estabelece que este de ser livre, expresso e informado. A LGPD, por sua vez, traz dez Bases Legais e quando conceitua o consentimento afirma que este deve ser livre, inequívoco e informado.

[11] Hern, Alex. Hacking risk leads to recall of 500,000 pacemakers due to patient death fears. The Guardian, 31 ago. 2017. Disponível em: https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update

[12] Article 29 Data Protection Working Party. Opinion 8/2014 on the Recent Developments on the Internet of Things. 16 set. 2014. Disponível em: https://www.pdpjournals.com/docs/88440.pdf

Soma-se a essas questões a dificuldade de cumprir com os direitos dos titulares dos dados, como o de acesso às informações sobre o tratamento realizado, o da eliminação dos dados, bem como o da portabilidade dos dados para outras empresas. Todas essas circunstâncias geram custos à organização responsável pelo tratamento, uma vez que esta precisa armazenar todas as informações sobre o tratamento dos dados, além de manter efetiva governança e segurança sobre todo o tratamento realizado.

Adicionalmente, a empresa precisa ter bem definidas quais são as atividades de tratamento que pretende realizar e, assim, verificar sua viabilidade por meio da identificação de uma base legal para cada uma dessas atividades, além de ter documentada essa definição. Por fim, precisa garantir que todas as partes envolvidas no tratamento (titulares, operadores e co-controladores) saibam quais informações estão sendo coletadas, para que estão sendo utilizadas e por quanto tempo serão armazenadas.

Além disso, a transparência é o ponto chave para a conformidade com a LGPD. A principal medida para se garantir a transparência é a elaboração de Avisos e Políticas de Privacidade de forma objetiva e precisa em relação ao tratamento dos dados pessoais realizado.

Neste sentido, para se dar efetividade às disposições da LGPD, espera-se que mais orientações sobre como proceder no caso de tratamento de dados em grande escala, inclusive no caso da IoT, sejam indicadas pela Autoridade Nacional de Proteção de Dados. No entanto, é possível extrair de uma leitura objetiva da LGPD que, até referida entidade iniciar as suas atividades, as organizações já podem tomar algumas medidas capazes de promover a conformidade das suas atividades de tratamento de dados com a nova legislação.

Aliás, no último dia 26, foi publicado o Decreto nº 10.474/20 que, entre outras medidas, aprovou a estrutura regimental da Autoridade Nacional de Proteção de Dados. Esta será responsável por apontar as diretrizes sobre o tratamento de dados pessoais no Brasil, inclusive mediante a edição de normas e procedimentos, o estabelecimento de protocolos de segurança e a aplicação de sanções às organizações que infringirem suas obrigações legais e regulatórias na área de proteção de dados.

5. A transparência e a viabilidade do desenvolvimento da IoT

Como soluções para viabilizar o desenvolvimento da IoT em conformidade com a LGPD, podem ser pontuadas as seguintes[13]: (i) a compreensão das exigências da Lei; (ii) o desenvolvimento de uma estratégia de mitigação de riscos na concepção de novos produtos e serviços; (iii) a priorização da transparência no tratamento de dados; (iv) a consideração das limitações tecnológicas e de custos da organização; e (v) a indicação de um encarregado de proteção de dados pessoais pela organização.

[13] Personal Data Protection for Internet of Thing Deployments: Lessons learned from the European large-scale pilots of Internet of Things. Disponível em: https://european-iot-pilots.eu/wp-content/uploads/2020/06/Personal-Data-Protection-for-IoT-Deployments_2020.pdf

Para o desenvolvimento de uma estratégia de mitigação de riscos, é necessário considerar os princípios de proteção de dados. Para tanto, as análises de *Privacy by Design (PbD)* e *Privacy by Default* podem ser uma boa alterativa.

Uma análise *Privacy by Design* consiste na avaliação de produtos, serviços e atividades de tratamento de dados pessoais levando em consideração os princípios e as regras da Lei desde a sua concepção até a sua implementação e o seu pleno funcionamento, a fim de: (i) identificar as medidas necessárias à adequação desses produtos e serviços à LGPD e, consequentemente; (ii) mitigar riscos decorrentes do tratamento de dados pessoais aos direitos e às liberdades dos titulares de dados[14].

A LGPD define que os agentes de tratamento de dados pessoais devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como que tais medidas devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução[15].

Já a análise *Privacy by Default* decorre da análise *Privacy by Design* na medida em que direcionará a configuração dos produtos e serviços, sempre partindo, por padrão, de formatos mais protetivos e menos invasivos para, apenas após interações livres dos titulares de dados, alcançar modelos que utilizem dados pessoais de forma mais acentuada. Nesta análise, é fundamental avaliar o volume de dados tratados, quais deles são estritamente necessários para o funcionamento e oferecimento do serviço/produto, a duração das atividades de tratamento, o período de retenção de dados pessoais etc.[16]

Na prática, a análise PbD pode ser feita por meio da elaboração de resposta para os seguintes questionamentos relacionados aos princípios da Lei, como podemos ver a seguir:

[14] DAVOLI, Gabriela; OLIVEIRA, Amanda; SILVA, Gustavo; GABRIADES, Felipe; BOUSSO, Fernando; RAMOS, Pedro; PESSOA, Rafael; MONTEIRO, Renato. Afinal, que caminho preciso percorrer para me adequar à Lei Geral de Proteção de Dados Pessoais?. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2020/05/BLuz-Metodologia-LGPD.pdf

[15] BRASIL. Lei Geral de Proteção de Dados Pessoais. Art. 46, §1º. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

[16] DAVOLI, Gabriela; OLIVEIRA, Amanda; SILVA, Gustavo; GABRIADES, Felipe; BOUSSO, Fernando; RAMOS, Pedro; PESSOA, Rafael; MONTEIRO, Renato. Afinal, que caminho preciso percorrer para me adequar à Lei Geral de Proteção de Dados Pessoais?. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2020/05/BLuz-Metodologia-LGPD.pdf

Princípio	Descrição	IoT
Finalidade	A realização do tratamento deve atender a propósitos legítimos, específicos, explícitos e informados aos titulares, sendo vedado o tratamento posterior incompatível com essas finalidades.	• Foram identificadas todas as finalidades para as quais a empresa tratará dados pessoais nesse novo produto, solução ou sistema? • Essas finalidades são legítimas, específicas e explicitas? • Essas finalidades foram informadas ao titular?
Adequação	O tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.	• A forma que os dados estão sendo tratados é coerente com as finalidades que foram informadas ao titular?
Necessidade	Os dados tratados devem ser limitados ao mínimo necessário para a realização de suas finalidades.	• Os dados tratados são os mínimos necessários para atingir as finalidades do tratamento? • Todos os dados tratados são relevantes e úteis para a finalidade de tratamento? • Existe alguma informação excessiva?
Livre Acesso	Deve ser garantido aos titulares dos dados consulta gratuita e facilitada sobre a forma e a duração do tratamento dos seus dados.	• A política de privacidade da empresa dispõe sobre a forma e duração de tratamento dos dados? • A empresa está apta a responder consultas sobre a forma e a duração do tratamento dos dados? • A empresa está apta a atender solicitações sobre acesso aos dados?
Qualidade dos dados	Deve ser garantida aos titulares a exatidão, clareza, relevância e atualização dos dados pessoais tratados.	• Existem controles para validar dados inconsistentes, incompletos ou imprecisos? • Existem mecanismos para revisão periódica da base de dados?
Transparência	Os titulares devem receber informações claras, precisas e facilmente acessíveis sobre o tratamento dos dados pessoais.	• As ferramentas, configurações e funcionalidades de privacidade são claras, visíveis, fáceis de encontrar e de usar? • Existem mecanismos de transparência específicos para dados sensíveis? • A política de privacidade cumpre todos os requisitos legalmente previstos (art. 9)?
Segurança	Devem se empregadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alterações, comunicação ou difusão.	• Uma avaliação técnica foi realizada para identificar e corrigir vulnerabilidades identificadas neste novo sistema, produto ou solução? • Medidas técnicas ou organizacionais foram adotadas para mitigação dos riscos detectados nas avaliações? • Quais medidas foram empregadas para prevenção da ocorrência de incidentes de segurança da informação?
Prevenção	Devem ser utilizadas medidas no sentido de prevenir a ocorrência de danos em virtude do tratamento dos dados pessoais.	• Riscos foram identificados e medidas de mitigação forma implementadas?
Não discriminação	Os dados pessoais não devem ser tratados para fins discriminatórios, ilícitos ou abusivos.	• O produto ou sistema utiliza dados sensíveis? Se sim, o tratamento desses dados pode gerar inferências discriminatórias ou abusivas? • O produto ou sistema segmenta a base de dados pessoais em perfis comportamentais? Se sim, há garantia de que os *clusters* não são discriminatórios ou abusivos?
Responsabilização e prestação de contas	Deve ser possível demonstrar que comprovem que foram adotadas medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.	• A análise *privacy by design* foi documentada e armazenada?

Já para o caso de atividades de tratamento já existentes e em desenvolvimento, nas quais se identifica potencial risco às liberdades civis e aos direitos fundamentais dos titulares, a Lei indica a possibilidade de elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD)[17]. Referido documento pode servir para a organização demonstrar boas práticas em tratamento de dados pessoais e identificar os seus processos mais relevantes e mais sensíveis, inclusive em atendimento ao princípio da prestação de contas (*accountability*)[18].

[17] Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. BRASIL. Lei Geral de Proteção de Dados Pessoais. Art. 5º, XVII. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

[18] Ibidem.

Além disso, o RIPD pode ser exigido pela ANPD em algumas situações[19]. Contudo, o conteúdo mínimo e a forma que o documento precisará ter nestes casos também estão pendentes de definição pela autoridade.

De qualquer forma, alguns questionamentos podem ser feitos para auxiliar nessa identificação como:

- Quais são os dados tratados?
- Para onde os dados são enviados?
- Foram identificadas as bases legais para cada atividade de tratamento?
- Com quem os dados são compartilhados?
- Esses parceiros/fornecedores estão em conformidade?
- Quantos titulares estão envolvidos no tratamento?
- Apenas as pessoas necessárias têm acesso a esses dados?
- Onde os dados são armazenados?
- Por quanto tempo os dados são armazenados?
- Qual é o nível de segurança dos dados ao serem transferidos e ao serem armazenados?
- Como os titulares serão notificados no caso de vazamento de dados?
- O tratamento gera algum prejuízo às liberdades civis ou aos direitos fundamentais dos titulares?

A partir da elaboração de um RIPD, será possível indicar as medidas de mitigação de riscos necessárias para o tratamento dos dados envolvidos no funcionamento de dispositivos de IoT, como medidas relacionadas à segurança dos sistemas (ex. utilização de criptografia), até medidas que confiram maior transparência ao usuário (ex. política de privacidade) e que possibilitem a gestão dos dados pelo próprio titular (ex. gestão do consentimento[20]). Assim, será possível o desenvolvimento de novos produtos e serviços de IoT já em conformidade com as boas práticas de proteção de dados pessoais, bem como a análise daquelas atividades já existentes e a indicação de mitigação de riscos para que tais soluções possam ser consideradas adequadas.

[19] BRASIL. Lei Geral de Proteção de Dados Pessoais. art. 38 e art. 10, §3º. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

[20] Manifestação livre – possibilidade de não fornecer o consentimento; informada – fornecimento de informações sobre a finalidade e as consequências do tratamento; e inequívoca – garantia de que o titular agiu de forma clara e afirmativa. BRASIL. Lei Geral de Proteção de Dados Pessoais. art. 5º, XII. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

6. Considerações finais

Sem dúvidas, o desenvolvimento da IoT tem facilitado algumas das atividades mais comuns do dia-a-dia, ao mesmo tempo que tem contribuído para o avanço tecnológico das mais diversas áreas de pesquisa. Consequentemente, a publicação do Plano Nacional de Internet das Coisas é um importante avanço para que o país possa progredir nesse sentido.

Para que esse avanço ocorra de forma adequada, especialmente considerando a recente entrada em vigor da Lei de Proteção de Dados Pessoais, é necessário que as organizações levem em consideração os princípios de proteção de dados pessoais e os direitos das pessoas sobre seus dados no momento de avaliação das suas atividades. Dessa maneira, organizações do ramo devem se preparar para realização de análises sob o viés da proteção de dados no momento da concepção de produtos e serviços, bem como no momento de avaliação daqueles produtos e serviços já existentes.

Esse material contém conteúdo meramente informativo, e não deve ser entendido como um aconselhamento ou orientação jurídica específica. Cada modelo de negócio tem suas peculiaridades e implicações, de modo que recomendamos que as organizações sempre procurem o auxílio de um advogado de sua confiança para o acompanhamento dos aspectos jurídicos para o desenvolvimento de novos produtos e serviços de IoT.

/ SÃO PAULO
Rua Ramos Batista, 444 / 2° Andar
Vila Olímpia / São Paulo / SP
Tel +55 11 3040 7050

/ PORTO ALEGRE
R. Carlos Trein Filho, 599 / 11° andar
Auxiliadora / Porto Alegre / RS
Tel +55 51 3207 9057

/ FLORIANÓPOLIS
Rua Bento Gonçalves, 183 / Sala 1001
Centro / Florianópolis / SC
Tel +55 48 3225 6468

/ LONDRINA
Rua Ayrton Senna da Silva, 300 / Sala n° 1801
Gleba Palhano / Londrina / PR
Tel +55 43 3367 7050

/ MIAMI
1110 Brickell Ave / Ste 200
Miami / FL 33131

contato@baptistaluz.com.br
www.baptistaluz.com.br

BAPTISTA LUZ
ADVOGADOS