Internet das Coisas: privacidade e segurança na perspectiva dos consumidores

[Contribuição à consulta pública do consórcio MCTIC/BNDES de fevereiro de 2017]

Instituto Brasileiro de Defesa do Consumidor

“Internet das Coisas: privacidade e segurança na perspectiva dos consumidores”

Autor:

Rafael A. F. Zanatta

***

O **Instituto Brasileiro de Defesa do Consumidor** é uma associação de consumidores fundada em 1987. Não possui fins lucrativos. É independente de empresas, governos ou partidos políticos. Os recursos financeiros para o desenvolvimento de suas atividades têm sua origem nas contribuições dadas pelos seus associados. O Idec também desenvolve projetos que recebem recursos de organismos públicos e fundações independentes, como Fundação Ford e Open Society Foundation. Esse apoio não compromete a independência do Instituto. O Idec é membro pleno da *Consumers International* e faz parte do Fórum Nacional das Entidades Civis de Defesa do Consumidor e Associação Brasileira de Organizações Não-Governamentais. Em 2016, o Instituto tornou-se membro do *Civil Society Information Society Advisory Council* (CSISAC), que representa a sociedade civil perante o Comitê de Políticas para Economia Digital da Organização para Cooperação e Desenvolvimento Econômico (OCDE). O Idec também integra o Grupo de Trabalho de Consumo e Telecomunicações da Secretaria Nacional do Consumidor, do Ministério da Justiça e Cidadania.

idec
Instituto Brasileiro de Defesa do Consumidor

Sumário

1. Introdução

A preocupação do governo brasileiro com a chamada "Internet das Coisas" – rede de objetos que se comunicam e interagem de forma autônoma pela Internet – é crescente. Em 2014, houve a instituição da Câmara de IoT, cujo objetivo é "subsidiar a formulação de políticas públicas, promover e acompanhar o desenvolvimento de soluções de comunicação máquina a máquina (M2M) e Internet das Coisas para o mercado brasileiro". No ano passado, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MTIC) e o Banco Nacional de Desenvolvimento Econômico e Social (BNDES) estabeleceram um convênio para apoiar a realização de um amplo estudo sobre Internet das Coisas no país. Em dezembro, o convênio anunciou uma consulta pública por meio da plataforma Participa.br,[1] com perguntas organizadas em doze eixos:

i. Pesquisa e desenvolvimento;
ii. Recursos humanos;
iii. Oferta tecnológica e composição de ecossistemas;
iv. Investimento, financiamento e fomento;
v. Demanda;
vi. Aspirações;
vii. Gerenciamento de infraestrutura;
viii. Suporte a aplicações e serviços;
ix. Redes e transporte de dados;
x. Gateways e dispositivos;
xi. **Segurança e privacidade**;
xii. Papel do Estado;
xiii. Assuntos regulatórios;

A contribuição do Instituto Brasileiro de Defesa do Consumidor concentra-se exclusivamente no item 11 da consulta pública, que trata de segurança e privacidade. Na visão do Idec, esse é o eixo que possui maior aderência ao Código de Defesa do Consumidor e o Marco Civil da Internet – dois pilares jurídicos que dão sustentação à proteção do consumidor no uso da Internet no país.

[1] Ver http://www.telesintese.com.br/consulta-publica-sobre-politica-de-iot-ja-esta-aberta/

O Idec entende que o desenvolvimento da indústria de Internet das Coisas no Brasil levanta questões fundamentais relacionadas aos princípios do Código de Defesa do Consumidor. Em especial, a existência de milhões de dispositivos conectados, com diferentes funções automatizadas e controladas por servidores conectados à Internet, coloca em evidência o direito de "proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos" (Art. 6º, I). Veículos com direção autônoma e "fogões inteligentes", por exemplo, tornam-se exemplos cotidianos de riscos reais relacionados à invasão de sistemas e riscos direcionados aos consumidores (sistemas de freios que podem ser modificados ou controle de temperatura e liberação de gás à distância).

Como notado pela *Federal Trade Commission* (FTC) em relatório de 2015,[2] há um problema grave quando fornecedores de produtos e serviços da "indústria off-line" passam a fazer parte da cadeia de produtores de tecnologias de conexão à Internet, sem *expertise* técnica e sem os cuidados dos profissionais de segurança da informação, tipicamente ligados ao universo da computação, da T.I. e do gerenciamento de redes. Esse movimento da indústria exige atenção e atuação regulatória para evitar lesão aos consumidores.

Dizer que um dispositivo é "inteligente" não significa dizer que ele é seguro ou que ele não traz vulnerabilidades aos consumidores. Pelo contrário. Conforme notado por estudos técnicos da área e pela própria consulta pública, os riscos são elevados, considerando que as vulnerabilidades existem no "software utilizado pelo dispositivo, na gestão de identidade e controle de acesso e na comunicação entre dispositivos e sistemas". O Idec reforça o entendimento firmado pela *Federal Trade Commission* de que as regras de segurança devem ser aplicadas no processo de design e *não posteriormente*. As empresas precisam (1) conduzir avaliação de risco e privacidade, (2) minimizar o conjunto de dados coletados e retidos (princípio da necessidade), e (3) testar as medidas de segurança antes de lançar produtos.

Um dos desafios primordiais consistirá no dever de informação adequada e clara sobre os "riscos apresentados por um produto ou serviço" (Art. 6º, II). Assim, do mesmo modo que existem "bulas" com informações sobre riscos causados em determinados medicamentos, será preciso pensar em formas obrigatórias de comunicação sobre potenciais riscos aos consumidores de dispositivos que integram o universo da Internet das Coisas.

---

[2] Federal Trade Commission, *Internet of Things: privacy & security in a connected world*. FTC. January, 2015.

Com relação à privacidade e proteção de dados pessoais, o Idec entende que o fomento da indústria de Internet das Coisas sem a aprovação da lei geral de proteção de dados pessoais é extremamente danosa, considerando que o projeto de lei n. 5276/16 estabelece uma sistemática principiológica sobre a coleta e tratamento de dados pessoais, definindo regras fundamentais como o "legítimo interesse" (coleta de dados a partir do que foi informado ao consumidor e para os fins legítimos daquela atividade comercial) e o "princípio da necessidade", que afirma ser dever daquele que realiza a coleta e processamento de dados a *utilização mínima*, limitada ao necessário, para as funcionalidades esperadas pelo consumidor. As considerações sobre privacidade e proteção de dados pessoais não devem se ater apenas os dispositivos relacionados ao consentimento expresso do Marco Civil da Internet (art. 7., inciso IX), mas devem considerar a arquitetura jurídica presente no Projeto de Lei n. 5276/16, fruto de amplos debates com a sociedade civil e diferentes partes interessadas.[3]

O Idec entende que a "minimização de dados" – o atendimento ao princípio da necessidade na coleta de dados pessoais – deve ser vista também como uma medida de segurança para as empresas. Um grande conjunto de dados coletados por tais dispositivos gera incentivos para ataques hackers e ladrões, *dentro e fora das empresas*. Qualquer política pública formulada sobre esse setor deve ter em mente um conjunto de medidas regulatórias para (i) incentivar o uso mínimo de dados pessoais e (ii) desincentivar o uso desproporcional de dados, violando os princípios da futura lei geral de proteção de dados pessoais.

A utilização de dispositivos conectados pelo Estado na prestação de serviços públicos ou em serviços outorgados à exploração por entes privados também deve possuir as mesmas preocupações com privacidade e proteção de dados pessoais. Não deve haver exceção ou "excepcionalismo regulatório" em proteção de dados pessoais quando se trata de Poder Público – motivo pelo qual se faz necessária a criação de uma Autoridade de Proteção de Dados Pessoais independente, com capacidade de monitoramento do

O Idec defende que as informações sobre os padrões de segurança adotados pelos provedores de aplicação – e pelos dispositivos que possuem aplicações imbutidas – devem ser divulgadas de forma clara e acessível a qualquer interessado por meio de seus sítios na Internet. No caso de dispositivos que não possuem interface de uso, deve ser obrigatório o envio de tais informações por meio físico e a publicidade de tais informações nas lojas de

[3] Ver manifestação do Idec sobre o PL 5276/16: http://www.idec.org.br/em-acao/em-foco/idec-e-outras-ongs-declaram-apoio-a-projeto-de-lei-sobre-proteco-de-dados-pessoais

venda de tais produtos, tanto lojas físicas quanto lojas virtuais, em respeito ao Código de Defesa do Consumidor e ao decreto de regulamentação do Marco Civil da Internet.

O Idec também enxerga uma relação virtuosa entre plataformas abertas, interoperabilidade e maior segurança para usuários. Padrões abertos e tecnologias de código aberto (*open source*) possuem impacto positivo na segurança, pois possibilita o controle por inúmeros pares e desenvolvedores, permitindo, além disso, o aprendizado conjunto e o estímulo a um maior número de competidores – o que possui o potencial efeito de redução de oligopólios, aumento da competição e benefícios aos consumidores finais.

2. Mecanismos de segurança a vulnerabilidade ao consumidor

Quais os desafios para a implementação dessas camadas de capacidade de segurança em dispositivos M2M/IoT? Em sua opinião, existe no contexto de M2M/IoT a necessidade de novos mecanismos de segurança, devido a particularidades desses novos ambientes? Se sim, existe oportunidade para desenvolvimento local? Poderia citá-los juntamente com os cenários de uso?

O documento de consulta pública acerta ao apontar as falhas de segurança em diferentes camadas (interface web insegura, autenticação e autorização insuficientes, serviços de rede, ausência de transporte seguro, interface com nuvem, interface móvel, configurações de segurança, software e firmware, segurança física) e que a "segurança e a privacidade devem ser blocos essenciais de qualquer modelo de referência para o IoT".

Segundo modelo proposto pela União Internacional de Telecomunicações – camada de "capacidade de segurança" com enfoques distintos em aplicação, rede e dispositivos –, temos os seguintes desafios a serem enfrentados no Brasil da perspectiva de proteção dos consumidores.

Confidencialidade dos dados e proteção à privacidade: o Brasil ainda possui um grave vácuo normativo pois não há uma lei geral de proteção de dados pessoais. Apesar da existência de diversas normas setoriais (telecomunicações, setor bancário, saúde) e do Marco Civil da Internet (Lei 12.965/14), não há uma definição conceitual sobre dados pessoais (se incluem os metadados), dados sensíveis, consentimento, nem há uma definição clara dos princípios que devem reger as práticas de coleta, tratamento e processamento de dados pessoais. Sem dúvidas, entre os desafios de implementação da chamada "camada de capacidade de segurança" está a criação de incentivos para o setor privado, punindo aqueles

que descumprem as regras de proteção à privacidade. Por tal motivo, o Idec defende a aprovação de uma legislação que ofereça a devida tutela aos consumidores e consiga, ao mesmo tempo, estimular o desenvolvimento de melhores práticas e códigos de regulação elaborados pelos próprios atores privados, sendo posteriormente validados pela Autoridade de Proteção de Dados Pessoais em um sistema de corregulação. É preciso, também, garantir enforcement aos artigos 11 e 12 do Marco Civil da Internet, sob pena de criar um regime regulatório frouxo, onde há incentivos para aqueles que descumprem os deveres de proteção de dados pessoais e privacidade.[4] A discussão sobre medidas de segurança também não pode estar desconectada com o princípio básico de direito à informação, assegurado pelo Marco Civil no art. 10, parágrafo 4: "As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento".

Atualizações e vulnerabilidade: Como identificado pela FTC em 2015, um dos problemas graves consiste na falta de incentivos para que empresas promovam a atualização dos dispositivos e promovam a correção de vulnerabilidades quando há um alto custo para determinado agente econômico (fornecedor). Será preciso pensar, a partir das ferramentas jurídicas existentes no Código de Defesa do Consumidor, em processos de *recall* e obrigatoriedade de fornecedores de promoverem atualizações em seus sistemas para que haja menos risco aos consumidores e garantia da devida confidencialidade de dados. Um segundo aspecto importantíssimo – e que colabora para a formação dos incentivos corretos para os fornecedores – é a manutenção da regra de responsabilidade solidária por lesão causado ao consumidor na cadeia de tratamento de dados pessoais. Sem a regra de responsabilidade solidária (tal como defendido por determinados setores organizados da indústria, em completa oposição ao direito consumerista), os incentivos serão altos para baixo compliance às regras de segurança.

Dispositivos, ataques e franquias: há, por fim, uma grande preocupação com relação à vulnerabilidade de dispositivos que podem ser utilizados como instrumentos para spams ou ataque do tipo "denial of service". O relatório de 2015 da FTC é enfático ao apontar os vários casos em que dispositivos são hackeados e colocados à serviço desses grupos. No contexto brasileiro, esse fator de risco merece especial atenção, pois há aqui uma ameaça grave ao consumidor caso o modelo de precificação do acesso à Internet por "consumo mensal" de dados trafegados seja autorizado pela Agência Nacional de Telecomunicações. Imagine o caso

[4] Sobre o problema de enforcement no caso dos termos de uso do WhatsApp, ver: Idec, *Consentimento Forçado?*. São Paulo: Idec, 2016. Disponível em: https://www.idec.org.br/pdf/relatorio-whatsapp-termos-de-uso.pdf

hipotético em que uma "geladeira inteligente" (capaz de catalogar os produtos dentro dela e realizar pedidos em lojas virtuais de supermercados de forma automática) é atacada e transformada em instrumento para ataque do tipo DDoS, gerando intenso tráfego de dados. Imagine agora que esse consumidor – o proprietário da "geladeira inteligente" conectada ao seu wi-fi doméstico – possui um plano de acesso à Internet com uma franquia mensal de 100GB, sendo rapidamente utilizada, sem seu conhecimento, pela geladeira. Será preciso pensar não somente nos padrões de segurança adequados, mas também nas regras de responsabilidade em caso de lesão ao consumidor por negligência do fornecedor. Em um cenário de franquias de dados na Internet fixa, esse cenário torna-se dramático para o consumidor.

3. Uso de criptografia e padrões de segurança

Quanto a criptografia, embora ela seja técnica fundamental para se manter a segurança e a privacidade em dispositivos M2M/IoT, a grande maioria dos dispositivos possui limitações técnicas e de capacidade de processamento que dificultam a utilização de soluções de criptografia robustas. Desse modo, quais algoritmos e soluções de criptografia devem ser incentivados em dispositivos M2M/IoT para garantir eficiência e segurança no ecossistema?

O Idec não possui condições de oferecer respostas técnicas sobre a capacidade de processamento de dados que dificultam ou facilitam a utilização de criptografia, porém há questões fundamentais que se relacionam à criptografia e direito dos consumidores no Brasil que precisam ser comentadas.

É crucial que o Decreto 8771/2016 seja mantido e tenha normatividade plena no sistema jurídico brasileiro. No art. 13, já existe uma regra que impõe que os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as diretrizes sobre padrões de segurança. Primeiro, deve existir estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades de pessoas que terão possibilidade de acesso e de privilégio de acesso exclusivo para determinados usuários. Segundo, a previsão de mecanismos de autenticação de acesso aos registros, usando sistemas de autenticação dupla para assegura individualização do responsável pelo tratamento dos registros. Terceiro, criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações. Quarto, uso de soluções de gestão dos registro por meio de técnicas que garantam a inviolabilidade dos

dados, como encriptação ou medidas equivalentes. Existe, portanto, base legal para encriptação/criptografia, que deve estar presente no plano nacional em discussão.

Além disso, o Idec defende que as informações sobre os padrões de segurança adotados pelos provedores de aplicação devem ser divulgadas de forma clara e acessível a qualquer interessado por meio de seus sítios na Internet. No caso de dispositivos que não possuem interface de uso, deve ser obrigatório o envio de tais informações por meio físico e a publicidade de tais informações nas lojas de venda de tais produtos, tanto lojas físicas quanto lojas virtuais, em respeito ao Código de Defesa do Consumidor e ao Decreto de regulamentação do Marco Civil da Internet. As informações sobre criptografia devem ser claras ao consumidor, havendo, se possível, vídeos interativos que facilitem a compreensão do modo de funcionamento das soluções de criptografia adotadas.

Por fim, o estímulo ao uso de criptografia não deve ser visto como incentivo para criação de soluções técnicas para interceptação de dados, como "backdoors". O Supremo Tribunal Federal realizará em breve audiência pública sobre o tema, sendo razoável que qualquer elaboração normativa em sede de política pública tenha como base as interpretações do STF sobre legalidade e validade de técnicas criptográficas, como, por exemplo, a utilização do Protocolo Signal (criptografia ponta-a-ponta)[5].

4. Cooperação e ataques de negação de serviço

Conceitualmente, o ecossistema de IoT exige a cooperação e compartilhamento de informações entre seus agentes, em especial para se ter uma rápida divulgação de vulnerabilidades de *software* que possam comprometer a segurança de toda a rede. Como desenvolver um ambiente de cooperação entre os agentes do ecossistema de M2M/IoT? Em especial, como prevenir os riscos de ataques de negação de serviço massivos implementados através de redes de dispositivos M2M/IoT?

Conforme defendido por outras entidades que integram a Coalizão Direitos na Rede, a cooperação para prevenção de ataques de negação de serviço passa necessariamente pela integração do Brasil em fóruns internacionais de CyberSegurança e o fortalecimento do projeto de manutenção e criação dos Centros de Resposta a Incidentes de Segurança.

[5] Ver nota técnica do Idec sobre criptografia ponta-a-ponta do WhatsApp: http://www.idec.org.br/pdf/criptografia_whatsapp.pdf

Acima de tudo, é prioritário o apoio ao CERT.br – Grupo de Resposta a Incidentes de Segurança para a Internet brasileira –, mantido pelo NIC.br, do Comitê Gestor da Internet.[6] De acordo com decreto de regulamentação do CGI.br, o CERT, como integrante do Comitê Gestor, possui como atribuições estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet, promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para a segurança das redes e serviços de Internet, bem como pela adequada utilização pela sociedade, bem como ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet.

O CERT.br tem, desde sua formação, uma lógica de trabalho colaborativo com outras entidades, como outros CSIRTs, empresas, universidades, provedores de acesso e serviços Internet e backbones. É inadequado atribuir essa função de cooperação e prevenção de incidentes de segurança a outro ator, ou duplicar estruturas institucionais semelhantes. O Idec entende que o sistema de cooperação desejado pelo plano nacional passa necessariamente pelo fortalecimento do Comitê Gestor da Internet, do NIC.br e do CERT.br.

O CERT.br também possui um papel importante de diálogo com a Secretaria Nacional do Consumidor. Na última apresentação realizada por Cristine Hoepers em nome do CERT.br no Seminário de Privacidade do CGI, foram discutidos casos práticos como (i) a criptografia fraca das lâmpadas Phillips Hue LED (que permitem descobrir a senha do wi-fe e controlar remotamente as lâmpadas), (ii) o envio de informações das TVs Samsung para a sede (nomes de arquivos, drives de rede, etc) e (iii) carros da Fiat Chrysler que permitem o controle do veículo via 4G com vulnerabilidades do sistema Uconnect. Esse trabalho deve ser estimulado, fortalecendo o Sistema Nacional de Defesa do Consumidor.

5. Big Data e proteção de dados pessoais

No que tange a privacidade e proteção de dados pessoais, além das vulnerabilidades já mencionadas é importante ter em mente que o ecossistema de M2M/IoT poderá potencializar os negócios com *big data*, em especial com empresas interessadas em monetizar bases de dados, seja para fins publicitários ou outras destinações. Essas bases de dados podem possuir dados pessoais individualizados ou dados agregados/anonimizados sobre indivíduos. Nesse cenário, ciente da coleta e comunicação de dados potencializada pelo desenvolvimento do ecossistema de M2M/IoT, qual a abordagem legal, existente ou a ser implementada, necessária para proteger a privacidade e os dados pessoais dos indivíduos? Como deve ser tratada a coleta de dados de sensores IoT? Existem experiências estrangeiras

[6] O CGI.br também tem produzido excelente videos sobre Internet das Coisas: https://www.youtube.com/watch?v=jlkvzcG1UMk

que lidam com o binômio desenvolvimento e proteção à privacidade dos indivíduos no ecossistema M2M/IoT? Os projetos de lei em trâmite no Congresso Nacional referentes a proteção de dados pessoais (PL 4060/2012 da Câmara dos Deputados, PL 330/2013 do Senado e PL 5276/2016 de Autoria do Executivo) possuem regras adequadas para lidar com esse cenário e ao mesmo tempo possibilitar o desenvolvimento do ecossistema de M2M/IoT? É possível desenvolver dispositivos M2M/IoT com "políticas de privacidade" embarcadas, de modo a possibilitar a comunicação entre dispositivos com políticas compatíveis?

Conforme defendido publicamente em diversas audiências públicas e textos de posição, o Idec entende que o Projeto de Lei (PL) n. 5276/16 é o que melhor oferece proteção jurídica aos consumidores, oferecendo o nível adequado de tutela à privacidade e proteção de dados pessoais, conforme redação atual. Os PLs 4060/12 e 330/13 são incompletos e desbalanceados, criando sistemas frouxos e benéficos à indústria de tratamento e monetização de dados pessoais.

O PL 5276/16 segue uma tendência mundial de realizar uma separação entre dado "anônimo" e dado "pseudo-anônimo", ou seja, aquele que é capaz de ser "de-aninomizado" a partir de um conjunto de regras razoáveis empregados pela indústria em determinado momento de desenvolvimento técnico. Assim como estipulado na nova Diretiva de Proteção de Dados Pessoais da União Europeia, se os dados forem de-anonimizados com certa facilidade a partir de processos de reidentificação e análise agregada, então passam a ser considerados dados pessoais – aplicando-se regras mais rigorosas. Se o processo de de-anonimização for extremamente custoso e de difícil realização, podem ser explorados com regras menos rigorosas, sem aplicação do sistema principiológico criado no PL 5276/15.

O PL 5276/16 também é superior por utilizar como fundamento central a "autodeterminação informativa", ao lado da defesa do consumidor. Tal princípio centra-se na ideia de que o consumidor de um dispositivo conectado – assim como o consumidor off-line que está simplesmente comprando um medicamento na farmácia – possui o direito de determinar como seus dados serão coletados e processados. Essa determinação depende de informações claras a respeito da coleta e do consentimento expresso, livre e informado sobre a coleta de tais dados.

Conforme analisado por diversos especialistas no Brasil – entre eles, Renato Monteiro, Bruno Bioni, Danilo Doneda e Laura Mendes –, o PL 5276 possui inovações jurídicas relevantes, como o direito de saber quando dados foram hackeados, o dever de tratamento e processamento de dados conforme "legítimo interesse", a obrigatoriedade de design de dispositivos com enfoque em privacidade (*privacy by design*), a obrigatoriedade de produção de relatórios de impacto e a criação de postos de trabalho específicos como *Oficiais de Proteção de Dados* (para empresas com grande número de funcionários).

É importante lembrar que os princípios gerais do PL 5276/15 não diferem muito dos *Fair Principles* adotados nos Estados Unidos da América em 1973 e dos princípios presentes na nova Diretiva de Proteção de Dados Pessoais do Parlamento Europeu, baseados nos princípios da OCDE de 1980 e na Diretiva de 1995. Assim, a garantia da moldura jurídica construída no PL 5276/15 não configura obstáculo à inovação, estando bastante alinhada com os desenvolvimentos jurídicos recentes.

O consumidor precisa estar devidamente informado das políticas de privacidade dos diferentes dispositivos conectados. Por tal motivo, o Idec considera como extremamente relevantes as sugestões feitas pelo *Federal Trade Commission* (FTC) de que as empresas devem garantir as informações de privacidade por diferentes formas: seja por meio de códigos QR ("QR Codes") que podem ser facilmente compreendidos pelos consumidores, por meio de instruções em vídeo antes de utilização de um dispositivo ou por meio de "privacy dashboards" que devem ser construídos fisicamente nas lojas onde o consumidor adquire um produto (um sistema de iluminação inteligente).

O Idec manifesta-se contrário à flexibilização das regras de proteção de dados pessoais sob o argumento de que "é preciso fomentar a inovação e desenvolvimento da indústria local"[7]. O Idec também é frontalmente contrário a termos de uso generalistas, que permitem a ampla coleta de dados pessoais de consumidores. O Instituto defende incentivo às melhores práticas de *privacy by design* – por meio de premiações e incentivos fiscais – e amplo controle regulatório sobre os princípios da finalidade legítima e princípio da necessidade.

[7] O Idec combateu publicamente o lobby empresarial feito em setembro de 2016 com a publicação do "manifesto pela lei de proteção de dados pessoais", que propõe a deformação do PL 5276/15 em vários pontos: http://www.idec.org.br/ckfinder/userfiles/files/Posic_a_o%20do%20Idec_Dezembro%20de%202016.pdf