Revista Brasileira de Direito e Gestão Pública
www.gvaa.com.br/revista/index.php/RDGP/
ISSN: 2358-2405

Anonimização de dados como garantia ao direito à privacidade na internet das coisas (internet of things-IoT)

Data anonimization as a guarantee to the right to privacy on the internet of things (internet of things-IoT)

Marina Santos[1], Norma Cerqueira[2] e Rayssa Meneghetti[3]

v. 8/ n. 5 (2020)
Novembro

Aceito para publicação em 05/09/2020.

[1]Graduanda do Curso de DIREITO da Faculdade de Minas-BH. E-mail: marina-ferrazl@hotmail.com;

[2]Graduada pelo Curso de DIREITO da Faculdade de Minas-BH. E-mail: normacerqueira01@outlook.com;

[3]Mestra e Doutoranda em proteção dos direitos fundamentais pela Universidade de Itaúna-UIT. E-mail: rayssa-rm@hotmail.com;

https://www.gvaa.com.br/revista/index.php/RDG

Resumo

A presente pesquisa tem por objetivo analisar a forma como os dados são utilizados, bem como ponderar acerca do direito à privacidade dos usuários desses produtos e a necessidade de preservar também o desenvolvimento tecnológico. Nesse sentido busca trazer algumas técnicas da anonimização de dados com intuito de encontrar um equilíbrio entre os pontos acima mencionados. A problemática gira em torno das seguintes perguntas: os produtos ligados à internet das coisas só poderão ser colocados no mercado quando os riscos forem previsíveis? As empresas poderão tratar os dados dos consumidores de forma indiscriminada? O método utilizado foi o dedutivo, por meio da técnica teórico-bibliográfica, seguindo uma estrutura lógica de raciocínio, com o objetivo de atingir os resultados propostos na problemática apresentada.

Palavras-chave: direitos da personalidade, gestão de dados, surveillance, segurança na internet.

Abstract

The present research aims to analyze the way data are used, as well as to consider the right to privacy of users of these products and the need to preserve technological development as well. In this sense, it seeks to bring some techniques of data anonymization in order to find a balance between the points mentioned above. The problem revolves around the following questions: can products connected to the internet of things only be placed on the market when the risks are predictable? Will companies be able to handle consumer data indiscriminately? The method used was the deductive, through the theoretical-bibliographic technique, following a logical structure of reasoning, with the objective of achieving the results proposed in the presented problem.

Keywords: personality rights, data management, surveillance, internet security.

1. Introdução

Conforme a LGPD (Lei Geral de Proteção de dados) os dados anonimizados são aqueles que não possibilitam a identificação do seu titular. Esse procedimento é de extrema importância para garantir o desenvolvimento dos dispositivos ligados à Internet das Coisas e o direito à privacidade de todos os usuários dessa tecnologia.

O conceito de internet das coisas (IoT), possui algumas divergências, mas, basicamente, pode ser entendido como os objetos que interagem com outros, processam informações e dados e podem ser controlados através de uma conexão de rede e acaba facilitando o dia a dia das pessoas. Como exemplo, podem ser citados os aparelhos que executam músicas, verificam a previsão do tempo, estabelecem um diálogo com seus proprietários, entre outras tarefas, tudo através do comando de voz.

Um ponto relevante nesses dispositivos IoT é a quantidade de dados que eles são capazes de gerar e o risco que eles criam ao direito à privacidade e à intimidade de seus usuários.

No cenário da Internet das Coisas (IoT) tem-se várias empresas que fabricam diversos dispositivos que estão ligados ao universo da internet e que são capazes de colher inúmeros dados pessoais de seus usuários e que, em sua maioria, não dispõem de um sistema de segurança adequado para impedir que haja futuras violações, logo é indispensável que sejam estabelecidos limites e regras para resguardar os direitos de ambas as partes dessa relação, tanto o consumidor, quanto o fornecedor.

O Código de defesa do consumidor prevê que os produtos e serviços disponibilizados no mercado de consumo não acarretem risco à segurança das pessoas, entretanto no cenário dos dispositivos ligados à Internet esse risco nem sempre será previsível.

Como esses dispositivos tendem a estarem cada dia mais presentes em nosso cotidiano, é de extrema importância que sejam levadas em consideração a proteção e a privacidade do consumidor, preservando sempre o desenvolvimento tecnológico.

Diante de tudo isso, a anonimização de dados mostra-se como uma saída eficaz na garantia do equilíbrio entre o direito dos consumidores desses produtos e o desenvolvimento dessas tecnologias, possibilitando uma maior liberdade e segurança dos usuários.

Os dispositivos ligados à Internet estão cada vez mais presentes no dia a dia das pessoas e sempre estão em constante desenvolvimento, logo, é essencial que o direito consiga acompanhar toda essa dinamicidade.

É necessário que seja encontrado um equilíbrio entre os direitos dos consumidores dessas inovações e o direito dos desenvolvedores e fornecedores, para que nenhum seja prejudicado.

Dito isso, destacam-se os seguintes problemas a serem respondidos a partir da presente pesquisa: Os produtos ligados à internet das coisas só poderão ser colocados no mercado quando os riscos forem previsíveis? As empresas poderão tratar os dados dos consumidores de forma indiscriminada?

A escolha do tema justifica-se pela extrema importância da discussão acerca da segurança e proteção do direito fundamental à privacidade, para garantir que ambas as partes dessa relação sejam resguardadas, possibilitando uma maior liberdade dos usuários desses produtos ligados à internet.

2. Metodologia

O método utilizado para a realização da presente pesquisa foi o dedutivo, por meio da metodologia teórico-bibliográfica, com ênfase na análise da literatura jurídica e da legislação referente à matéria, seguindo uma estrutura lógica de raciocínio, com o objetivo de atingir os resultados propostos na problemática apresentada.

3. Resultados e Discussão

A internet das coisas (IoT) possui alguns conceitos, entretanto, poderá ser entendida fundamentalmente como os diversos dispositivos que se conectam uns aos outros e que estão ligados à internet. Nas palavras do autor Eduardo Magrini, em seu livro Entre dados e Robôs:

> A Internet das Coisas (Internet ofThings — IoT) é a expressão que busca designar todo o conjunto de novos serviços e dispositivos que reúnem ao menos três pontos elementares: conectividade, uso de sensores e capacidade computacional de processamento e de armazenamento de dados. (EDUARDO MAGRINI, 2019, p.19)

Essas inovações tecnológicas estão cada vez mais presentes no cotidiano das pessoas, e a tendência é que com o passar dos anos a maior parte[1] da população tenha acesso a algum tipo de

[1] (...) 25 bilhões - ou três para cada pessoa no planeta - até o final de 2020. (...) No ano passado, a Cisco, que deveria lidar com esse tipo de dados tão bem quanto qualquer outro, previu que o dobro de dispositivos, cerca de 50 bilhões,

aparelho ligado a IoT. São nítidos os benefícios e comodidades advindas desses objetos, entretanto é necessário considerar os perigos a que os consumidores estão expostos ao fazerem uso dessas máquinas, já que a quantidade de dados coletados diariamente por cada dispositivo tende a colocar em risco direitos fundamentais, como a intimidade.

A utilização de dados é um fator de extrema relevância para a criação e desenvolvimento de uma empresa, o uso de informações auxilia nas diversas[2] tomadas de decisões dos empreendedores. Em especial nas estratégias de marketing, que em sua maioria, são criadas a partir de uma análise de dados pessoais, de inúmeros de indivíduos, que permitem a obtenção de resultados mais precisos e lucrativos para esses negócios.

Conforme a Lei Geral de Proteção de Dados Pessoais - (LGPD), que deverá entrar em vigor em 2021, os dados pessoais, são aqueles que permitem uma ligação com o seu titular, já os dados pessoais sensíveis são aqueles que tratam sobre informações íntimas de usuários, como por exemplo dados sobre saúde, etnia, origem racial, opiniões políticas, dados genéticos entre outros previstos no art 5º, II, da LGPD.

É importante entender que nem todas as informações serão consideradas pessoais, já que para isso ocorrer, é necessário a existência de um vínculo com o seu titular, ou seja, que a partir dessa informação seja possível a identificação de uma pessoa natural, nesse sentido temos o seguinte entendimento do autor Danilo Doneda:

> A informação pessoal, aqui tratada, deve observar certos requisitos para sua caracterização. Determinada informação pode possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela. Este vínculo significa que a informação se refere às características ou ações desta pessoa, que podem ser atribuídas a ela em conformidade à lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como sobre opiniões que manifesta e tantas outras. (DONEDA, 2011, p.93)

É indiscutível a necessidade da utilização de dados pessoais nos dias atuais, como base para a tomada de decisões em vários negócios, bem como para o desenvolvimento de dispositivos

deve ser conectado até o final de 2020.COLIN BARKER. Disponível em: https://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-internet-of-things/. Acesso em: 26 de maio de 2020.

[2] Os dados são a base para todos os tipos de análises dentro de uma empresa, sejam elas preditivas — ou seja, que têm como objetivo prever tendências a partir de determinado fator, como o crescimento estimado da empresa dentro de um período de três anos — ou não-preditivas, como identificar qual período obteve o melhor faturamento dentro dos doze meses anteriores, ou constatar o desempenho e a produtividade de um dos setores de dentro da empresa. Qualidade de dados: o que é e qual a importância para negócios?. GS1 Brasil: Associação Brasileira de Automação, 2017. Disponível em: https://blog.gs1br.org/qualidade-de-dados-o-que-e-e-qual-a-importancia-para-negocios/. Acesso em: 01 de agosto de 2020.

ligados à Internet das coisas, entretanto, a coleta de forma indiscriminada e o tratamento inadequado podem gerar uma série de consequências para os titulares desses dados, violando diversos direitos assegurados constitucionalmente.

Como a Lei 13.709/2018 (Lei Geral de Proteção de Dados) teve a sua *vacatio legis* ampliada, com a publicação da Medida Provisória 959/2020 no dia 29 de abril de 2020, o Brasil ainda não possui em vigor nenhuma regulamentação acerca da proteção de dados pessoais. Entretanto, a falta de regulamentação não impede que haja uma aplicação das garantias constitucionais para resguardar o direito dos integrantes das relações de consumo que envolvam produtos ligados a IoT. Nesse sentido, entende Bruno Miragem:

> Por outro lado, na falta desses instrumentos, é impostergável que as situações que envolvam já essas novas tecnologias devem encontrar no jurista a prudência necessária para bem aplicar o Direito posto em soluções que equilibrem o desenvolvimento tecnológico e a liberdade da ciência, com a proteção da pessoa humana em relação aos novos riscos da vida comunitária. (MIRAGEM, 2017)

O artigo 5º, inciso X, da Constituição da República, garante aos brasileiros a inviolabilidade da intimidade e da vida privada, assegurando, ainda, o direito à indenização nos casos em que existam violações. Com o passar dos anos, e com o desenvolvimento das tecnologias, essas garantias constitucionais passam a ser analisadas sob uma óptica de garantir direitos no âmbito da gestão de dados pessoais. Nesse sentido, entende Rita Ferreira (2018, p.27) que é "interessante notar que o direito ao respeito à privacidade tem cada vez menos relação com o segredo e mais proximidade com o controle da pessoa sobre os seus dados."

Um ponto importante a ser ressaltado é sobre a coleta de dados de forma indiscriminada, que permite no âmbito das relações de consumo o que é entendido como "publicidade comportamental" e que fere a privacidade das pessoas, já que os dados coletados por meio desses dispositivos são utilizados sem o conhecimento do consumidor, para realização de publicidades de forma mais convenientes e convincentes. Nesse sentido, diz Danilo Doneda:

> A publicidade comportamental utiliza-se, naturalmente, de informações sobre o comportamento de uma pessoa para que lhe seja especificado o tipo de abordagem que seria o mais adequado. Hoje, com a grande penetração da rede Internet, uma das fontes de dados mais visadas para a obtenção de dados que permitam estabelecer o "perfil" de um consumidor a partir do seu comportamento é justamente o conjunto de hábitos de sua navegação na Internet (...) a publicidade comportamental (behavioraladvertising) representa a fronteira na qual se desenvolvem as novas tecnologias de abordagem do consumidor a partir da utilização intensiva de informações pessoais a seu respeito. Seus efeitos devem ser cuidadosamente assimilados pela prática consumerista pois, além do risco concreto de ampliar a assimetria informacional na relação de consumo, soma-se uma boa parcela de

> outros riscos inerentes à utilização de dados pessoais, refletindo na potencial discriminação entre consumidores, na relativização da idéia de escolha livre e outros. (DONEDA, 2010, p.62)

Acerca da coleta indiscriminada de dados o autor Elias Jacob de Menezes Neto (2016) explica o conceito e aplicação do termo *Surveillance*, que em uma tradução livre seria "vigilância". Para o autor, o conceito supera a mera vigilância. Não se trata apenas de uma questão quantitativa – mais informações, e sim qualitativa – quais informações. O objetivo desse mecanismo é sistematizar a coleta, o armazenamento, o processamento, a individualização, a combinação e a classificação das informações sobre determinadas pessoas e/ou grupos, para serem usadas oportunamente, com o propósito de influenciar ou gerenciar aqueles que tiveram os dados coletados. Para o autor:

> (...) acaba ocorrendo um desvio daquilo que se entende como privacidade, que deixa de ser considerada um direito fundamental para se transformar uma moeda de troca virtual (...)Isso é facilmente percebido através da proliferação de diversas empresas gratuitas de busca, redes sociais, e-mails etc., onde os serviços são pagos através da exploração das informações privadas dos usuários. (MENEZES NETO, 2016, p.220)

Diante do acima exposto, é nítida a necessidade de uma delimitação da coleta de dados pessoais, bem como a adoção de técnicas que assegurem a privacidade dos usuários, já que os dispositivos ligados à internet das coisas representam um risco, pela quantidade de dados que são capazes de coletar, e muitas das vezes pela falta de expertise técnica das empresas fabricantes desses dispositivos em assegurar futuras falhas nesses objetos.

Embora o Código de Defesa do Consumidor, em seu artigo 8º, limite o fornecedor a colocar no mercado apenas produtos que não acarretem risco à saúde ou segurança do consumidor, é questionável que existam apenas riscos convencionais e previsíveis. Nesse sentido dispõe Bruno Miragem:

> Esse estado de coisas resulta na própria reavaliação da extensão do dever de segurança dos produtos e serviços no mercado de consumo. A legislação brasileira é expressa ao limitar o fornecedor, indicando que coloque no mercado apenas produtos cujos riscos sejam normais e previsíveis (artigo 8º do CDC). A pergunta óbvia aqui será: todos os riscos destas novas tecnologias serão normais e previsíveis? (MIRAGEM, 2017)

Entretanto, uma forma de reduzir todos esses riscos, como também garantir a proteção dos direitos constitucionais dos consumidores e o desenvolvimento tecnológico, é a utilização de técnicas que possibilitam a anonimização de dados pessoais.

A anonimização de dados, objetiva que os dados pessoais, sejam eles sensíveis ou somente pessoais, não possam ser relacionados ao seu titular, protegendo assim a sua privacidade, dignidade, bem como a inviolabilidade da vida privada. O processo para anonimização de dados é composto por algumas técnicas, que conforme Bruno Ricardo Bioni (2020, p.61) "buscam eliminar tais elementos identificadores de uma base de dados".

Dentre as principais técnicas é possível encontrar a supressão, a generalização, a randomização e a pseudonimização.

A supressão é caracterizada pela retirada de uma coluna, uma parcela inteira de dados. Como exemplo, pode-se citar um campo preenchido com informações sobre idade, nome, sexo, endereço, e um produto que será adquirido, após a supressão ser realizada, permanecerão apenas os campos sobre o produto, e o sexo.

A generalização, consiste em retirar um dado mais específico, e transformá-lo em um dado mais genérico. Um exemplo pode ser visualizado em uma tabela com informações precisas sobre idade e endereço, com a generalização, essa tabela passará a constar apenas uma idade aproximada, ou faixa etária, e uma localização mais ampla, ou em regiões.

A randomização, poderá ser entendida como o mascaramento das informações com o uso de algum dado não original, sem prejudicar a análise das estatísticas, com o objetivo apenas de impedir que o usuário seja identificado. Como exemplo, temos uma tabela, com um produto, CEP e data de nascimento, com a randomização, os números desse CEP poderão ser alterados por outros.

A pseudonimização está prevista na LGPD, no parágrafo 4º do artigo 13º, e é um tratamento que impossibilita que um dado seja associado direta ou indiretamente a um usuário. Exceto por um controlador de dados com o uso de alguma informação adicional que é mantida em separado em um ambiente seguro. Na pseudonimização os dados serão separados em duas partes, entre os dados sensíveis, e os dados mais genéricos, sendo que os mais sensíveis deverão ser mantidos em um local seguro.

Além desses procedimentos, o *Guide to basic data anonymisation techniques* - Guia para técnicas básicas para anonimização de dados, publicado pela Comissão da Proteção de Dados Pessoais de Singapura (*Personal Data Protection Commission of Singapore*), em 25 de janeiro de 2018, traz outros métodos de anonimização de dados, como o encobrimento de caracteres, troca, agregação de dados entre outros.

É necessário salientar, que todas as técnicas acima mencionadas, possuem o mesmo objetivo, que é garantir a proteção dos dados, já que quando a desvinculação do dado ao seu titular

não é realizada, abre-se um grande leque de possibilidade de os dados serem tratados de forma inadequada, e com isso gerar uma serie de transtornos aos seus titulares, bem como a utilização desses métodos permite a garantia aos direitos constitucionais como a privacidade, a dignidade e o desenvolvimento de diversas tecnologias, como a Internet das Coisas (IoT).

4. Considerações Finais

Com base em todo exposto, o presente trabalho de pesquisa visou buscar uma solução acerca da problemática apresentada, qual seja, a garantia da proteção do direito fundamental à intimidade diante do avanço das novas tecnologias de armazenamento de dados, que são indiscriminadamente utilizados na captação de consumidores de diversos setores.

A internet das coisas está cada vez mais presente no cotidiano das pessoas e é cada vez mais comum encontrar dispositivos como máquinas de lavar programadas à distância pelo celular, *smart* TV's, relógios inteligentes, carros com assistentes de voz, entre outros, já que são criados para auxiliar a vida de seus adquirentes e a tendência é que ocupem cada vez mais a rotina de todos. O que deve ser levado em consideração, é que além dos benefícios e comodidades que esses objetos proporcionam, eles podem apresentar um risco à privacidade das pessoas, já que colhem milhares de informações que podem ser tratadas de forma inadequada, gerando uma série de consequências para os consumidores.

É imperioso considerar que os dispositivos ligados à IoT estão em constante desenvolvimento, logo, é muito difícil que todos os riscos que eles possam causar sejam previsíveis, ainda mais considerando que as empresas fabricantes nem sempre possuem um quadro de funcionários com expertise técnica para blindar esses dispositivos de futuros riscos, e, ainda, a coleta de dados de forma indiscriminada tende a expor os consumidores ao risco de seus dados serem usados indevidamente, entretanto, a adoção de técnicas para anonimização de dados, representa um grande avanço na garantia da segurança na Internet, possibilitando ainda, uma maior liberdade aos usuários e preservando diversos direitos assegurados constitucionalmente.

Dessa maneira, a hipótese apresentada girou em torno do entendimento de diversos autores e estudiosos sobre a temática, alavancando a possibilidade de criação de uma legislação capaz de proteger a intimidade do consumidor sem prejudicar o desenvolvimento tecnológico.

A conclusão a que se chega é que as tecnologias estão em constante desenvolvimento, portanto é necessário que sejam adotadas medidas que ajudem a superar e evitar a ocorrência de

danos com a captação e tratamento de dados pessoais; e a utilização das técnicas de anonimização de dados mostra-se uma excelente medida para que haja uma harmonização entre o desenvolvimento tecnológico e os direitos à privacidade, à liberdade e à igualdade dos usuários de todos esses produtos conectados à internet.

Referências

Associação Brasileira de Automação. GUIDE TO BASIC DATA ANONYMISATION TECHNIQUES. **Personal Data Protection Commission Singapore (PDPC)**, 2018. Disponível em: https://iapp.org/media/pdf/resource_center/Guide_to_Anonymisation.pdf. Acesso em: 01 de agosto de 2020.

BARKER, Colin. 25 billionconnected devices by 2020 to build the Internet ofThings. ZDNet, 11 nov. 2014. Disponível em: http://www.zdnet.com/article/25-billion- -connected-devices-by-2020-to-build-the-Internet-of-things. Acesso em: 13 de maio de 2020.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais** - A Função e os Limites do Consentimento. 2ª ed. Rio de Janeiro: Forense, 2020.

BLUM, Rita Ferreira. ***O Direito à Privacidade e à Proteção dos Dados do Consumidor***. São Paulo: Almedina, 2018.

BRASIL. **Escola Nacional de Defesa do Consumidor**. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010. Disponível em: https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf. Acesso em: 27 de maio de 2020.

DONEDA, Danilo. **A proteção dos dados pessoais como um Direito fundamental**, 2011. Disponível em: file:///C:/Users/W8/Desktop/Dialnet-AProtecaoDosDadosPessoaisComoUmDireitoFundamental-4555153.pdf. Acesso em 01 de agosto de 2020.

LASSALE, José Maria. **Ciberleviatan**: el colapso de la democracia liberal frente a la revolución digital. Barcelona: Arpa, 2019.

MAGRANI, Eduardo**. Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2ª ed. Porto Alegre: Arquipélogo Editorial, 2019.

MAGRANI, Eduardo. **A internet das coisas**. 1ª ed. Rio de Janeiro: FGV Editora, 2018.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENEZES NETO, Elias Jacob de. **SURVEILLANCE, DEMOCRACIA E DIREITOS FUNDAMENTAIS**: os limites do Estado na era do big data. Tese (Doutorado) – Programa de Pós-graduação em Direito da Universidade do Rio dos Sinos. São Leopoldo, 2016.

MENEZES NETO, Elias Jacob de; MORAIS, José Luis Bolzan de. **A fragilização do Estado-nação na proteção dos direitos humanos violados pelas tecnologias da informação e comunicação.** Rev. direitos fundam. democ., v.23, n.3, p.231. set/dez, de 2018. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1135/562. Acesso em 03/06/2020.

MIRAGEM, Bruno. **A Internet das Coisas e os riscos do admirável mundo novo**. Conjur. 2017. Disponível em: https://www.conjur.com.br/2017-mar-29/garantias-consumo-internet-coisas-riscos-admiravel-mundo. Acesso em: 21 de maio de 2020.

QUALIDADE DE DADOS: O QUE É E QUAL A IMPORTÂNCIA PARA NEGÓCIOS?. GS1 Brasil: Associação Brasileira de Automação, 2017. Disponível em: https://blog.gs1br.org/qualidade-de-dados-o-que-e-e-qual-a-importancia-para-negocios/. Acesso em: 01 de agosto de 2020.

RIO GRANDE DO SUL. Tribunal de Justiça. **EXPOSIÇÃO DE VÍDEO COM IMAGENS ÍNTIMAS**. Ap. 70070862073, Rel. Eugênio Facchini Neto, 2016). Disponível em: https://www.tjrs.jus.br/site/busca

solr/index.html?aba=jurisprudencia&conteudo_busca=ementa_completa. Acesso em: 21 de maio de 2020.

RODRIGUES, Juciana. **Anonimização como forma de proteção de dados**. ABRACD: Associação Brasileira de ciências de dados, 2020. Disponível em: https://abracd.org/anonimizacao-como-forma-de-protecao-de-dados/. Acesso em: 01 de agosto de 2020.

ZANATTA, Rafael A. F. **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, 2017. Disponível em:https://www.idec.org.br/ckfinder/userfiles/files/Contribuic%CC%A7a%CC%83o%20Pu%CC%81blica_%20Idec_%2006022017.pdf. Acesso em: 06 de maio de 2020.