

O USO DE DADOS PELO PODER PÚBLICO: A IDEIA DE UM *SMART GOVERNMENT* E SUAS POSSÍVEIS CONSEQUÊNCIAS

Giovanna de Carvalho Argôlo (IC) e Dra. Larissa Dias Puerta dos Santos (Orientadora)

Apoio: PIBIC Mackenzie

RESUMO

Neste artigo foi explorado sobre o uso de dados pessoais pelo poder público no Brasil, analisando suas possíveis vantagens, como é o caso dos *Smart government*, ou seja, a construção de governos mais inteligentes visando um aprimoramento nas políticas públicas e ainda, um governo mais eficiente que garanta uma segurança para todos seus cidadãos. Portanto, para que se consiga atingir esta finalidade, o governo brasileiro investe em diversas tecnologias, utilizando por exemplo, plataformas de interoperabilidade, que fazem a unificação de inúmeras informações. Contudo, foi feita uma ponderação observando seus possíveis benefícios, mas mostrando em contrapartida quais poderiam ser seus riscos. Dessarte conclui-se, a partir do método hipotético-dedutivo e diante de uma abordagem bibliográfica, que o uso incorreto desses dados pode colocar em risco diversos direitos, podendo citar a autodeterminação informativa, no qual, muitas vezes, usufruem dos dados pessoais e até mesmo de dados sensíveis das pessoas, sem que exista um breve consentimento das mesmas, podendo ser correlacionado a isso, a violação do direito a transparência, tendo em vista que inúmeras vezes a população não tem nem se quer noção da real finalidade deste aproveitamento. Existe, além disso, uma grande preocupação com a própria Lei Geral de Proteção de Dados Pessoais (LGPD) e com o direito à privacidade, uma vez que se tem uma vigilância massiva, e ainda no que diz respeito ao direito ao esquecimento, no tocante ao vazamento de dados.

Palavras-chave: Dados pessoais. Administração Pública. *Smart Government*.

ABSTRACT

This article explores the use of personal data by public authorities in Brazil, analyzing its possible advantages, such as the case of Smart government, that is, with the construction of smarter governments, aiming at an improvement in public policies and also in a more efficient government that guarantees security for all its citizens. Therefore, in order to achieve this purpose, the Brazilian government invests in various technologies, used for example, interoperability platforms, in which they unify numerous information. However, a consideration was made, noting its possible benefits, but showing in contrast what its risks might be. Thus, it is concluded, from the hypothetical-deductive method and in front of a bibliographical approach, that the incorrect use of this data can put at risk several rights, being able to mention

the informative self-determination, in which they often use personal data and even even sensitive data of people, without their brief consent, which may be correlated with the violation of the right to transparency, considering that, many times, the population has no idea of the real purpose of this use. There is, in addition, a great concern with the General Law for the Protection of Personal Data (LGPD) and with the right to privacy, since there is massive surveillance, and even the right to be forgotten, with regard to leakage of data.

Keywords: Personal data. Public administration. *Smart Government*.

1. INTRODUÇÃO

Com a 4ª Revolução Industrial a tecnologia promoveu uma série de transformações em todo o mundo, uma das mais evidentes foi a maior facilidade para coletar dados pessoais dos usuários, justamente porque o uso massivo de computadores pela população cresce cada vez mais. A maior parte das pessoas oferecem seus dados por diversos motivos, seja para fazer uma compra online ou para se cadastrarem em uma rede social, instituição, ou em diversas outras plataformas incessantemente. O fazem em muitas vezes de maneira involuntária cumprindo uma exigência para que a pessoa consiga ter acesso alguma informação ou serviço que necessita.

Aliado a isso, vários governos também usufruíram dessa facilidade que foi proporcionada pela tecnologia, visando uma simplificação em suas atividades, sendo assim, os mais variados dados que antes eram dados offline se transformaram em dados online, facilitando a coleta e tratamento destes. Os mais diversos órgãos públicos que antes eram apenas em espaços físicos e que antigamente era necessário se deslocar até o local para se obter alguma informação ou fazer algum procedimento, se tornaram digitais, e agora com apenas alguns “clicks” é possível fazer tudo o que se pretende em pouquíssimo tempo.

Destarte, os investimentos nessa área foram ampliados pelos governos nos meios digitais, com a criação de governos eletrônicos, contudo, existe ainda uma pretensão cada vez mais forte de se alcançar o que é denominado de *smart government*, ou ainda, governos inteligentes. Uma das formas de operacionalização acontece a partir de plataformas de interoperabilidade, que fazem a unificação de diversas informações dentro delas.

Esses dados serão usados para que se tenha uma melhoria nas políticas públicas, dando uma maior segurança para sua população. Todavia, o desconhecimento da concreta finalidade do tratamento deles é corriqueiro, o que não deveria ser, tendo até uma vigilância massiva e consequentemente a violação de numerosos direitos.

2. DESENVOLVIMENTO DO ARGUMENTO

2.1 O uso de dados e o *Smart government*, a questão da melhoria nas políticas públicas

A invisibilidade ou ainda a inconsciência do constante uso da tecnologia já permeia a vida de inúmeras pessoas, ademais a mesma possui a peculiaridade de ser onipresente, e é

nesse sentido que o termo “*Ubiquitous Computing*”¹ se encaixa, podendo ainda ser traduzido como computação ubíqua, cuja finalidade é que a sua utilização se torne tão involuntária, que se transfigure no âmago do ser humano.

Destarte, aliado a isso, a tecnologia também proporcionou a simplificação da coleta de dados, no qual, dados *off-line* que ficavam registrados nos mais variados órgãos públicos, em locais físicos e que dispunham em lautas pilhas de papeis, guardando diversificadas informações de seus cidadãos, se converteram também em dados *on-line*, pertencendo as heterogêneas plataformas do governo eletrônico, concernindo assim, ao ciberespaço², no qual, no governo brasileiro estas foram implementadas no ano 2000³, através do Decreto Presidencial de 3 de abril do mesmo ano, e com a colaboração das Tecnologias da Informação e Comunicação (TIC). Outrossim, existe também o governo digital, em que, foi concretizado no Brasil em 2015⁴, com intuito de tornar o vínculo com a sociedade de forma descomplicada, compreensível e mais eficaz, por meio dos serviços que oferece para os seus cidadãos, por intermédio das tecnologias digitais.

Deste modo, é de suma importância ressaltar que os dados pessoais estão sendo utilizados tanto pelo setor público quanto pelo privado, podendo ser usados tanto de forma benéfica, como é o caso do proveito visando uma maior segurança ou melhorias na administração pública, tendo a elaboração e a execução de políticas públicas, com um fim de fornecer uma melhor qualidade de vida para todos ou podem ser utilizadas de uma forma extremamente prejudicial, contudo, isso será abordado de forma mais aprofundada no próximo subtópico.

Em vista disso, tem como exemplo, do que foi aludido acima, o Decreto 10.046 de 2019, em que delibera sobre o compartilhamento de dados na esfera da administração pública federal, com a implementação do Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. No que tange a este Decreto, é possível ter diversas suposições sobre o mesmo, primeiramente, observando com um olhar mais positivo, nota-se que seu intuito é primar por um melhoramento na administração pública, tanto na questão de sua qualidade

¹ Cf., por todos, KÜHLING, Jürgen. Datenschutz und die Rolle des Rechts. In: STIFTUNG FÜR DATENSCHUTZ (Ed). Die Zukunft der informationellen Selbstbestimmung. Berlin: Erich Schmidt Verlag, 2016. p. 49.

² Termo cunhado por Willian Gibson, em seu livro Neuromancer, em 1984, sendo um espaço virtual, que de acordo com Cascais (2001), está palavra foi empregada para caracterizar o espaço constituído pela correlação de todas as bases de dados, das telecomunicações e das redes de computadores.

³ Informação retirada do governo digital (gov.br). acesso em: <https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital>

⁴ Informação retirada do governo digital (gov.br). acesso em: <https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital>

como em sua eficiência e ainda na oferta da simplificação de seus serviços, podendo observar o que está sendo elucidado em seu artigo primeiro⁵.

Por conseguinte, chama atenção a questão de que o governo pretende ter um aperfeiçoamento em suas atividades, simplificando-as para atingir esta finalidade, podendo até mesmo falar que almeja alcançar a ideia de um "smart government", que de acordo com Maria Alexandra Cunha, dispõe do seguinte entendimento:

Define-se, assim, um governo inteligente e integrado que possa oferecer os serviços que a cidade necessita, interagindo com todos os agentes públicos e privados. Para isso, é necessário que haja uso de tecnologia (infraestruturas, hardware e software) no contexto de processos inteligentes, com dados e interoperabilidade. Uma cidade inteligente assim se faz porque é um nó da rede urbana global. Um governo inteligente implica **colaboração: colaboração entre governos, colaboração público-privada e ainda colaboração com todos os diferentes atores locais na busca de objetivos compartilhados**. (CUNHA, *et al.*, 2016, p.32) (g.n.).

Neste mesmo livro, cita ainda, quais são os tipos de melhorias que devem ser feitas para se ter um governo mais inteligente, mencionando a "implantação dos modelos de e-government" (CUNHA, *et al.*, 2016, p.91), todavia, é de suma importância ressaltar que o e-gov não se circunscreve apenas a automação, contudo é marcada também por uma transformação da forma no qual o governo alcança seus propósitos, como aponta Abranson e Means, especificando o que foi elucidado com alguns exemplos:

O e-gov não se restringe a mera automação, mas envolve uma mudança na maneira com que o governo, pelo uso das TIC, atinge os seus objetivos, incluindo, assim, melhoria nos processos, aumento da eficiência, melhor governança, elaboração e monitoramento de políticas públicas, aumento da transparência. (ABRANSON; MEANS, 2001, apud GUSMÃO, 2018, p.11).

Considerando o final deste trecho, é possível notar que existe uma grande semelhança com os objetivos do Cadastro supramencionado, deste modo, pode-se dizer que o governo está visando chegar cada vez mais perto de um "smart government" e um dos seus primeiros passos é justamente a transformação em um governo mais tecnológico, ou seja, um governo eletrônico, ou ainda, um e-government.

⁵ "Art. 1º Este Decreto estabelece as normas e as diretrizes para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União, com a finalidade de:

I - simplificar a oferta de serviços públicos;

II - orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas;

III - possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais;

IV - promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e

V - aumentar a qualidade e a eficiência das operações internas da administração pública federal."

Ademais, observa-se que a interoperabilidade, detém um papel importante quando se refere a este assunto, no qual, no governo brasileiro, no ano de 2004 foi elaborada uma versão inicial do documento que se tratava sobre os padrões de interoperabilidade em governo eletrônico, denominado e-PING⁶. À vista disso, é imprescindível entender primordialmente, no que concerne a interoperabilidade, que de acordo com o IEEE (The IEEE Standard Dictionary of Electrical and Electronics Terms), pode ser explicada como: “a capacidade de dois ou mais sistemas ou componentes trocarem informação e usarem a informação trocada” (IEEE (1997). The IEEE Standard Dictionary of Electrical and Electronics Terms. 6th Edition. New York: Institute of Electrical and Electronics Engineers, apud, SOARES, 2009, p.60).

Por conseguinte, é exatamente um desses pontos abordados pelo Decreto, conseguindo analisar isso em seu art. 2º ⁷, e como já mencionado anteriormente esse compartilhamento de dados pelos órgãos e entidades, juntamente com esse mecanismo de interoperabilidade, tende a buscar uma agilidade no que se refere a prestação de políticas públicas, podendo enxergar isso a partir do que está disposto em seu artigo 3º.⁸ Ademais, no capítulo IV deste mesmo decreto, nomeado como: “DO CADASTRO BASE DO CIDADÃO”, vai abordar de uma forma mais detalhada sobre como funciona esse cadastro, no qual, em seu artigo 17º⁹ mostra um pouco sobre a composição do mesmo, referindo-se novamente aos componentes de interoperabilidade e ainda sobre a base integradora¹⁰.

Sobre o desenvolvimento de plataformas que integrem todos os serviços inteligentes da cidade, que também é considerada uma benesse quando são executadas em

⁶ Informação retirada do governo digital (gov.br). acesso em: <https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital>.

⁷ “Art. 2º Para fins deste Decreto, considera-se:

XVIII - interoperabilidade - capacidade de diversos sistemas e organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais troquem dados;”

XX - mecanismo de compartilhamento de dados - recurso tecnológico que permite a integração e a comunicação entre aplicações e serviços do receptor de dados e dos órgãos gestores de dados, tais como serviços **web**, cópia de dados, lago de **dados compartilhado e plataformas de interoperabilidade**;

XXI - plataforma de interoperabilidade - conjunto de ambientes e ferramentas tecnológicas, com acesso controlado, para o compartilhamento de dados da administração pública federal entre órgãos e entidades especificados no art. 1º;”

⁸ “Art. 3º O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes:

III - os mecanismos de compartilhamento, interoperabilidade e auditabilidade devem ser desenvolvidos de forma a atender às necessidades de negócio dos órgãos e entidades de que trata o art. 1º, **para facilitar a execução de políticas públicas orientadas por dados**;”

⁹ “Art. 17. O Cadastro Base do Cidadão será composto pela **base integradora** e pelos componentes de **interoperabilidade** necessários ao intercâmbio de dados dessa base com as bases temáticas, e servirá como base de referência de informações sobre cidadãos para os órgãos e entidades do Poder Executivo federal.”

¹⁰ De acordo com o Decreto 10.046, a base integradora é uma base de dados que integra os atributos biográficos ou biométricos das bases temáticas;

governos inteligentes, atentando-se para o que está disposto no artigo 2º, inciso VI e VII, e ainda o artigo 16, nos incisos III e IV, deste mesmo Decreto¹¹, observa-se então, que no caso do Cadastro base do Cidadão a plataforma vai reunir todos os dados do cidadão, desde seu CPF, sendo este considerado como um dado cadastral, até a maneira de andar, permanecendo dentro dos atributos biométricos e por um lado, isso é bem importante no tocante a questão da segurança pública, uma vez que, com dados unificados em apenas uma plataforma fica mais fácil conseguir identificar quem realmente é aquela pessoa que se pretende analisar, pois todas as informações da mesma, estarão reunidas, facilitando, por exemplo, quando se tem a ocorrência de um crime, observando todos os fatos ocorridos naquele momento e junto a isso, tem-se o potencial de fazer uma investigação mais aprofundada, conseguindo assim, chegar a uma conclusão mais assertiva de quem realmente é o criminoso.

À vista disso, sabe-se que a segurança pública é um direito extremamente importante para o exercício da cidadania, que segundo Valente:

a segurança pública é um direito fundamental que garante o exercício de todos os outros direitos da legislação brasileira, assegura o exercício da cidadania, fortalece o Estado Democrático de Direito, mantendo um estado de ordem, proteção e relativa ausência de perigo ao cidadão, que o ajuda na recomposição de sua vida (VALENTE, 2012, apud MINUSCOLI e de ALMEIDA, 2016).

Ela é um direito assegurado pelo ordenamento brasileiro, sendo tão valiosa que no preâmbulo da Constituição da República Federativa do Brasil de 1988 é considerada como um valor supremo da sociedade, estando prevista no caput de seu artigo 5º, pertencendo aos direitos fundamentais; no artigo 6º, em seu caput, sendo considerada como um direito social e ainda no caput de seu artigo 144, tratando especialmente da segurança pública. Outrossim, este direito fundamental é mencionado em algumas Convenções e Tratados Internacionais, como a Convenção Europeia dos Direitos do Homem, a Declaração Americana dos Direitos e Deveres do Homem, Declaração Universal dos Direitos Humanos e na Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica).

¹¹ “Art. 2º Para fins deste Decreto, considera-se:

VI - base integradora - base de dados que integra os atributos biográficos ou biométricos das bases temáticas;

VII - base temática - base de dados de determinada política pública que contenha dados biográficos ou biométricos que possam compor a base integradora;

“Art. 16. Fica instituído o Cadastro Base do Cidadão com a finalidade de:

III - viabilizar a criação de meio unificado de identificação do cidadão para a prestação de serviços públicos;

IV - disponibilizar uma interface unificada de atualização cadastral, suportada por soluções tecnológicas interoperáveis das entidades e órgãos públicos participantes do cadastro;”

Contudo, a segurança no Brasil precisa ser urgentemente fortificada, tendo em vista que o país tem um índice de homicídio semelhante aos países que estão em guerra, encontrando-se entre os 10% de países que possuem as maiores taxas de homicídio do mundo, como é demonstrado na dissertação de mestrado, intitulada como: *vigilância das forças de segurança através de câmeras de reconhecimento facial e o conflito com o direito à privacidade – Brasil e Portugal*”.

o Brasil está entre os 10% de países com maiores taxas de homicídio do mundo. Apesar de ter uma população equivalente a 3% da população mundial, o país concentra cerca de 14% dos homicídios do mundo. As taxas de homicídio brasileiras são semelhantes às de Ruanda, República Dominicana, África do Sul e República Democrática do Congo. (*vigilância das forças de segurança através de câmeras de reconhecimento facial e o conflito com o direito à privacidade – Brasil e Portugal*, apud CARVALHO, 2019, p. 7)

Em vista disso, com a finalidade de reduzir o índice de criminalidade, alguns países estão utilizando ferramentas de reconhecimento facial e o uso do sistema de CFTV¹², obtendo assim, resultados satisfatórios, como é o caso de Londres e da Índia.

Em Londres, a tecnologia de reconhecimento facial está sendo testada e já apresentou bons resultados. A polícia realizou os testes durante os dias de 17 e 18 de dezembro de 2018, com foco no comércio de natal, a fim de tentar identificar criminosos procurados. O resultado foram quatro prisões, sendo que duas das pessoas eram procuradas pela polícia, e as outras duas foram chamadas “prisões proativas” – uma por uma suposta ameaça de estupro e outra por um suposto delito de drogas (Corum, 2019, apud CARVALHO, 2019, p. 45).

Ao que se concerne a Londres, os testes com esse dispositivo são executados por meio de câmeras situadas em postes ou ainda em vans, usufruindo do software concebido pela empresa japonesa NEC, no qual, serve para fazer uma leitura facial das pessoas que transitam naquela região. Portanto, é somente a partir da utilização do banco de dados de fotos pertencentes à polícia que o software consegue fazer uma comparação com o rosto do sujeito, sendo assim, é necessário que os policiais analisem minuciosamente. Outrossim, a polícia de Londres evidencia que essa tecnologia não é autossuficiente para adotar uma decisão, este meramente filtra as faces dos prováveis suspeitos entre todos aqueles que se deslocam por aquela área, não obstante, faz-se mister a apreciação de um humano, deliberando quem será analisado. (Corum, 2019, apud CARVALHO, 2019, p.45).

¹² CFTV é uma sigla para Circuito Fechado de Televisão, originada da sigla em inglês que possui o mesmo significado da sigla CCTV (Closed Circuit Television), sendo assim, um sistema de monitoramento interno, efetuado a partir de câmeras distribuídas e conectadas a um sistema central, no qual concede as imagens por meio de monitores, desempenhando ainda a gravação desses registros. E são empregados, principalmente para monitoramento e vigilância. (Central CFTV, 2019).

Já no tocante a Índia, está também teve um resultado formidável na aplicação deste instrumento de reconhecimento facial, no entanto, a polícia indiana não desfrutou do mesmo, para aprisionar delinquentes, mas sim para o rastreamento de crianças desaparecidas. E, somente em quatro dias em que foi lançado esse nosso dispositivo na cidade de Nova Delhi, aproximadamente, 3.000 crianças desaparecidas conseguiram ser reconhecidas pelos policiais. (Cuthbertson, 2018, apud CARVALHO, 2019, p.45).

A tecnologia foi utilizada em cerca de 45.000 crianças em toda cidade, onde foram reconhecidas 2.930 crianças como desaparecidas. A Índia tem quase 200 mil crianças desaparecidas e cerca de 90 mil em várias instituições de cuidado infantil, sendo humanamente impossível, ou altamente improvável, localizar crianças conferindo fotos manualmente e combiná-las com as crianças localizadas nas ruas (Cuthbertson, 2018, apud CARVALHO, 2019, p.45).

Contudo, no Brasil as tecnologias de reconhecimento facial não estão sendo utilizadas com tanta frequência, por ser algo relativamente novo para o país, todavia, a mesma começou a ser aplicada no Rio de Janeiro e na Bahia, no carnaval de 2019, alcançando um êxito quanto aos seus efeitos. Isto posto, no Rio de Janeiro, foi feita a instalação de 28 câmeras no bairro de Copacabana, sendo que, nos dez primeiros dias do mês de março, foram encontradas oito pessoas que possuíam um mandado de prisão ou apreensão em aberto, deste modo, a polícia militar do Rio de Janeiro tenciona-se a expansão dessas câmeras que proporcionam o reconhecimento facial (Alves, 2019, apud CARVALHO, 2019, p.46). Já em Salvador, a partir de câmeras com esta mesma função e que foram implementadas em 42 portais de acesso aos seus circuitos de carnaval, um homem que também havia um mandado de prisão aberto e sendo investigado pela polícia por suspeitarem que este tinha praticado um homicídio, foi reconhecido e, a posteriori, preso. Faz-se mister destacar ainda que, mesmo estando maquiado e fantasiado, as câmeras tiveram o potencial de reconhecê-lo. (Redação Correio, 2019, apud CARVALHO, 2019, p.46).

Levando em consideração todos esses fatos já mencionados, a unificação dos dados pode ser considerada como um meio efetivo para garantia do direito a segurança.

2.2. A unificação dos dados dos cidadãos e suas possíveis consequências

A priori, poderia até mesmo dizer que o dado por si só não possui tanto valor, podendo até mesmo fazer uma analogia com um quebra cabeça, em que estes representam as peças e somente quando as mesmas são encaixadas corretamente, vislumbra-se a imagem por completo. O mesmo acontece quando se fornece um dado biométrico, por exemplo, como o nome civil ou social, a data de nascimento, a naturalidade, o sexo, entre outros, em que, uma

vez que esses são observados de forma isolada muitas vezes acabam não gerando uma elucidação tão nítida de quem realmente é a pessoa, no entanto, quando as “peças deste quebra-cabeça” são investigadas e unidas, obtém-se informações minuciosas sobre a vida da mesma e é por este motivo que pode-se afirmar que Clive Robert Humby está correto quando diz: *“Data is the new oil”*, ou seja, que os dados são considerados o “novo petróleo”, não somente pelo fato de ambos serem preciosidades e pelos seus altos valores econômicos, mas também pela questão de que do mesmo jeito que o petróleo precisa ser refinado, os dados também precisam ser investigados.

Ademais, costuma-se pensar que o fornecimento dos dados só é feito nas ocasiões em que o próprio titular os proporciona e com o seu consentimento, contudo, não é o que ocorre: ao nascer, o recém-nascido já fornece suas primeiras informações através da sua certidão de nascimento e ao longo de sua vida, terá, nas mais diversas oportunidades o armazenamento de seus dados, sobretudo no setor público, sendo que essas informações vão se fortalecendo gradativamente.

Portanto, conforme foi exposto no tópico acima, percebe-se que de um lado tem esse aspecto que dispõe de uma certa esperança, pela qual o governo aspira por uma governança mais adequada e uma melhor qualidade de vida para todos seus cidadãos, tendo em vista que, no Decreto citado anteriormente estabelece que tenha uma maior integração entre os órgãos e as entidades da administração pública, em que os mesmos poderão compartilhar dados de caráter biográficos, biométricos e cadastrais entre eles, por meio de uma plataforma de interoperabilidade¹³.

No entanto, esses dados podem ser utilizados de uma forma extremamente prejudicial, podendo citar o uso de dados sensíveis como forma de espionagem da vida das pessoas, tentando monitorar e controlar as mesmas, o que é denominado como “vigilância líquida” por Bauman e Lyon.

Vigilância líquida é menos uma forma completa de especificar a vigilância e mais uma orientação, um modo de situar as mudanças nessa área na modernidade fluida e perturbadora da atualidade. A vigilância suaviza-se especialmente no reino do consumo. Velhas amarras se afrouxam à medida que fragmentos de dados pessoais obtidos para um objetivo são facilmente usados com outro fim. A vigilância se espalha de formas até então inimagináveis, reagindo à liquidez e reproduzindo-a sem um contêiner fixo, mas sacudida pelas demandas de “segurança” e aconselhada pelo marketing

¹³ “Art. 2º Para fins deste Decreto, considera-se:

I - atributos biográficos - dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios;

II - atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar;

III - dados cadastrais - informações identificadoras perante os cadastros de órgãos públicos”

insistente das empresas de tecnologia, a segurança se esparrama por toda parte. (BAUMAN; LYON, 2013, p. 10).

Um exemplo do que foi supracitado, são os próprios sistemas que foram mencionados anteriormente, que é o CFTV e o reconhecimento facial, e estão sendo utilizados pela China. Sendo que de acordo com o BBC News, este país possui mais de 170 milhões de câmeras CFTV e mais 400 milhões prestes a serem instaladas, deste modo, dispõem-se do maior e mais moderno sistema de vigilância do mundo, estando habilitado para reconhecer os rostos das pessoas e instantaneamente correlacionar com informações presentes no banco de dados. Outrossim, é capaz também de discernir qual é o gênero, idade, etnia, relacionando ainda, a face dos seus cidadãos a suas informações pessoais, como por exemplo, quem são seus parentes, as pessoas com quem se mantinha em contato entre outros. E consoante ao representante da produtora de câmeras *Dahua Technology*, esses aparelhos conseguem relacionar o rosto de uma pessoa com uma identidade, analisando seus deslocamentos por uma semana, desta maneira, se tiver câmeras o bastante, é capaz de detectar com quem essas pessoas convivem. (BBC News, 2017, apud CARVALHO, 2019, p.43).

Já na cidade de Guiyang, na China, sua polícia detêm um registro digital com uma foto de cada habitante da cidade, assim sendo, o correspondente da BBC John Sudworth foi testar esse sistema de câmeras, no qual, os policiais introduziram a foto e os dados de Sudworth passando-se por um suspeito no sistema, e a partir daquele momento instaurou um alerta. Deste modo, John foi passear pela cidade e em apenas 7 minutos já estava sendo interrogado pela polícia. (Liu e Xiqing, 2017, apud CARVALHO, 2019, p.43).

Nesta mesma linha, um outro exemplo de tecnologia criada no país referido acima, é o Social Credit System (Sistema de Crédito Social), em que, segundo o State Council of China, ou ainda, Conselho de Estado da República Popular da China:

Esse sistema pretende atribuir a cada cidadão uma pontuação pessoal elaborada por um algoritmo concebido para interpretar uma série de dados relativos a ele. O objetivo, em suma, é identificar a boa conduta, a confiabilidade e a honestidade de cada cidadão para encorajar um comportamento positivo e penalizar aqueles que se comportam mal em relação à sociedade e ao Estado. O projeto, iniciado de forma experimental em 2010, foi oficialmente adotado pelo governo em 2014 e levará à definição de uma pontuação para cada cidadão chinês em 2020 (State Council of China, 2014).

Richeri, aduz que esse Sistema tem como objetivo avaliar qual é o grau de confiança que se pode ter de uma pessoa ou empresa, no qual, as pessoas que alcançarem uma boa pontuação irão desfrutar de algumas vantagens e aquelas que não conseguirem obtê-la serão penalizadas.

Um aspecto importante do Sistema é o uso pretendido e a disseminação das informações coletadas. Na verdade, a iniciativa deve permitir que todos conheçam o grau de confiabilidade de uma pessoa e de uma empresa; a classificação prevista será usada para dar a possibilidade de uma pessoa obter um empréstimo, ser contratada para um trabalho específico, viajar livremente para o exterior, obter ou ser excluída dos serviços públicos, para acessar lugares, manifestações e eventos. Aqueles que obtiverem uma pontuação maior que certo nível irá obter vantagens, enquanto aqueles que permanecerem abaixo serão penalizados. Dessa forma, de acordo com declarações oficiais, o Sistema permitirá construir um contexto judicial credível, formará uma opinião pública para a qual ser considerado confiável se tornará um fator de prestígio e fortalecerá a sinceridade sobre os negócios do Governo, no comércio e na sociedade em geral. Outro resultado esperado é a redução da corrupção, fraudes alimentares e o comportamento clientelista de autoridades locais. (RICHERI, 2019, p.21-22)

Mesmo que esse sistema tenha trazido alguns benefícios para a sociedade chinesa, este pode ainda ser utilizado como forma de uma vigilância em massa, no qual, o governo acaba tendo um poder enorme diante de seus cidadãos, tendo além do controle de sua população, a censura, e a supressão de opiniões e comportamentos críticos, como pode ser analisado no trabalho: “China: problemas emergentes e medidas para orientar a opinião pública e combater a dissidência”.

A possibilidade de que este Sistema tenha sido pensado não apenas como uma ferramenta para promover energias positivas e melhorar a sociedade, mas também como um poderoso meio de controle, ou possibilidade de, é um assunto atualmente em discussão, e terá uma ressonância crescente na web à medida que sua efetivação progride e todos podem verificar seu uso – e possivelmente o abuso – pela liderança no poder. Em conclusão, podemos, no entanto, sublinhar a percepção diferente que o projeto até agora despertou na China e no Ocidente. No primeiro caso, as pesquisas de opinião chinesas e ocidentais destacam o alto grau de aceitação do projeto pelos cidadãos chineses (Kostka, 2019; Minter, 2019): prevalece a opinião de que o Sistema de Crédito Social pode ser uma ferramenta positiva para melhorar o comportamento dos indivíduos, sua confiabilidade e, de maneira mais geral, a coesão social e a confiança dos chineses em seu país, suas instituições e sua liderança. Ao contrário, a opinião amplamente predominante na mídia ocidental (Kuhnreich, 2018) é que o Sistema de Crédito Social pode ser uma ferramenta poderosa para controlar indivíduos para reduzir, censurar e suprimir opiniões e comportamentos críticos e, em alguns casos, hostis ao Estado, ao Partido Comunista e ao atual governo do país. (RICHERI, 2019, p.23).

Ademais, o uso de reconhecimento facial, está trazendo alguns riscos em diversas questões, podendo até mesmo ser comprovados por meio de estudos que foram realizados. Um grande exemplo disso, é um estudo que foi realizado pelo National Institute of Standards and Technology, que segundo o artigo “regulação de sistemas de reconhecimento facial para fins de segurança pública no Brasil: riscos e desafios” foi feita uma investigação de 189 algoritmos de 99 desenvolvedores diversos, para observar qual seria a efetividade dos softwares de reconhecimento facial quando analisavam pessoas com idades, sexo e raças diversificadas, e portanto, o que se pôde concluir é que com relação as compatibilidades de

um para um, os índices de falsos positivos eram de 10 a 100 vezes mais aos asiáticos e afro-americanos em comparação com os caucasianos. (MAGALHÕES E GOMES, 2021, p.173)

Além disso, poderia citar mais alguns exemplos, sendo um deles o estudo que foi feito, examinando o uso de sistemas de reconhecimento facial da Microsoft, IBM e Face ++, chegando à conclusão que na maior parte, esses programas possuem um melhor desempenho em rostos masculinos quando comparados com os rostos femininos, no qual, possui uma diferença nas taxas de erro de 8.1% - 20.6%, o mesmo acontece com pessoas com a pele clara com relação aquelas que possuem uma pele escura, em que, as taxas de erro são de 11.8% - 19.2% de diferença. (BOULAMWINI e GEBRU 2018, p. 8 apud MAGALHÕES E GOMES, 2021, p.174). Outrossim, analisa-se ainda a eficiência do uso desses sistemas de reconhecimento facial que são utilizados pela Metropolitan Police - NeoFace Watch, tendo em vista que através de demonstrações, 98% dos casos, pessoas que eram inocentes foram reconhecidas de forma equivocada (BIG BROTHER WATCH, 2018, p. 3 apud MAGALHÕES E GOMES, 2021, p.174).

Deste modo, esses sistemas, juntamente com a unificação dos dados pessoais dos cidadãos, em uma única plataforma, podem trazer enormes riscos para os últimos, como os que já foram abordados acima e além do mais, pode ter ainda a exclusão de uma parcela da sociedade, se estas não obtiverem notas positivas. Ademais, pode haver a invasão de crackers, fazendo uma utilização dessas informações de forma maldosa, e ainda, existe a possibilidade de vazamento desses dados, como aconteceu recentemente com 220 milhões de pessoas, segundo a Agência Brasil.

No ofício enviado à ANPD, a Ordem dos Advogados manifesta preocupação com o vazamento, que compreende uma base de CPFs em número superior ao da população brasileira. São 37 bases de dados que abarcam nome, endereço, foto, score de crédito, renda, situação na Receita Federal e Instituto Nacional do Seguro Social (INSS). Parte dos dados, como nome e CPF, foi publicada na internet gratuitamente. Já o conjunto completo dos registros está sendo vendido em fóruns da rede. (OAB PEDE INVESTIGAÇÃO DO VAZAMENTO DE DADOS DE 220 MILHÕES DE PESSOAS, 2021)

De acordo com o que foi noticiado por essa agência, verifica-se que essa divulgação causou um risco muito grande para as pessoas, visto que muitos de seus dados foram propagados de forma gratuita na internet e ainda muitos deles estão sendo comercializados, ou seja, uma vez que essas informações foram espalhadas, nunca mais vão ser apagadas, tendo em vista que no momento de sua divulgação podem ter sido armazenadas por diversas pessoas, que possivelmente intencionam-se em usufruir de maneira excessivamente proveitosa, sendo capaz de causar graves lesões na vida do titular destes dados, podendo ter a violação do direito a dignidade da pessoa humana, prevista no artigo 1º, no inciso III, da Constituição da República Federativa do Brasil de 1988.

Ademais, é significativo salientar que o direito ao esquecimento, muitas vezes associado ao direito a intimidade, a vida privada, a honra e a imagem das pessoas é uma garantia prevista pela Constituição em seu artigo 5º, inciso X e ainda pelo Código Civil em seu artigo 21, contudo, este direito no âmbito da internet é complicado de ser tutelado, como já dito anteriormente.

2.3. A segurança pública em confronto com a autodeterminação informativa, a transparência e o direito à privacidade

A segurança pública, como um direito tutelado pelo Estado, pode acabar gerando conflitos com outros direitos, deste modo, o compartilhamento de informações pessoais da sociedade em geral, entre órgãos e entidades da administração pública federal, pode acarretar em possíveis violações de alguns direitos, como é o caso da autodeterminação informativa, prevista no Art. 2º, inciso II, da Lei Geral de Proteção de Dados Pessoais, levando em consideração que um dos fundamentos para a disciplina da proteção dos dados pessoais é justamente essa tutela. Destarte, faz-se mister, uma alusão ao conceito desse direito de acordo com Canotilho (2000, p.507) “faculdade de o particular determinar e controlar a utilização de seus dados pessoais”.

Considerando o conceito mencionado acima, atentando-se ao fato de que o Decreto 10.046 não prevê que haja explicações de qual seria a real finalidade do uso das informações destes cidadãos, tem-se assim, uma afronta ao princípio da transparência na administração pública, positivada na Lei nº 12.527/2011, que segundo Martins (p.5):

A nova Lei da Transparência visa regular a relação jurídica que se compõe do direito à informação dos cidadãos e do dever de prestação de informações por parte do Poder Público em sentido bem amplo. A amplitude pode ser vista no parágrafo único do art. 1º da lei, que, em seus incisos, engloba a União, Estados, Distrito Federal e municípios, todos os poderes republicanos, bem como os entes controlados e até as empresas (públicas e sociedades de economia mista), nas quais haja controle pelo Estado. Ainda, o art. 2º da lei define que ela se aplica às entidades privadas que recebam verbas públicas.

Logo, uma vez que não se tenha previsão de forma clara da utilização das informações da sociedade pela administração pública, ocorre, dessa maneira, uma colisão com o direito da autodeterminação informativa, como já tinha sido referenciado acima.

A própria LGPD diz que o tratamento de dados pessoais tem como um de seus princípios sua finalidade, tendo que ter propósitos legítimos, específicos, explícitos e informados ao titular, dizendo que a posteriori, só será possível realiza-lo se for compatível com as mesmas.

Reforçando novamente, este Decreto não se atenta a questão do propósito explícito e sobre a questão da informação que deve ser dada ao titular, pois não existe uma explicação detalhada para utilização de cada dado. Entretanto, a autodeterminação informativa é essencial para que não haja uma perseguição ou uma massiva vigilância estatal, em que se fosse fazer um regaste histórico, teria a Ditadura Militar como exemplo, no qual, neste período foram produzidos pelo Estado diversos documentos que estão até hoje guardados em arquivos públicos, sendo muitas vezes utilizados para oprimir certas pessoas, tendo uma grande intolerância política, religiosa e intelectual.

Nesta época, tentaram até mesmo criar o RENAPE (Registro Nacional de Pessoas Naturais), que seria um banco de dados unificado com informações dos cidadãos brasileiros, contudo, sua criação não deu certo.

Sabe-se que a Ditadura foi uma época de grande violação à direitos humanos, por isso, foi até mesmo criado o remédio constitucional, denominado como habeas data, para que as pessoas conseguissem acessar os dados que as pertenciam, principalmente de banco de dados de aparelhos policiais e de censura, como o Departamento de Ordem Política e Social (DOPS).

No Brasil, a trajetória deste remédio constitucional teve início juntamente com a vigência da Constituição Federal de 1988, porém, sua discussão existe desde a época da ditadura militar. Em 1964, foi criado o Serviço Nacional de Informação (SNI), um órgão estatal que fiscalizava e amedrontava a população, em razão das torturas e perseguições. Após o período de recessão democrática era necessário um recurso que permitisse as informações adquiridas durante as duas décadas de ditadura militar (TRUGILLO e AMARAL, p.3)

Assim como ocorreu nesse período histórico supramencionado, o uso dessas informações como forma de perseguições, de censura e até mesmo de torturas são muito utilizadas em outros regimes autoritários.

[...] um pressuposto para uma administração pública eficiente é o conhecimento tão acurado quanto possível da população [...], o que implica, por exemplo, a realização de censos e pesquisas e o estabelecimento de regras para tornar compulsória a comunicação de determinadas informações pessoais à administração pública. Em relação ao controle, basta acenar às várias formas de controle social que podem ser desempenhadas pelo Estado e que seriam potencializadas com a maior disponibilidade de informações sobre os cidadãos, aumentando seu poder sobre os indivíduos - não é por outro motivo que um forte controle da informação é característica comum aos regimes totalitários (DONEDA, 2020, p. 34, apud, SIQUEIRA, LARA E ALVES, 2021, p. 309-310).

Entretanto o Brasil é o um Estado Democrático de Direito, que visa o oposto desses outros regimes, por isso o acesso à informação é algo tão valioso.

A informação é o oxigênio da democracia. Nessa toada, esclarece que a democracia acontece nos países nos quais os cidadãos possuem capacidade

de tomar decisões que os atingem. Depreende-se, pois, que a informação é princípio fundamental das democracias, em todas suas acepções. Assim, as sociedades democráticas devem dispor de mecanismos diversificados e eficazes de envolvimento das ações estatais, não só por eleições periódicas, mas, principalmente, nos campos de fiscalização e avaliações dos projetos e políticas públicas. (MENDEL, 2009, apud MONTOLLI, 2020, p. 8).

Além disso, durante o século XX, foram aprovadas várias normas de proteção de dados pessoais em todo o mundo, como descreve Doneda:

No século XX, foram aprovadas quatro gerações de normas de proteção aos dados pessoais em todo o mundo. A primeira surgiu na década de 70 e foi contra a concepção de centralização de bancos de dados nos países. A segunda geração está relacionada ao consentimento do cidadão e o real exercício de sua liberdade de escolha. A terceira (iniciada na década de 80) é marcada pela formulação de um direito à autodeterminação informativa, fornecendo uma participação maior do cidadão sobre seus dados pessoais desde a coleta, o armazenamento e a transmissão. A quarta geração surgiu para tentar melhorar as gerações anteriores. Nesta última geração, algumas normas fortaleceram a posição do indivíduo por meio de normativas. (DONEDA, 2011, apud MONTOLLI, 2020, p. 8).

Exemplos de legislações da quarta geração que possuem grande destaque mundialmente:

Ainda com relação a quarta geração, as que mais se destacam globalmente são: Lei Federal de Proteção de Dados alemã, legislação da Noruega, da Finlândia, da Dinamarca, da França, da Grã-Bretanha, da Suíça e a Diretiva Europeia sobre proteção de dados pessoais de 1995. Essa geração tem como principal característica oferecer aos usuários das redes de internet maior autocontrole sobre seus dados pessoais, com a preocupação de não permitir que o titular dos dados considerados sensíveis possa decidir se fornece ou não, ou seja, cria-se uma imposição para a proteção dos dados sensíveis. O aumento de normas setoriais sobre a proteção de dados pessoais visa à complementação das normas gerais, fornecendo detalhes específicos e culturais para a proteção dos dados dos cidadãos dos respectivos países. (BEZERRA, 2019, apud MONTOLLI, 2020, p. 8).

No Brasil a principal legislação que regula as questões do tratamento e da coleta dos dados pessoais é a Lei Geral de Proteção de Dados Pessoais (LGPD), que foi sancionada pela Lei nº 13.709. Sendo de suma importância, pois, além da proteção de dados online, está também protege dados offline, que de acordo com Leonardi (2011, p. 122) “A tutela de dados pessoais é essencial para a manutenção da estrutura social e da vida comunitária”.

Outrossim, atenta-se ainda a questão do direito à privacidade, tendo em vista que houve uma mudança de significado do mesmo, dado que ocorreu uma transformação da sociedade e um avanço nos meios tecnológicos, que de acordo com Bessa:

Se é certo que, em sua origem, a privacidade estava associada ao direito de ser deixado em paz – right to be alone –, a preocupação de hoje é proteger o cidadão em relação aos modernos – e cada vez mais eficientes – mecanismos da informática de tratamento (coleta, armazenamento e difusão) de dados. (Bessa, 2019, p. 48)

Por isso, o direito à privacidade na era da sociedade da informação, deve ser olhado com muito cuidado, tendo em vista, que ele pode ser violado de diversas maneiras, podendo pegar como exemplo, o próprio dado pessoal, uma vez que houve a violação da privacidade da pessoa, coletando esses dados e até mesmo vazando com os mesmos, isso irá causar danos irreparáveis para elas, podendo ainda, gerar danos morais para as mesmas. Desta maneira é válido ressaltar o que Mendes e Doneda (2018) dizem: “não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação” (apud, SIQUEIRA, LARA e ALVES, 2021, p.301).

3. CONSIDERAÇÕES FINAIS

Diante da argumentação apresentada ao longo desse ensaio, verificou-se que a tecnologia permitiu diversas transformações em seus mais variados aspectos, proporcionando proveitos inimagináveis.

Uma dessas principais transformações foi justamente a simplificação na unificação e coleta de dados pessoais. No entanto essa simplificação, por mais oportuna que seja, acabou gerando alguns problemas, os quais, como analisado neste artigo, podem acarretar a violação de diversos direitos. Em uma vigilância massiva, pode até mesmo dar ensejo à exclusão de pessoas da sociedade, tornando-as mais vulneráveis, como ocorre no caso do Sistema de Crédito Social, utilizado pela China, o qual leva em consideração a atribuição de notas para as atitudes de seus cidadãos.

Verificou-se a necessidade de solidificar a compreensão de que a utilização de dados, principalmente pelo poder público, seja tratada fidedignamente no tocante a sua finalidade. Talvez essa seja uma das poucas formas de se assegurar que a proteção das informações pessoais dos cidadãos seja realizada da maneira mais acertada.

Além disso, também é preciso considerar o dever de ofício, por parte do Poder Público, sobre a necessidade de existência de reforço por parte do governo para que não ocorra vazamento de dados e ainda uma maior proteção na segurança deles, buscando incansavelmente a ocorrência de o ataque de crackers, como medida inevitável de promoção da segurança e estabilidade da sociedade.

4. REFERÊNCIAS

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Rio de Janeiro: Zahar, 2014.

CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da constituição**. 5 ed. Coimbra: Almedina, 2000.

CARVALHO, William Anderson Eloi de. **VIGILÂNCIA DAS FORÇAS DE SEGURANÇA ATRAVÉS DE CÂMERAS DE RECONHECIMENTO FACIAL E O CONFLITO COM O DIREITO À PRIVACIDADE – BRASIL E PORTUGAL**. 2019. 123 f. Dissertação (Mestrado) - Curso de Direito, Universidade Nova de Lisboa, Lisboa, 2019. Disponível em: https://run.unl.pt/bitstream/10362/97545/1/Carvalho_2020.pdf. Acesso em: 20 abr. 2021.

CENTRAL CFTV. Disponível em: <http://www.centralcftv.com/>. Acesso em: 18 abr. 2021

CHINA: PROBLEMAS EMERGENTES E MEDIDAS PARA ORIENTAR A OPINIÃO PÚBLICA E COMBATER A DISSIDÊNCIA. São Paulo: Matrizes, v. 13, n. 2, 2019. Disponível em: <file:///C:/Users/55306130/Downloads/161831-Texto%20do%20artigo-367305-1-10-20190904.pdf>. Acesso em: 18 abr. 2021.

CUNHA, Maria Alexandra *et al.* **SMART CITIES: transformação digital de cidades**. São Paulo: Fgv Eaesp, 2016. 83 p. Disponível em: https://ceapg.fgv.br/sites/ceapg.fgv.br/files/u60/smart_cities_bra_versao_final.pdf. Acesso em: 19 abr. 2021.

GIBSON, William. **Neuromancer**. São Paulo: Aleph, 2013. 237 p.

GUSMÃO, Katiúscia Valle Souza. **CONTROLE INTERNO E SISTEMA DE INFORMAÇÃO GERENCIAL: ESTUDO EM UMA FUNDAÇÃO MUNICIPAL**. 2018. 29 f. Monografia (Doutorado) - Curso de Gestão Pública, Universidade da Integração Internacional da Lusofonia Afro- Brasileira Instituto de Educação A Distância Especialização em Gestão Pública, São Francisco do Conde, 2018. Disponível em: http://www.repositorio.unilab.edu.br:8080/xmlui/bitstream/handle/123456789/980/2018_mon_o_kgusmao.pdf?sequence=1&isAllowed=y. Acesso em: 19 abr. 2021.

MAGALHÃES, Alice Azevedo *et al.* **REGULAÇÃO DE SISTEMAS DE RECONHECIMENTO FACIAL PARA FINS DE SEGURANÇA PÚBLICA NO BRASIL: RISCOS E DESAFIOS**. 2021. 15 f. Tese (Doutorado) - Curso de Direito, Universidade Federal da Bahia, Bahia, 2021. Disponível em: <https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/5639>. Acesso em: 22 nov. 2021.

MARTINS, Humberto. **LEI DA TRANSPARÊNCIA E SUA APLICAÇÃO NA ADMINISTRAÇÃO PÚBLICA: VALORES, DIREITO E TECNOLOGIA EM EVOLUÇÃO**. Disponível em: https://www.stj.jus.br/internet_docs/ministros/Discursos/0001182/LEI%20DA%20TRANSPAR%C3%84NCIA%20E%20SUA%20APLICA%C3%87%C3%83O%20NA%20ADMINISTRA%C3%87%C3%83O%20P%C3%94BLICA%20VALORES,%20DIREITO%20E%20TECNOLOGIA%20EM%20EVOLU%C3%87%C3%83O.pdf. Acesso em: 20 abr. 2021.

MEZZAROBÀ, Orides; MONTEIRO, Cláudia Servilha. **Manual de Metodologia da Pesquisa no Direito**. 6. ed. rev. e atual. São Paulo: Saraiva, 2014

MONTEIRO, Silvana Drumond. O Ciberespaço: o termo, a definição e o conceito: the cyberspace: the term, the definition and the concept. **Revista de Ciência da Informação**, [s. l.], v. 8, n. 3, p. 1-20.

MONTOLLI, Carolina. **SEGURANÇA DA INFORMAÇÃO: TRANSPARÊNCIA E PROTEÇÃO DE DADOS NA ADMINISTRAÇÃO PÚBLICA: LGPD, ACESSO À INFORMAÇÃO E OS INCENTIVOS À INOVAÇÃO E À PESQUISA CIENTÍFICA E TECNOLÓGICA NO ÂMBITO DO ESTADO DE MINAS GERAIS**. **Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro**, Rio de Janeiro, v. 3, n. 3, p. 1-23, 2020. Disponível em:

file:///C:/Users/55306130/Downloads/176-Texto%20do%20artigo-428-1-10-20201231.pdf.
Acesso em: 27 abr. 2021.

OAB PEDE INVESTIGAÇÃO DO VAZAMENTO DE DADOS DE 220 MILHÕES DE PESSOAS. Brasília: Agência Brasil, 2021. Disponível em: <https://agenciabrasil.ebc.com.br/justica/noticia/2021-01/oab-pede-investigacao-do-vazamento-de-dados-de-220-milhoes-de-pessoas>. Acesso em: 19 abr. 2021.

PRESIDÊNCIA DA REPÚBLICA SECRETARIA-GERAL SUBCHEFIA PARA ASSUNTOS JURÍDICOS. Constituição (2019). Decreto nº 10.046, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. **Disposições Gerais.** Brasília, DF, 10 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 18 abr. 2020.

SIQUEIRA, Dirceu Pereira *et al.* DIREITOS DA PERSONALIDADE, PROTEÇÃO DE DADOS PESSOAIS E O PODER PÚBLICO. **Revista Húmus**, [s. l.], v. 25, n. 11, p. 296-317. Disponível em: file:///C:/Users/55306130/Downloads/16011-50462-1-PB.pdf. Acesso em: 26 abr. 2021.

SOARES, Defilna Fernanda Moreira Garcês de Sá. **Interoperabilidade entre sistemas de informação na Administração Pública.** 2009. 666 f. Tese (Doutorado) - Curso de Engenharia, Universidade do Minho. Disponível em: <http://hdl.handle.net/1822/10539>. Acesso em: 20 abr. 2021.

TRUGILLO, Muriel de Lima *et al.* **HABEAS DATA E O MARCO CIVIL DA INTERNET.** Disponível em: file:///C:/Users/55306130/Downloads/4109-10623-1-PB.pdf. Acesso em: 20 abr. 2021.

Contatos: giovannaargolo@icloud.com e larissa.puerta@mackenzie.br