Múltiplos Olhares em Ciência da Informação

VOLUME 12, 2022
ISSN: 2237-6658

ARTIGO

A LGPD E A ATUAÇÃO DE ARQUIVISTAS E CIDADÃOS EM RELAÇÃO À PROTEÇÃO DE DADOS PESSOAIS

THE LGPD AND THE ACTIVITIES OF ARCHIVISTS AND CITIZENS IN RELATION TO THE PROTECTION OF PERSONAL DATA

Suellen Alves de Melo
Bacharel em Arquivologia, Universidade Federal de Minas Gerais, alvesdemelo.s@gmail.com
https://orcid.org/0000-0002-9674-595X

Como citar este artigo (ABNT):
MELO, S. A. de. A LGPD e a atuação de arquivistas e cidadãos em relação à proteção de dados pessoais. Múltiplos Olhares em Ciência da Informação, Belo Horizonte, v. 12, p. 103-120, dezembro./dezembro. 2022. DOI: https://doi.org/10.35699/2237-6658.2022.42046

Recebido em: 07/12/2022. **Revisado em:** 22/12/2022. **Aceito em:** 22/12/2022.

Acesso Aberto

Copyright: Esta obra está licenciada com uma Licença Creative Commons Atribuição 4.0 Internacional.

Conflito de interesses: Os autores declaram que não há conflito de interesses.

Financiamento: Não há.

Declaração de Disponibilidade dos dados: Todos os dados relevantes estão disponíveis neste artigo.

RESUMO

A partir do capitalismo de vigilância, reflete sobre a importância do debate da proteção de dados pessoais por profissionais com formação em Arquivologia e pelos cidadãos, tendo em vista que a temática vigilância e privacidade impacta esses dois grupos. Com isso, apresenta parte dos dispositivos da Lei Geral de Proteção de Dados Pessoais, além de discussões sobre a gestão e a elaboração de estudos de usuários de arquivo com base em dados pessoais e acerca de casos em que instituições agiram incorretamente em relação ao tratamento de dados. Considera que é necessário que arquivistas atuem respeitando princípios éticos e observando os dispositivos da Lei, que os cidadãos reflitam criticamente sobre a atuação de instituição públicas e privadas em relação ao tratamento de seus dados, assim como que políticas públicas que envolvam vigilância e privacidade sejam construídas pelo Estado em conjunto com a sociedade.

Palavras-Chave: Vigilância e privacidade. Capitalismo de vigilância. Lei Geral de Proteção de Dados Pessoais. Arquivistas e cidadãos.

ABSTRACT

Based on surveillance capitalism, it reflects on the importance of the debate on the protection of personal data by professionals trained in Archivology and by citizens, considering that the issue of surveillance and privacy impacts these two groups. With this, it presents part of the provisions of the General Law for the Protection of Personal Data, in addition to discussions on the management and preparation of studies of file users based on personal data and on cases in which institutions acted incorrectly in relation to the treatment of data. Considers that it is necessary for archivists to act respecting ethical principles and observing the provisions of the Law, for citizens to critically reflect on the performance of public and private institutions in

relation to the processing of their data, as well as for public policies involving surveillance and privacy to be constructed by the State together with society.

Keywords: Surveillance and privacy. Surveillance capitalism. General Law for the Protection of Personal Data. Archivists and citizens

1 INTRODUÇÃO

Vigilância e privacidade são palavras que emergem na contemporaneidade, sobretudo pelo uso acentuado de artefatos tecnológicos conectados à internet e pela comunicação em tempo real nas mídias sociais *on-line*, como Facebook e Instagram. O significado da palavra vigilância relaciona-se ao ato de vigiar, à prudência e à atenção desvelada na realização ou cumprimento de algo. Por sua vez, o significado de privacidade refere-se à vida particular de alguém e ao direito que as pessoas têm de não revelar informações ao seu respeito (GODOY, 2021; MICHAELIS, 2022).

Apesar do termo vigilância estar relacionado com prudência - cautela de quem quer evitar perigos -, na prática, nem sempre a cautela é percebida como algo positivo nos processos de vigilância (MICHAELIS, 2022). Isto porque, um estabelecimento comercial pode utilizar câmeras de monitoramento para garantir parte da segurança do local, no entanto, ao mesmo tempo em que executa esta ação, também vigia os comportamentos sociais dos indivíduos naquele lugar, podendo utilizar essa informação para benefício próprio. Assim, a prudência relativa à vigilância depende do ponto de referência. Para o comerciante é prudente vigiar seu estabelecimento. No entanto, a pessoa vigiada tem sua privacidade invadida. Na perspectiva das interações sociais mediadas pela internet, a discussão em torno dessa questão tende a se tornar ainda mais potente.

A professora de Harvard, Shoshana Zuboff (2021, p. 14), apresenta sua definição para capitalismo de vigilância como "uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas", assim como "[...] uma expropriação de direitos humanos críticos que pode ser mais bem compreendida como um golpe vindo de cima: uma destituição da soberania dos indivíduos.". Ainda de acordo com a autora, no capitalismo de vigilância, a experiência humana é captada por meio de dados disponibilizados pelas pessoas em dispositivos inteligentes conectados em rede (ZUBOFF, 2021). A partir dos dados coletados, os capitalistas de vigilância são dotados do poder instrumentário, ou instrumentarismo, que é usado para conhecer e modelar os comportamentos humanos para fins de terceiros (ZUBOFF, 2021).

Cathy O'Neil (2020) também elucida essa questão ao apontar que, por volta de 2008, a Matemática deixou de ter seu foco nos mercados financeiros e passou a enfatizar os seres humanos. Para a autora, a economia do *big data* anunciava ganhos extraordinários, já que, por exemplo, um *software* poderia encontrar um grande número de currículos e organizá-los, apresentando "[...] os candidatos mais promissores no topo" (O'NEIL, 2020, p. 5). Assim, além da economia com o tempo gasto na execução da atividade, o serviço também aparentava ser imparcial e objetivo, já que a ideia da neutralidade da máquina era vendida às pessoas. No entanto, é notório que as

ferramentas tecnológicas dependem de comandos construídos e executados pelos seres humanos, dessa forma, a imparcialidade e a objetividade podem ser, no mínimo, questionadas.

Posto isso, a vigilância contemporânea está pautada principalmente na coleta e na análise de dados pessoais. Mas, o que são dados pessoais? De acordo com a Lei n. 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), dados pessoais são todas as informações relacionadas a pessoas naturais identificadas ou identificáveis (BRASIL, 2018). Dessa forma, nome, idade, CPF (Cadastro de Pessoa Física) e naturalidade são exemplos simples de dados pessoais. A LGPD também apresenta a definição de dados pessoais sensíveis, a qual engloba dados pessoais sobre convicção religiosa, opinião política, saúde ou vida sexual, origem racial ou étnica, filiação a sindicato ou a organização religiosa, filosófica ou política, dado genético ou biométrico (BRASIL, 2018). Ou seja, dados sensíveis são aqueles que podem ser usados de maneira mal intencionada para gerar discriminação à pessoa natural.

A critério de exemplificação, um cadastro no Facebook solicita a inserção de dados pessoais como nome completo, número de celular ou *e-mail*, data de nascimento e gênero (FACEBOOK, 2022). Além disso, os usuários também podem inserir outros dados, como sua convicção religiosa. Sem contar nos dados coletados a partir de páginas seguidas e de mensagens envidas pela rede social de Mark Zuckerberg. O usuário cadastrado no Facebook tem seus dados coletados pela empresa norte-americana a partir de uma série de parâmetros estabelecidos na política de privacidade dessa mídia social. Ocorre que, muitas vezes, as pessoas não leem a política de privacidade e, consequentemente, não sabem quais dados são coletados e para quais finalidades.

O próprio Facebook já foi acusado pelo uso inapropriado dos dados de seus usuários, como no caso conhecido como o escândalo da Cambridge Analytica, empresa de análise dados que, em 2016, teve acesso aos dados de pessoas cadastradas na rede social norte-americana e, na sequência, utilizou as informações coletadas para influenciar os eleitores dos Estados Unidos durante a votação para presidente, possibilitando em certa medida a vitória de Donald Trump (BBC NEWS, 2018). Além do uso político, os dados pessoais também podem ser usados de outras formas, como, por exemplo, quando determinada plataforma *on-line* correlaciona o endereço dos indivíduos com o potencial deles pagarem ou não empréstimos bancários, conforme cita Cathy O'Neil (2020).

Dentre tantas possibilidades, o resultado desse cruzamento de dados pode, por exemplo, impossibilitar que alguém que more na periferia de uma cidade consiga a aprovação de crédito para a compra de um imóvel.

A coleta e a análise de dados pessoais não devem estar alheias à reflexão das pessoas, uma vez que esses processos modificam seus comportamentos, como apontado por Zuboff (2021),

trazendo implicações reais às suas vidas. Por isso, é fundamental que a temática vigilância e proteção de dados pessoais seja regulada por dispositivos legais e discutida em diversas esferas da vida social. Profissionais que lidam diretamente com tratamento e organização da informação, como bibliotecários, arquivistas e analistas de *big data*, dentre outros, devem refletir sobre a relação entre vigilância e privacidade, assim como sobre os impactos que seus ofícios podem causar à sociedade. Além da questão profissional, é imprescindível que as pessoas saibam os direitos estipulados em legislações específicas de proteção de dados e também que possam participar ativamente da construção de políticas públicas que englobem vigilância e proteção de dados
pessoais.

Essas questões possibilitam a inserção e a relevância deste texto na discussão em torno da vigilância *versus* privacidade, na medida em que sua finalidade é contextualizar brevemente a Lei Geral de Proteção de Dados Pessoais e, em seguida, apresentar quais são seus impactos no quefazer de profissionais da informação, sobretudo em relação ao labor de arquivistas, e na vida cotidiana dos cidadãos brasileiros. Para alcançar êxito, a pesquisa buscou artigos científicos que discutem a temática, assim como casos noticiados sobre o uso e o compartilhamento indevido de dados pessoais por empresas e pelo Estado brasileiro.

2 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Já dizia a canção dos Titãs (1985), *homem primata, capitalismo selvagem*. Deste modo, como enfrentar as corporações internacionais que ditam o mundo globalizado contemporâneo? Como enfrentar o capitalismo de vigilância? Como enfrentar esse contexto se o Estado continua pautado pelo neoliberalismo? Primeiramente, é preciso que fique claro que esses enfrentamentos não são fáceis de serem feitos. Para Zuboff (2021, p. 25, grifos da autora),

> o capitalismo de vigilância age por meio de assimetrias nunca antes vistas referentes ao conhecimento e ao poder que dele resulta. Ele sabe tudo *sobre nós*, ao passo que suas operações são programadas para não serem conhecidas por nós. Elas acumulam vastos domínios de um conhecimento novo *proveniente de nós*, mas que não é *para nós*. Elas predizem nosso futuro a fim de gerar ganhos para os outros, não para nós.

Independentemente deste contexto, a dificuldade não pode ser um agente de impossibilidade, pelo contrário, deve ser um aspecto de propulsão de mudança de cenário. Mesmo estando "vendido" para a iniciativa privada em algumas situações, o Estado democrático ainda deve ter sua atuação pautada, entre outros princípios, pela cidadania e dignidade da pessoa humana. Ou seja, é seu dever, dentre outras atribuições, regulamentar as relações entre as corporações desse novo capitalismo e as pessoas que utilizam seus serviços. Essa regulamentação é imprescindível para que a tecnicidade e a aparente falta de intencionalidade dos aparatos

tecnológicos inteligentes e dos serviços disponibilizados na internet possam ser desveladas e estruturadas a partir de direitos e deveres de ambas partes.

Assim, a legislação brasileira concernente às questões de vigilância e proteção de dados pessoais é um veículo fundamental para essa regulamentação, já que é um dos componentes de uma política pública. O professor José Maria Jardim (2006, s.n.) explica que "as políticas públicas tendem a serem compreendidas como o 'Estado em ação', ou seja, o Estado implantando um projeto de governo.". Jardim (2006) também destaca que apenas dispositivos legais não bastam para identificar a existência de uma política pública, tendo em vista que outros elementos também são importantes, como os agentes envolvidos (Estado e sociedade civil) e os recursos estabelecidos para a consecução da política. Além disso, o ciclo "formulação, implementação e avaliação" é fundamental para o estabelecimento e o funcionamento de uma política pública.

Ao discutir sobre políticas públicas de informação, o autor afirma que, notadamente, a ideia de "política de informação" vem englobando ações promovidas por áreas como arquivos, bibliotecas, governo eletrônico, tecnologia da informação, entre outras. Ainda para o autor, um conjunto de decisões que digam respeito ao campo da informação, podem não resultar em uma formalização de política pública de informação, visto que esta "[...] é mais que a soma de um determinado número de programas de trabalho, sistemas e serviços." (JARDIM, 2006, s.n.).

Dito isso, analisar a LGPD isoladamente pela seara da política pública de informação torna-se um tanto quanto árduo, sobretudo porque, a exemplo de outras legislações brasileiras, esse dispositivo legal é resultado de imposições colocadas por outros países, neste caso, pelos países pertencentes ao bloco econômico da União Europeia (LORENZON, 2021). No entanto, conhecer e discutir a Lei Geral de Proteção de Dados Pessoais são ações igualmente fundamentais para que ocorram diálogos e mudanças nas relações entre corporações do capitalismo de vigilância e a sociedade.

Sendo assim, ao comparar a LGPD com o Regulamento Geral sobre Proteção de Dados (GDPR, em inglês) da União Europeia a partir de seus instrumentos de *enforcement*, a pesquisadora do campo de Relações Internacionais, Laila Lorenzon (2021), afirmou que as discussões sobre direitos e deveres relacionados à privacidade cresceu à medida que os recursos e a utilização da internet aumentaram. Para ela, essas discussões têm como finalidade possibilitar que as pessoas

> [...] tenham maior controle sobre os próprios dados pessoais, compreendam melhor a importância que esses possuem no ambiente virtual e o perigo que se apresenta com a ausência de regulamentações apropriadas para salvaguardar suas informações pessoais. (LORENZON, 2021, p. 40-41).

O trabalho que deu origem ao GDPR se iniciou em 2012, tendo sido finalizado em 2016, todavia, a aplicação do regulamento europeu passou a ser obrigatória apenas dois anos mais tarde. A legislação de proteção de dados europeia foi pioneira ao conceder diversos direitos às pessoas em relação à privacidade no meio virtual, bem como a exigir que as corporações que lidam com dados tenham atitudes responsáveis. Por ser a primeira regulamentação sobre o assunto e também por ser considerada uma das mais completas, a lei europeia vem sendo empregada como base para a elaboração de legislações sobre privacidade virtual em vários países (LORENZON, 2021). Um exemplo, é a própria LGPD, a qual utiliza de conceitos semelhantes aos registrados no marco legal da União Europeia, como a definição de "dado pessoal".

A respeito dessa tendência, cabe uma reflexão. Pela atual configuração econômica do mundo globalizado, a delimitação de legislações estrangeiras impacta vários segmentos, como, por exemplo, a venda de alimentos de origem animal e vegetal. Assim, os países exportadores cumprem determinadas normas de outras nações, para que suas economias não sejam prejudicadas. Portanto, não seria diferente em relação à legislação de proteção de dados, ainda mais porque a internet amplia as relações econômicas. Dessa forma, as legislações nacionais necessitam dialogar entre si para que os negócios continuem sendo realizados satisfatoriamente. É claro que os países, especialmente os do sul global (CASSINO, 2021), não podem apenas traduzir as normas de outros países. É necessário que a realidade e a soberania nacionais sejam respeitadas.

Em relação ao contexto brasileiro, o professor Moisés Rockembach (2020) explica que os fundamentos da LGPD trazem à tona alguns conflitos que precisam ser discutidos, como, por exemplo, os direitos de acesso à informação e à memória em oposição aos "[...] direitos ao esquecimento, à autodeterminação informativa, à vida privada, à intimidade, à honra e à imagem." (ROCKEMBACH, 2020, p. 106). A proteção de dados pessoais no Brasil tem como fundamentos: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, Lei n. 13.709, 2018, Art. 2º).

Aprovada em agosto de 2018, a LGPD passou a vigorar a partir de agosto de 2020, em plena pandemia de Covid-19. O dispositivo legal brasileiro dispõe sobre o tratamento de dados pessoais, inclusive em meios digitais. Isso significa que tanto a farmácia que pede o número de CPF aos seus clientes quanto um aplicativo digital devem obedecer às disposições previstas na Lei Geral de Proteção de Dados Pessoais. É importante destacar que a aplicação da LGPD independe

do meio utilizado no tratamento de dados pessoais, do país de sede do controlador de dados ou do país onde estão localizados os dados. Além disso, a LGPD deve ser obedecida por todos os entes federativos (BRASIL, 2018).

A Lei Geral de Proteção de Dados Pessoais não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e sem fins econômicos, ou para o tratamento realizado para fins jornalístico, artístico e acadêmicos, ou para o tratamento realizado com fins voltados à segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. Em relação aos requisitos para o tratamento de dados pessoais, a Lei estipula que este procedimento apenas poderá ser feito em determinadas situações, entre elas, com o consentimento de seu titular - por isso é importante conhecer o conteúdo das políticas de privacidade -; para o cumprimento de obrigação legal ou regulatória pelo controlador; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (BRASIL, 2018).

Em relação aos direitos do titular dos dados, a qualquer momento e mediante requisição, as pessoas têm direito a confirmar a existência de tratamento; ter acesso aos dados; solicitar correção de dados incompletos, inexatos ou desatualizados; solicitar anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD; solicitar portabilidade de dados; solicitar eliminação dos dados pessoais; solicitar informação das entidades com as quais o controlador compartilhou seus dados; entre outras ações (BRASIL, 2018).

Com os objetivos de zelar pela proteção de dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e de Privacidade, fiscalizar e aplicar sanções, entre outros, a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com sede e foro no Distrito Federal (BRASIL, 2018). Apesar disso, de acordo com Lorenzon (2021), por estar vinculada à Presidência da República, a ANPD pode ter seu poder de fiscalização diminuído em relação aos órgãos do governo brasileiro, sobretudo em relação ao tratamento de dados pessoais empregados na elaboração de políticas públicas.

É importante ressaltar que a legislação não é "letra morta", sendo assim, modificações são normais, visto que os contextos social, político e econômico sofrem mudanças com o tempo. Dessa forma, a contextualização realizada neste trabalho sobre a LGPD, certamente, estará desatualizada com o tempo, por isso, é importante conferir o texto oficial da Lei. No entanto, a explanação

realizada é interessante na medida em que mostra que é possível se posicionar diante das corporações do capitalismo de vigilância, neste caso, por meio da legislação.

Contudo, conforme discutido, uma política pública não é apenas um conjunto de leis, assim, é fundamental que a sociedade civil participe dos fóruns de discussão relativos à privacidade e vigilância promovidos pelo Estado, para que as pessoas conheçam o que se passa nas caixas obscuras das tecnologias e dos serviços *on-line* e, em consequência, saibam também como os dados pessoais são tratados. Além disso, como os pais ensinam seus filhos, é necessário desconfiar do que é estranho, daquilo que se oferece de maneira fácil e sem custos. Conhecer as políticas de privacidade é essencial, já que, na LGPD, por exemplo, o consentimento é fundamental para a autorização do tratamento de dados.

3 IMPLICAÇÕES DA PROTEÇÃO DE DADOS PESSOAIS: ENTRE A PROFISSÃO E A CIDADANIA

A proteção de dados pessoais tem atravessado a vida profissional e cotidiana das pessoas, independentemente se o indivíduo está numa posição mais próxima às questões relacionadas à informação ou não. Todos lidam em maior ou menor quantidade com essa área, basta estar com um *smartphone* nas mãos. Em relação à Ciência da Informação, essa proximidade é mais nítida, tendo em vista que o campo lida justamente com os fenômenos relacionados à informação, como, por exemplo, o tratamento e a representação de informações. No Brasil, institucionalmente, áreas como Biblioteconomia e Arquivologia são enquadradas como subáreas da Ciência da Informação, especialmente na Tabela de Áreas do Conhecimento da CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) (CAPES, 2020).

Em relação à Biblioteconomia, as pessoas com formação na área podem trabalhar com a organização de banco de dados, catalogação de acervos e atendimento ao público presencial e à distância de unidades de informação, entre outros campos de atuação. Nesse sentido, a privacidade e a coleta de dados das pessoas é uma questão colocada em diversos aspectos dessa profissão, como, por exemplo, nos sistemas de empréstimo de livros, os quais, normalmente, coletam dados variados dos leitores, como, por exemplo, nome completo, endereço, matrícula ou CPF, *e-mail*, títulos de livros lidos, entre outras informações. Munidos desses dados, as pessoas com formação em Biblioteconomia devem estar conscientes que a má fé de algum profissional, da instituição ou mesmo da empresa proprietária do *software* de empréstimo de obras pode causar danos aos leitores. O compartilhamento dos dados dos leitores para outras plataformas digitais,

por exemplo, pode possibilitar a correlação de dados e, por conseguinte, gerar análises discriminatórias ou predileções mercadológicas.

Com o objetivo de aproximar a discussão de proteção de dados com a Arquivologia, este trabalho tem como intenção enfatizar essa área, já que, muitas vezes, legislações que dizem respeito aos documentos de arquivo, como a Lei de Acesso à Informação (LAI), Lei n. 12.527, de 18 de novembro de 2011, não estabelecem diálogo com a Arquivística. No caso da LGPD, é comum encontrar notícias que registram o vazamento de dados pessoais ou o compartilhamento de dados pessoais sob a tutela do Estado com a iniciativa privada que focam apenas nos dados pessoais, sem mencionar que tais dados estão registrados em documentos de arquivo. A critério de esclarecimento, todo documento produzido e/ou recebido por pessoas físicas ou jurídicas durante a execução de suas atividades é considerado documento de arquivo.

Como exemplo da problemática citada acima, Silveira (2021), ao discutir sobre o colonialismo de dados e o neoliberalismo, inicia seu trabalho apresentando o caso do Tribunal de Justiça de São Paulo que, em 2019, tinha como objetivo hospedar os processos judiciais sob sua guarda em uma nuvem da Microsoft - por intervenção do Conselho Nacional de Justiça, o contrato não foi executado. Todavia, o autor apenas evidencia em seu texto a falta de discussão em noticiários brasileiros sobre o risco do compartilhamento dos dados pessoais de brasileiros com uma instituição de outro país, quando, na verdade, o contrato previa o compartilhamento de processos judiciais, ou seja, de documentos de arquivo. Os dados pessoais poderiam ser extraídos dos processos, contudo, os processos é que seriam compartilhados com a Microsoft.

A esse respeito é interessante evidenciar como os documentos de arquivo podem ser empregados para a extração de dados e, consequentemente, para a correlação de dados pessoais coletados de outras formas. Assim, a terceirização da guarda de documentos digitais em nuvens privadas nacionais e internacionais, conforme exemplo apresentado por Silveira (2021), coloca em risco o direito à privacidade e possibilita o uso indevido de dados pessoais sem que os indivíduos possam consentir em sua utilização. Mesmo que existam contratos estabelecidos entre o Estado e a iniciativa privada para a execução do serviço, acreditar que esses documentos de ajuste sejam seguidos cuidadosamente é um tanto quanto inocente (SILVEIRA, 2021), tendo em vista que, como apontado por Zuboff (2021), o capitalismo atual é o de vigilância.

Em 2021, o Arquivo Nacional do Brasil, publicou o dossiê temático “Dados e arquivos” na Revista Acervo, demonstrando que a área tem se preocupado com a questão da proteção de dados, sobretudo pelo fato de a produção de documentos de arquivo está ocorrendo com maior ênfase no ambiente digital (ARQUIVO NACIONAL, 2021). Entre os artigos publicados, o trabalho

"Reflexões sobre a contribuição da gestão de documentos para programas de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD)" merece destaque.

De autoria de Schwaitzer, Nascimento e Costa (2021), o trabalho busca apresentar em que medida a gestão de documentos (GD) pode contribuir para a adequação da LGPD. A gestão de documentos é uma área da Arquivologia que surgiu após a Segunda Guerra Mundial, quando houve um aumento exponencial na produção documental e passou a ser necessário estabelecer critérios para a gestão dos arquivos. Sendo assim, a gestão de documentos lida com os processos que perpassam a elaboração, classificação, tramitação, avaliação e destinação (eliminação ou recolhimento) dos documentos de arquivo (SCHWAITZER; NASCIMENTO; COSTA, 2021).

Os autores levantam uma discussão fundamental em relação ao "*status*" do documento de arquivo na contemporaneidade. A produção de documentos no meio digital contribui para o surgimento de alguns desafios aos profissionais da área, como, por exemplo, a manutenção da materialidade do documento. Isto porque, é normal ouvir que no contexto digital não há mais documento, somente informação (SCHWAITZER; NASCIMENTO; COSTA, 2021). Nesse sentido, para os autores,

> com a edição da LGPD, esse processo de indução e de desassociação da unidade de tratamento ao conhecimento arquivístico é ainda mais pungente, já que a unidade de tratamento não é mais o documento, como previsto na Lei de Arquivos, nem a informação, como consta na LAI, mas os dados. (SCHWAITZER; NASCIMENTO; COSTA, 2021, p. 13).

Ainda de acordo com os autores, ao reconhecer que os dados necessitam ser organizados para serem compreendidos como informação e que esta, por sua vez, somente pode ser considerada confiável, integra e autêntica quando está registrada em um documento de arquivo, fica notória a importância da gestão de documentos "[...] para que ocorra uma eficiente e correta adequação à LGPD." (SCHWAITZER; NASCIMENTO; COSTA, 2021, p. 14). Dessa forma, os autores afirmam que uma instituição que já tenha programas de gestão de documentos incorporados às suas rotinas, certamente, tem melhores condições de adaptação aos dispositivos estabelecidos na LGPD. Como conclusão, afirmam que

> [...] apesar de o mercado brasileiro estar sendo dominado por profissionais da área de tecnologia da informação e do direito, quando se trata de auxiliar os agentes na identificação, classificação, avaliação e delimitação de tempo de tratamento e hipóteses de guarda conforme previsto em lei, o arquivista, por meio da adoção de um programa de GD, é um dos profissionais mais bem preparados para enfrentar o desafio atual de implantação e adequação à LGPD. Sendo assim, se o arquivista possui as competências para o desenvolvimento da GD, ele está apto, consequentemente, a coordenar programas de adequação à LGPD, preservando os interesses organizacionais e protegendo o direito dos titulares dos dados. (SCHWAITZER; NASCIMENTO; COSTA, 2021, p. 16).

Portanto, com as reflexões desses autores, fica nítida a importância da gestão de documentos para a adequação à LGPD, contribuindo para que a área de proteção de dados

pessoais também seja exercida por pessoas com formação em Arquivologia. Além disso, como enfatizaram os autores, é importante destacar que, apesar da Lei Geral de Proteção de Dados Pessoais focar nos dados pessoais, estes não estão "pairando" nas plataformas *on-line*, ao contrário, fazem parte de documentos de arquivo.

O professor Moisés Rockembach (2020) também discutiu os impactos da LGPD na Arquivologia, sobretudo em relação aos estudos de usuários. De acordo com o autor, os estudos de usuários são fundamentais para que as instituições arquivísticas possam promover o acesso aos documentos de arquivo. Tal objetivo converge para a difusão de arquivos, função arquivística que possibilita o acesso aos documentos a partir de estratégias de acessibilidade, transparência, mediação e *marketing* (ROCKEMBACH, 2020). Assim, páginas em mídias sociais *on-line*, palestras, exposições, instrumentos de pesquisa, visitas guiadas são exemplos de estratégias de difusão que possibilitam que o público conheça os documentos custodiados pelas instituições arquivísticas e, consequentemente, que venha a ter interesse em consultá-los mais detalhadamente.

Ainda de acordo com o autor, ao conhecer os perfis e as necessidades dos usuários, podem ser realizadas modificações em "[...] sistemas de informação e nas formas de recuperação" (ROCKEMBACH, 2020, p. 106). Pensando em estudos de usuários de arquivo, a partir das análises de perfis e necessidades, é possível, por exemplo, modificar determinadas informações nas descrições de fundos de arquivo, sobretudo em relação aos pontos de acesso mais pesquisados pelos consulentes nos repositórios digitais, facilitando a recuperação dos resultados. Além disso, também é possível definir estratégias de educação pelo patrimônio arquivístico, como, por exemplo, eleger o conjunto documental a ser explorado e as atividades que serão construídas junto com o público.

Para Rockembach (2020), os estudos de usuários podem valer-se da coleta de dados a partir de plataformas do ambiente digital e de aplicativos móveis, sendo que os dados podem

> [...] ser coletados tanto na pesquisa por conteúdos dos acervos, perfis dos usuários e informações fornecidas pelos mesmos, como pelo uso de diferentes serviços que podem ser oferecidos pelos arquivos. Além disto, os dados que podem ser analisados pelas redes sociais (Facebook, Instagram, Twitter, Youtube, entre outras) dos perfis ou páginas das instituições, fornecem importantes informações sobre os usuários, levando em consideração a interatividade produzida. (ROCKEMBACH, 2020, p. 108).

Apesar de os estudos de usuários de arquivo poderem utilizar de dados pessoais, o autor enfatiza a importância de que as questões éticas não sejam deixadas de lado. Nesse sentido, Rockembach (2020) discute sobre a observância dos dispositivos da LGPD, bem como sobre a Resolução n. 510, de 07 de abril de 2016, do Conselho Nacional de Saúde, a qual trata de aspectos éticos de pesquisas realizadas no âmbito das ciências humanas e sociais. O autor conclui o trabalho

destacando o papel da ética nas questões que envolvem o tratamento de dados pessoais. De acordo com ele, para que a LGPD tenha efetividade

> [...] faz-se necessária uma mudança de cultura organizacional, de como pensamos os sistemas de informação, a adoção de princípios éticos digitais e procedimentos de coleta, análise e disseminação dos dados. A ética digital torna-se, portanto, uma extensão da ética no mundo real, com novos problemas e dilemas. Faz-se necessário pensar, representar e colocar em prática as virtudes em ambientes digitais, da mesma forma que fazemos fora deles. (ROCKEMBACH, 2020, p. 113).

A partir dos dois textos, é possível perceber que o tratamento e a proteção de dados pessoais, sobretudo em relação à LGPD, impõem possibilidades e desafios à Arquivística. Fazendo um paralelo como os documentos de arquivo, o tratamento de dados pessoais pode fazer parte do quefazer de arquivistas nas fases corrente, intermediária e permanente. Ou seja, profissionais da área podem contribuir para a gestão de dados pessoais a partir da gestão de documentos e, também, para a promoção da difusão e do acesso aos documentos, neste caso, especialmente, quando o foco são os arquivos permanentes. No entanto, a atuação de pessoas formadas em Arquivologia nessas atividades não pode estar descolada da aplicação das normativas vigentes, como, por exemplo, a LGPD, e dos princípios éticos. Nesse caso, o capitalismo de vigilância deve se sujeitar ao consentimento das pessoas e à transparência dos procedimentos de coleta, tratamento, uso e compartilhamento de dados pessoais.

Dito isso, ao se pensar na proteção de dados em relação aos cidadãos, ou seja, sem levar em conta o espaço profissional das pessoas, as discussões aumentam consideravelmente, tendo em vista que, nesse caso, os indivíduos estão no lado oposto do capitalismo de vigilância, já que os dados coletados pelas instituições são deles. Nesse sentido, serão apresentados três exemplos em que as pessoas tiveram sua privacidade invadida por procedimento executados tanto pela iniciativa privada, quanto pelo Estado brasileiro, tendo em vista que o objetivo é que esses casos remetam à relevância que há no debate da proteção de dados pessoais. Isso porque, como apresentado pelo pesquisador da área de Direito, Bruno Bioni (2018), proteção de dados pessoais importa, visto que, no atual contexto, seus dados são você.

Dito isso, o primeiro exemplo evoca um cenário recente no Brasil, trata-se do compartilhamento de dados de beneficiários de uma política governamental estabelecida durante a pandemia de Covid-19, o Auxílio Emergencial, programa que destinou recursos financeiros para pessoas cadastradas no Cadastro Único (CadÚnico). Nessa perspectiva, o trabalho de Oliveira e Araújo (2020) teve como objetivo contextualizar os dados pessoais dos beneficiários do Auxílio Emergencial a partir de sua natureza, para apontar se a atitude do Estado em compartilhar tais dados no Portal da Transparência foi correta ou não.

Durante a discussão, os autores enfatizam que a natureza de dados pessoais e de dados pessoais sensíveis não pode ser alterada se esses tornam-se dados públicos. O Estado também deve obedecer aos dispositivos regidos pela LGPD. Contudo, no caso dos beneficiários do Auxílio Emergencial não houve a observância da Lei por parte do governo, visto que, em junho de 2020, dados de cerca de 57 milhões de pessoas que receberam o benefício foram divulgados no Portal da Transparência, como, por exemplo, estado, cidade, Número de Identificação Social (NIS), seis dígitos do CPF, nome completo do beneficiário e valor recebido por cada cidadã e cidadão (OLIVEIRA; ARAÚJO, 2020). Ainda de acordo com os autores, o objetivo do Estado era possibilitar que a sociedade fiscalizasse o governo, no entanto, o que houve foi a violação do direito à privacidade (OLIVEIRA; ARAÚJO, 2020).

Os autores apontam que "[...] nem todo dado governamental é público e, quando não o é, não poderá se 'aberto', a exemplo dos dados sigilosos, como é o caso dos dados dos beneficiários do auxílio emergencial [...]" (OLIVEIRA; ARAÚJO, 2020, p. 7). Isto porque, de acordo com o Decreto n. 11.016, de 29 de março de 2022, os dados de identificação das famílias cadastradas no CadÚnico são sigilosos e somente podem ser usados para gestão de políticas públicas e realização de estudos e pesquisas (BRASIL, 2022). Nesse sentido, fica evidente que o governo federal agiu de maneira incorreta ao compartilhar os dados pessoais dos beneficiários do Auxílio Emergencial.

Além de possibilitar a reflexão sobre em que medida a transparência do governo e o direito ao acesso à informação podem impactar a privacidade das pessoas, conforme elucidado por Rockembach (2020), o caso apresentado também é interessante pelo fato de que, posteriormente, os dados pessoais compartilhados foram alvo de correlação com dados coletados em outro contexto. De acordo com Ferreira (2021), pessoas que passaram para a segunda etapa do vestibular da Universidade de São Paulo em 2021 e que receberam Auxílio Emergencial tiveram seu CPF exposto no mês de fevereiro daquele ano.

A correlação ocorreu da seguinte forma: "[...] a lista de convocados à segunda fase do vestibular inclui os primeiros seis dígitos do CPF do candidato. Já o governo federal divulga os dígitos intermediários do CPF de quem recebe programas sociais." (FERREIRA, 2021, s.n.). Assim, foi possível identificar o número completo do CPF de cerca de 3.600 pessoas. Apesar de os objetivos das duas exposições de dados serem diferentes, fica claro que não há uma integração na atuação das instituições dos entes federativos do país, denotando a ausência ou ineficiência de uma política pública de informação nacional.

Ainda no campo da educação superior, Silveira (2021) apresenta outro exemplo acerca do compartilhamento de dados de brasileiros em plataformas estrangeiras. O autor explica que, em

2020, o Ministério da Educação hospedou dados do Sistema de Seleção Unificada (SiSU) na nuvem da Microsoft, a Azure. “Ou seja, hospedou os dados do desempenho escolar de milhões de estudantes brasileiros para serem tratados na plataforma estadunidense.” (SILVEIRA, 2021, p. 40). Com a justificativa de que manter um data center próprio envolve dotações orçamentárias altas e, além disso, que o serviço oferecido pelo corporação norte-americana é extremamente ágil, dados como notas do Exame Nacional do Ensino Médio (Enem), renda familiar e declaração de cor, entre outros, foram colocados à mercê de uma empresa estrangeira.

Diante desse caso, algumas perguntas emergem: Como um país entrega informações imprescindíveis de seus cidadãos para uma empresa de outro país? Como foram tratados os dados do SiSU? Eles poderão ser usados como moeda no capitalismo de vigilância? Bom, certamente que sim. Basta pensar que, mesmo sem consentimento, as corporações multinacionais já infringem a privacidade das pessoas, agora, imagine quando os dados são entregues cordialmente pelas instituições públicas nacionais a essas empresas.

Para finalizar os exemplos práticos, o Google não poderia ficar de fora da discussão. Este gigante da tecnologia mundial está presente na vida das pessoas em diversos aspectos, desde o envio de e-mails pelo Gmail, passando pelas pesquisas em seu buscador e visualizações de vídeos no YouTube, até o compartilhamento de arquivos no Google Drive, reuniões síncronas no Meet e criação de rotas de localização no Google Maps - apenas para citar algumas das ferramentas da empresa. Todos esses serviços coletam dados das pessoas, nesse sentido, não seria difícil encontrar casos em que a privacidade dos usuários não foi respeitada.

Ao pesquisar no próprio buscador da empresa será possível encontrar diversos casos nacionais e internacionais em que a atuação do Google em relação aos seus procedimentos de coleta de dados e de proteção de dados pessoais foi, no mínimo, posta em xeque. Em 2019, por exemplo, o escritório do Google no Brasil foi notificado pelo Ministério da Justiça a respeito de possíveis capturas de geolocalização em smartphones Android sem o consentimento dos usuários (GZH, 2019).

Apesar de a notícia não apresentar o desfecho do caso, fica claro que o Google continuou ofertando seus serviços ao povo brasileiro. Ainda assim, a explanação é relevante, tendo em vista que, se as ferramentas dessa empresa são capazes de categorizar trajetos cotidianos a partir da identificação “casa” ou “trabalho” e criar linhas do tempo de locais visitados a cada mês, é notório que os dados de localização dos usuários da plataforma também podem ser empregados pelo Google em outros campos, como, por exemplo, na publicidade. Ao saber o deslocamento das

pessoas, é possível traçar perfis e alterar o comportamento dos indivíduos, conforme discute Zuboff (2021). O que mais é possível?

4 CONSIDERAÇÕES FINAIS

Com o objetivo de apresentar a relevância da proteção de dados pessoais, este trabalho discutiu parte dos dispositivos da Lei Geral de Proteção de Dados Pessoais, assim como as possibilidades e os desafios impostos às pessoas com formação em Arquivologia na gestão e na elaboração de estudos de usuários tendo como base dados pessoais. Além disso, a partir de exemplos em que o Estado brasileiro e o Google agiram incorretamente em relação à proteção de dados pessoais, também foi possível debater sobre a relevância dessa temática no dia a dia dos indivíduos. Reitera-se, portanto, que as reflexões em torno da vigilância e da privacidade dos cidadãos, especialmente no ambiente digital, deve ser pauta de debate em diferentes arenas, como em escolas, sindicatos, organizações não governamentais, estabelecimentos comerciais, universidades, hospitais, núcleos familiares. Em relação aos profissionais, além de sua presença nas arenas de discussão, também é necessário que sua atuação se baseie em condutas éticas e na observância dos dispositivos da LGPD.

O capitalismo de vigilância é um capitalismo selvagem, na medida em que os dados das pessoas são coletados, tratados e analisados e, consequentemente, empregados contra os próprios indivíduos, já que essa nova ordem econômica beneficia os interesses das grandes corporações de tecnologia. Apesar da aparente pequenez do indivíduo frente a esse cenário, a reflexão apontada neste trabalho é fundamental para trazer à tona as inverdades da falta de parcialidade e da objetividade dos aparatos técnicos inteligentes, assim como da relevância da proteção de dados pessoais e das regulamentações governamentais neste campo. Parafraseando um filme, é como se as pessoas pudessem pausar a cena das vantagens de serviços *on-line* gratuitos e pudessem refletir
criticamente sobre como estão sendo vigiadas e “privatizadas” pelo Estado, Facebook, Google, Amazon...

Além disso, a partir dos exemplos discutidos é possível perceber que o Estado brasileiro tem agido com pouco rigor no que diz respeito à proteção de dados pessoais, tendo em vista que realiza contratos com empresas estrangeiras com o objetivo de armazenar na nuvem documentos de arquivo em formato digital de seus cidadãos. Esse cenário não é muito assustador, visto que o governo já age dessa forma ao negligenciar a gestão de documentos públicos e terceirizar a guarda

de conjuntos documentais em suporte papel de diversos órgãos e entidades de sua estrutura para empresas da iniciativa privada, nacionais e internacionais.

Essas práticas estão alicerçadas na política neoliberal do Estado que valoriza as empresas em detrimento dos serviços realizados pelo setor público, apresentando argumentos baseados na inovação e na agilidade do setor privado, bem como na redução de gastos da máquina estatal. Enquanto isso, a soberania do país e a privacidade da sociedade brasileira permanecem sendo cerceadas. Portanto, é imprescindível que o filme seja pausado para que Estado e sociedade possam construir juntos políticas públicas que envolvam dados pessoais, informações e documentos de arquivo relacionando o tratamento desse "grupo de registro de conhecimento humano" à temática de vigilância e privacidade.

REFERÊNCIAS

ARQUIVO NACIONAL (BRASIL). **Revista Acervo**, Rio de Janeiro, n. 3, set./dez. 2021. Disponível em: http://revistaacervo.an.gov.br/index.php/revistaacervo/issue/view/85. Acesso em: 06 dez. 2022.

BBC NEWS. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira das autoridades. Publicado em 20 mar. 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 06 dez. 2022.

BIONI, Bruno. Por que a proteção de dados pessoais importa? TEDx Pinheiros. YouTube, [2018]. Disponível em: https://www.youtube.com/watch?v=TzI5VfvQA6I&list=PLhBAp9bhJ5WnXX01WxSwCYfQ9TuHZMO_x&index=5&ab_channel=TEDxTalks. Acesso em: 07 dez. 2022.

BRASIL. **Decreto n. 11.016, de 29 de março de 2022**. Regulamenta o Cadastro Único para Programas Sociais do Governo Federal, instituído pelo art. 6º-F da Lei nº 8.742, de 7 de dezembro de 1993. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11016.htm#art15. Acesso em: 07 dez. 2022.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 06 dez. 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 06 dez. 2022.

CAPES (COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR). Tabela de Áreas de Conhecimento/Avaliação. Publicado em 19 set. 2020. Disponível em: https://www.gov.br/capes/pt-br/acesso-a-informacao/acoes-e-programas/avaliacao/instrumentos/documentos-de-apoio-1/tabela-de-areas-de-conhecimento-avaliacao. Acesso em: 06 dez. 2022.

CASSINO, João Francisco. O sul global e os desafios pós-coloniais na era digital. In: SILVEIRA, Sérgio Amadeu da; SOUZA, Joyce; CASSINO, João Francisco (Orgs.). **Colonialismo de dados**: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia Literária, 2021. p. 13- 31.

FACEBOOK. Criar nova conta. Disponível em: facebook.com. Acesso em: 06 dez. 2022.

FERREIRA, Daniel. Recebeu auxílio emergencial e foi bem na Fuvest? O seu CPF foi exposto. Publicado em Pindorama, em 26 jul. 2021. Disponível em: https://pindograma.com.br/2021/07/26/fuvest.html. Acesso em: 07 dez. 2022.

GODOY, Claudio Luiz Bueno de. Enciclopédia jurídica da PUC-SP. Privacidade. Publicado em 01 dez. 2021. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/474/edicao-1/privacidade. Acesso em: 06 dez. 2022.

GZH CIÊNCIA E TECNOLOGIA. Agência Brasil. Google é investigado sobre possível violação à privacidade dos usuários no Brasil. Publicado em 22 ago. 2019. Disponível em: https://gauchazh.clicrbs.com.br/tecnologia/noticia/2019/08/google-e-investigado-sobre-possivel-violacao-a-privacidade-dos-usuarios-no-brasil-cjzn19fjg052d01pa0u5ryeht.html. Acesso em: 07 dez. 2022.

JARDIM, José Maria. Políticas públicas arquivísticas: princípios, atores e processos. **Arquivo & Administração**, Rio de Janeiro, v. 5, n. 2, 2006. Disponível em: http://hdl.handle.net/20.500.11959/brapci/51586. Acesso em: 06 dez. 2022.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. In: FGV Direito Rio. (Org.). **Revista do Centro de Excelência Jean Monnet da FGV Direito Rio**. 1 ed. Rio de Janeiro: FGV Direito Rio, 2021, v. 1, p. 38-52. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rpdue/article/view/83423. Acesso em: 06 dez. 2022.

MICHAELLIS. **Dicionário brasileiro da língua portuguesa**. [s.l.]: Editora Melhoramentos, 2022. Disponível em: michaelis.uol.com.br. Acesso em: 06 dez. 2022.

OLIVEIRA, Adriana Carla Silva de; ARAÚJO, Douglas da Silva. O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados. **Liinc em Revista**, Rio de Janeiro, v. 16, n. 2, p. 1-11, dez. 2020. Disponível em: https://revista.ibict.br/liinc/article/view/5318. Acesso em: 06 dez. 2022.

O'NEIL, Cathy. **Algoritmo de destruição em massa**. Santo André: Editora Rua do Sabão, 2020. ROCKEMBACH, Moisés. Estudos de usuários de arquivo e os desafios da Lei Geral de Proteção de Dados. **Acervo**, Rio de Janeiro, v. 33, n. 3, p. 102-115, set. /dez. 2020. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/1554. Acesso em: 06 dez. 2022.

SILVEIRA, Sérgio Amadeu. A hipótese do colonialismo de dados e o neoliberalismo. In: SILVEIRA, Sérgio Amadeu da; SOUZA, Joyce; CASSINO, João Francisco (Orgs.). **Colonialismo de dados**: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia Literária, 2021. p. 33-51.

SCHWAITZER, Lenora; NASCIMENTO, Natália; COSTA, Alexandre de Souza. Reflexões sobre a contribuição da gestão de documentos para programas de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD). **Acerv**o, [S. l.], v. 34, n. 3, p. 1–17, 2021. Disponível em: http://revistaacervo.an.gov.br/index.php/revistaacervo/article/view/1732. Acesso em: 6 dez. 2022. TITÃS.

Homem primata. [s.l.]: Wander Music: 1985. CD (3'25'').

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira de poder. 1. ed. Rio de Janeiro: Editora Intrínseca Ltda., 2021.